Utrecht University

Graduate School of Natural Sciences

Cyclic algebras over local fields arising from elliptic curves

Master's thesis

Abe ten Voorde

Supervisor: dr. Lennart Meier
Second reader: prof. dr. Gunther Cornelissen

Abstract

We consider Brauer groups of local fields and determine which of its elements can be reached by cyclic algebras of the form (χ, Δ), where χ is a character for a cyclic Galois extension L/K of degree dividing 12 and Δ is the discriminant of an elliptic curve over K. We answer this question using the explicit norm groups of unramified extensions. For finite field extensions of $\mathbb{Q}_2$ and $\mathbb{Q}_3$ we restrict ourselves further to discriminants of elliptic curves over the ring of integers $\mathcal{O}_K$. For this restriction, the unramified extensions no longer provide an answer. Instead we use local class field theory to construct suitable cyclic extensions and prove that the image of the respective cyclic algebras depends on the presence of certain roots of unity in K.

We also give a brief introduction to the mathematical theory we have used. This includes the theory of local fields, Brauer groups and Hilbert symbols.

Contents

1 Introduction

The concept of a Brauer group of a field K was introduced by Richard Brauer. He used them in particular as a way to classify central division algebras of K. By Wedderburn's theorem the Brauer group can also be seen as a way to classify central simple algebras. We call two central simple algebras A and B equivalent if they differ by a matrix algebra, i.e. if there exist integers n and m such that

$$A \otimes_K M_n(K) \cong B \otimes_K M_m(K).$$

The Brauer group is defined as the set of equivalence classes of this relation.

Later, the Brauer group was identified with cohomology groups using Galois cohomology. This allowed Grothendieck ([Gro66]) to generalize the concept to Brauer groups of schemes. These groups have been used in mathematics ever since. One application is the Brauer-Manin obstruction, an obstruction to local-global principles ([Sko99]).

Another topic of interest are Brauer groups of stacks. One can for instance consider the Brauer group of the stack of elliptic curves over a scheme. Antieau and Meier studied this problem and found for instance that the Brauer group of the stack of elliptic curves over $\mathrm{Spec}(\mathbb{Z})$ is trivial ([AM16, 10.2]). In this thesis, we will further explore one question that came up in this article.

Let L/K a cyclic Galois field extension and $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/m\mathbb{Z}$ an isomorphism. For any $b \in K^*$ we can define a cyclic algebra

$$(\chi, a) := L\langle y\rangle/(y^m = a, \text{ and } xy = y\chi^{-1}(\bar{1})(x)\ \forall x \in L)$$

This is a central simple algebra over K and we consider its class in $\mathrm{Br}(K)$. A question that came up in [AM16] is what elements of $\mathrm{Br}(K)$ we can reach by letting a be the discriminant of some elliptic curve over K. The discriminant of an elliptic curve over K is defined modulo $(K^*)^{12}$. In order for the cyclic algebra (χ, Δ) to be well-defined, we need that m divides 12. Therefore we only consider cyclic field extensions of degree $m|12$.

In this thesis, we explore this question for local fields. We focus on extensions of $\mathbb{Q}_2$ and $\mathbb{Q}_3$, since 2 and 3 are the prime divisors of 12 and these are expected to be the most problematic cases. Using only unramified extensions, we show the following theorem.

Theorem 1.1. *Let K be any local field. Every element of $\mathrm{Br}(K)[12]$ is represented by a cyclic algebra of the form (χ, Δ), where $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/12\mathbb{Z}$ is some injective homomorphism associated to an extension L/K and $\Delta \in K^*$ is the discriminant of an elliptic curve over K. Any cyclic algebra of this form induces a 12-torsion element of $\mathrm{Br}(K)$.*

We also consider the same question for elliptic curves over the ring of integers $\mathcal{O}_K$ of a local field K. We show that in this case the unramified extensions lead only to trivial cyclic algebras. We prove the following results.

Theorem 1.2. *Let $K/\mathbb{Q}_2$ be a local field.*

- *If K contains a primitive third root of unity, every element of $\mathrm{Br}(K)[12]$ can be represented by a cyclic algebra (χ, Δ), where $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/12\mathbb{Z}$ is an injective morphism associated to a cyclic Galois extension L/K and $\Delta \in \mathcal{O}_K^*$ is the discriminant of an elliptic curve over $\mathcal{O}_K$.*
- *If K does not contain a primitive third root of unity, every element of $\mathrm{Br}(K)[4]$ can be represented by cyclic algebras of the form above, and all of them induce 4-torsion points.*

Theorem 1.3. *Let $K/\mathbb{Q}_3$ be a local field.*

- *If K contains a primitive fourth root of unity, every element of $\mathrm{Br}(K)[12]$ can be represented by a cyclic algebra (χ, Δ), where $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/12\mathbb{Z}$ is an injective morphism associated to a cyclic Galois extension L/K and $\Delta \in \mathcal{O}_K^*$ is the discriminant of an elliptic curve over $\mathcal{O}_K$.*
- *If K does not contain a primitive fourth root of unity, every element of $\mathrm{Br}(K)[6]$ can be represented by cyclic algebras of the form above, and all of them induce 6-torsion points.*

In order to prove these theorems we will need some preliminary theory. The first part of this thesis is devoted to stating the definitions and results that we will use as well as some general observations and examples that illustrate how the theory can be used. We will refer to textbooks for most of the proofs, but sometimes explore some of the ideas that go into the proofs.

We start of by stating the main results concerning local fields, including Hensel's lemma and the decomposition of the multiplicative group. We will discuss extensions of local fields emphasizing the role of unramified extensions, and introduce some relevant results from local class field theory.

Then we move on to a brief discussion of elliptic curves, Weierstrass equations and their discriminants. We define what it means for an elliptic curve to be defined over the ring of integers of a local field.

Thirdly, we introduce Brauer groups of fields. We will give the basic definitions of central simple algebras as well as their primary example, cyclic algebras. Here we will also make a brief note on Kummer theory.

After this, we introduce some important notions from (Galois) cohomology. We identify the most important groups that go into our construction as cohomology groups and see how cohomology can be applied to deduce some basic properties. We will see for instance that the Brauer group of a field is a torsion group. We will later use this observation in a brief illustration to prove that the Brauer group of any local field is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

The last concept we will introduce in the preliminaries is that of Hilbert symbols. They provide the main computational tools for dealing with cyclic algebras. We will discuss some of the formulas that can be used to compute them and provide some examples. Finally, we observe why we can often reduce to the case where our field contains relevant roots of unity. This is for instance important for defining Hilbert symbols and using Kummer theory.

In the second part of the thesis, we focus only on proving Theorem 1.1, 1.2 and 1.3. We provide an example of how one can deal with norm equations by using techniques similar to ones used for dealing with Diophantine equations, and also show how the theory of unramified extensions provides a more robust way of computing the order of cyclic algebras and proving Theorem 1.1.

In the final chapter we show that the unramified extensions are insufficient to prove Theorem 1.2 and 1.3. Instead we make explicit use of class field theory and the decomposition of the multiplicative group of a local fields to construct useful extensions and show that there are some obstructions when the base field does not contain the relevant roots of unity. Finally, we observe that a specific form of elliptic curves can be used to answer our questions without the need for explicit computations.

We end with a brief discussion on related questions and generalizations.

Part I
Preliminaries

Before we tackle the main topic of this thesis, let us familiarize ourselves with the underlying theory that we will make use of. The reader is assumed to have a basic grasp of algebra, including knowledge of p-adic numbers, commutative algebra and the basics of algebraic number theory. The most important notions are covered in the first two chapters of [Neu99]. The purpose of this part of the thesis is twofold: to introduce definitions and fix notation; and to state the most important results and computational tools we will use throughout the thesis. We will start by discussing the basic theory of local fields including local class field theory. We move on to a brief discussion of elliptic curves, including elliptic curves over the ring of integers of a local field. Then we define the Brauer group of a field. In Section 5, we will use cohomology to reformulate the main research question and more closely inspect Brauer groups of local fields. Finally, we take a look at Hilbert symbols, which give the main computational tools for dealing with cyclic algebras.

2 Local fields

In this section we will introduce the concept of local fields. We will mainly follow [Neu99, Ch. II] with some additions from [Lan94, Ch.I-II] and [Mil13, Ch. 1]. We will give the definitions and results that are important for our further study. Most proofs have been omitted but references have been included to look them up. Where possible, we will provide the reader with some general observations and examples that turn out to be useful later in this thesis.

We start with the basic definitions regarding local fields and give a general version of Hensel's Lemma. Then we will describe the decomposition of the multiplicative group of a local field. We consider extensions of local fields, where we place special emphasis on ramification and cyclotomic extensions. Finally, we state the main theorems of local class field theory. Applying this theory together with the decomposition of local fields gives us some powerful tools that we will use later on in this thesis.

For now, we will begin by recalling the definition of a valuation.

Definition 2.1. Let K be a field. A valuation on K is a function

$$v\colon K \to \mathbb{R} \cup \{\infty\},$$

with the following properties:

- $v(a) = \infty$ if and only if $a = 0$.

- $v(ab) = v(a) + v(b)$.
- $v(a+b) \geq \min\{v(a), v(b)\}$.

Here we adhere to the conventions $a + \infty = \infty$ and $\infty > a$ for all $a \in K$. A valuation v is called *discrete* if $v(K^*) = s\mathbb{Z}$ and *normalized* if $s = 1$. An element $\pi \in K$ with $v(\pi) = s$ is called a *prime element* or *uniformizer*.

Fixing an element $q \in \mathbb{R}_{>1}$, we also get an associated norm $|a| := q^{-v(a)}$ with the convention $q^{-\infty} = 0$. The norm is called *non-archimedean* if it satisfies the strong triangle inequality $|a+b| \leq \max\{|a|, |b|\}$ for all $a, b \in K$. Otherwise, we call it archimedean.

Definition 2.2. Let K be a field and v a valuation on K. We define the *ring of integers* of K as

$$\mathcal{O}_K := \{a \in K \mid v(a) \geq 0\}.$$

The units of $\mathcal{O}_K$ are precisely those $a \in K$ for which $v(a) = 0$. The unique maximal ideal is given by

$$\mathfrak{p}_K = \{a \in K \mid v(a) > 0\}.$$

We define the *residue field* of K as

$$\kappa_K = \mathcal{O}_K / \mathfrak{p}_K.$$

We sometimes consider the *higher order unit groups*

$$U_K^{(n)} = 1 + \mathfrak{p}_K^n \quad \text{for } n \geq 1.$$

When there is no ambiguity about the field K, we will sometimes omit the subscript.

Remark 2.3. Because the set of uniformizers of K is a strict subset of the prime ideal $\mathfrak{p}_K$, we will refrain from using the word *prime element*.

Example 2.4. Consider $\mathbb{Q}$ and some prime p. We have the valuation v_p defined as $v_p(\frac{a}{b}p^n) = n$ for any $a, b, n \in \mathbb{Z}$ with a and b both non-zero and coprime to p. The completion of $\mathbb{Q}$ with respect to this valuation is $\mathbb{Q}_p$. The ring of integers is $\mathbb{Z}_p$ and contains the uniformizer p. The residue field is $\mathbb{F}_p$.

Given a field K, complete with respect to a valuation v_K, and an extension L/K, there is a non-ambiguous way extend this to a valuation $v_{L/K}$ on L. If the extension is finite and $N_{L/K}$ is the norm, we can set

$$v_{L/K}(x) = v_K(N_{L/K}(x))/[L : K] \quad \text{for } x \in L.$$

See [Neu99, Thm. II.4.8] for a proof and precise statement, also in the case of infinite field extensions.

Since the norm can be extended this way, we get the inclusions

$$v_K(K^*) \subseteq v_{L/K}(L^*) \quad \text{and} \quad \kappa_K \subseteq \kappa_L.$$

Definition 2.5. The index $e(L/K) = (v_{L/K}(L^*) : v_K(K^*))$ is called the *ramification index*. The degree $f(L/K) = [\kappa_L : \kappa_K]$ of the associated extension κ_L/κ_K of residue fields is sometimes called the *inertia degree*.

Remark 2.6. In the remainder of this thesis, we use v_K to denote the normalized valuation, i.e. for any extension L/K

$$v_L(x) = e(L/K)v_{L/K}(x).$$

Proposition 2.7 ([Neu99, II.6.8])**.** *If L/K is separable and v_K is discrete, the product of the ramification index and the inertia degree is*

$$e(L/K)f(L/K) = [L : K].$$

We now move on to the definition of local fields. We use the following two equivalent definitions interchangeably.

Proposition 2.8 ([Neu99, II.5.2])**.** *Let K be a field. The following are equivalent:*

- *K is complete with respect to a discrete valuation and has a finite residue field.*
- *There is a prime p such that K is isomorphic to a finite field extension of either $\mathbb{F}_p((t))$ or $\mathbb{Q}_p$.*

A field satisfying these criteria is called a local field*.*

Remark 2.9. Some authors do not require the norm of a local field to be non-archimedean. In this case, $\mathbb{R}$ and $\mathbb{C}$ are also considered to be local fields. In the remainder of this thesis, all local fields are non-archimedean and have characteristic 0. Furthermore, we shall sometimes refer to finite extensions of $\mathbb{Q}_p$ as *local fields over $\mathbb{Q}_p$*.

One of the most useful tools for studying local fields is Hensel's Lemma. We will state a slightly more general version than used in some textbooks.

Lemma 2.10 ([Lan94, Proposition II.2.2])**.** *Let K be any field complete with respect to a valuation v. Let $f \in \mathcal{O}_K[X]$ be a polynomial and f' its formal derivative. If there exists $a_0 \in \mathcal{O}_K$ such that*

$$v(f(a_0)) > 2v(f'(a_0)),$$

then $f(X)$ has a root $a \in \mathcal{O}_K$ satisfying $a \equiv a_0 \mod \mathfrak{p}_K$.

Since any local field is complete with respect to its valuation, we can quickly deduce the more standard version of Hensel's lemma.

Lemma 2.11 (Hensel's Lemma)**.** *Let K be a local field and let $f \in \mathcal{O}_K[X]$ be a polynomial. If $a_0 \in \mathcal{O}_K$ satisfies*

$$f(a_0) \equiv 0 \mod \mathfrak{p}_K \quad \textit{and} \quad f'(a_0) \not\equiv 0 \mod \mathfrak{p}_K,$$

then there exists some $a \in \mathcal{O}_K$ with

$$f(a) = 0 \quad \textit{and} \quad a \equiv a_0 \mod \mathfrak{p}_K.$$

The reason we use Lemma 2.10 is illustrated by the following corollary.

Corollary 2.12. *Let $K/\mathbb{Q}_p$ be any local field and $u \in \mathcal{O}_K^*$ a unit. The class of u in $K^*/(K^*)^p$ is the same as that of $u + p^3$.*

Proof. We claim that $u + p^3 = ua^p$ for some $a \in K^*$. This is the case when a is a solution to

$$a^p - 1 - p^3 u^{-1} = 0.$$

In other words, we need that $f(X) = X^p - 1 - p^3 u^{-1}$ has a root in K. Plugging in $a_0 = 1 \in \mathcal{O}_K$, we get

$$v(f(1)) = v(-p^3 u^{-1}) = 3v(p) > 2v(p) = 2v(f'(1)).$$

By Lemma 2.10 f indeed has a root. □

2.1 Structure of the multiplicative group

A direct consequence of Hensel's Lemma is the decomposition of the multiplicative group of any local field. The details and proofs of these results can be found in paragraph II.5 of [Neu99]. We will state the main results of this paragraph as they are important for our study.

Proposition 2.13 ([Neu99, II.5.3])**.** *Let K be a local field of residue field order $q = \#\kappa$ and let π be a prime element. We have*

$$K^* = \pi^{\mathbb{Z}} \times \mathcal{O}_K^* = \pi^{\mathbb{Z}} \times \mu_{q-1} \times U^{(1)},$$

where μ_{q-1} denotes the group of roots of unity in K^* whose order divides $q - 1$.

For any unit $u \in \mathcal{O}_K^*$, we write $\omega(u) \in \mu_{q-1}$ for the root of unity with $u \equiv \omega(u) \mod \mathfrak{p}$.

A further decomposition can be given by explicitly describing the unit group $U^{(1)}$. For this we will need the log and exp maps.

Lemma 2.14 ([Neu99, II.5.5]). *Let $K/\mathbb{Q}_p$ be a local field and let $e \in \mathbb{Z}_{>0}$ be such that $p\mathcal{O}_K = \mathfrak{p}_K^e$.*[1] *Let $n > e/(p-1)$ and consider the maps*

$$\mathfrak{p}_K^n \underset{\log}{\overset{\exp}{\rightleftarrows}} U^{(n)}$$

given by the power series

$$\exp(x) = \sum_{j=0}^{\infty} \frac{x^j}{j!} \quad \text{and} \quad \log(1+y) = -\sum_{j=1}^{\infty} \frac{(-y)^j}{j}.$$

These define inverse homeomorphisms

Using this lemma and the fact that $U^{(1)}/U^{(n)}$ is finite, we can write $U^{(1)}$ as the product of a torsion group and a finitely generated $\mathbb{Z}_p$-module. This gives us the following decomposition statement.

Proposition 2.15 ([Neu99, II.5.7]). *Let $K/\mathbb{Q}_p$ be an extension of degree d. Let q be the order of the residue field and let π be a prime element. We have*

$$K^* \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d,$$

where μ_{p^a} are the roots of unity in K that have order divisible by p.

Proof sketch. The first and second summand are obtained from Proposition 2.13 and the isomorphisms

$$\mathbb{Z} \xrightarrow{\sim} \pi^{\mathbb{Z}},\ k \mapsto \pi^k,$$
$$\mathbb{Z}/(q-1)\mathbb{Z} \xrightarrow{\sim} \mu_{q-1},\ \bar{b} \mapsto \zeta_{q-1}^b,$$

for any choice of root of unity ζ_{q-1} of order $q-1$ and any choice of lift $b \in \mathbb{Z}$ of $\bar{b}$. The other two summands can be obtained as follows: use Lemma 2.14 to get

$$U^{(n)} \cong \mathfrak{p}_K^n = \pi^n \mathcal{O}_K \cong \mathcal{O}_K.$$

We can write $\mathcal{O}_K \cong \mathbb{Z}_p^d$ by choosing an integral basis. Since $U^{(n)}$ is a finitely generated $\mathbb{Z}_p$-module and $U^{(1)}/U^{(n)}$ is finite, $U^{(1)}$ is also a $\mathbb{Z}_p$-module of rank d. The torsion subgroup is μ_{p^a}, the group of roots of unity of p-power order in K. This allows us to split $U^{(1)}$ as follows:

$$U^{(1)} \cong \mu_{p^a} \times \mathbb{Z}_p^d \cong \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d.$$

Using these isomorphisms and Proposition 2.13 gives us the decomposition we want. □

[1] Every local field is a dicrete valuation ring and in such rings every non-zero ideal is a power of the maximal ideal.

Example 2.16. Consider $\mathbb{Q}_2(i)/\mathbb{Q}_2$. Since X^2+1 does not have a root modulo 4, it does not have a root in $\mathbb{Q}_2$ and so $\mathbb{Q}_2(i)/\mathbb{Q}_2$ is an extension of degree 2. Since the polynomial does have a root modulo 2, the residue field κ_K is isomorphic to $\mathbb{F}_2$.[2] The powers of i are the only roots of unity in $\mathbb{Q}_2(i)$. The multiplicative group K^* is isomorphic to

$$\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}_2^2.$$

2.2 Local field extensions

For the study of local fields in general, and this thesis in particular, it is important to understand the extensions of local fields. For brevity of results, for any local field K we fix some algebraic closure $\bar{K}$ and understand that all extensions L/K are subextensions of $\bar{K}/K$. At the start of Section 2 we saw that any extension L/K also has an associated extension κ_L/κ_K of residue fields. One distinguishing property of local field extensions is the relation between their degree and the degree of their residue fields.

Definition 2.17. Let L/K be an extension of local fields. If $[L:K]$ is equal to $f(L/K) = [\kappa_L : \kappa_K]$, we call the extension *unramified*. If $f(L/K) = 1$, we call the extension *totally ramified*.

One can use Hensel's Lemma again to prove the following proposition.

Proposition 2.18 ([Neu99, II.7.2])**.** *Let L/K be an unramified extension of local fields. Every subextension of L/K is unramified and for every finite extension K'/K, the extension LK'/K' is unramified.*

Note that given a degree n the (finite) residue fields always have a unique extension of degree n. Lifting the corresponding defining polynomial to the level of local fields, we get the following.

Proposition 2.19. *Let K be a local field and n a positive integer. There exists a unique unramified extension K_n/K of degree n. Moreover, this is a cyclic Galois extension.*

Proof. A proof following the argument above can be found in [Lan94, §II.4].

Another approach is to use local class field theory (Section 2.3) and note that there is a unique subgroup of K^* that corresponds to the unramified degree n extension (see Example 2.32). □

Example 2.20. Note that the polynomial X^2+1 is irreducible modulo 3, and so $\mathbb{Q}_3(i)$ is the unique unramified extension of degree 2 over $\mathbb{Q}_3$. To contrast, we have already seen in Example 2.16 that $\mathbb{Q}_2(i)$ is totally ramified. The unramified degree 2 extension of $\mathbb{Q}_2$ is given by $\mathbb{Q}_2(\zeta_3) = \mathbb{Q}_2(\sqrt{-3})$, where ζ_3 is a primitive cube root of unity.

[2] We can pick the uniformizer $1-i$.

Remark 2.21. The composition of two unramified extensions is unramified. The composite of all unramified subextensions of an extension L/K is $T_{L/K}$, the maximal unramified subextension. The maximal unramified extension of $\bar{K}/K$ is denoted by $K_{un} = \bigcup_n K_n$.

Proposition 2.22 ([Neu99, 7.5])**.** *Let L/K be an extension of local fields and T the maximal unramified subextension. Then κ_T equals the separable closure of κ_K in κ_L.*

The example above is actually interesting for our further studies. Let us take a closer look at these cyclotomic extensions. We treat the two extreme cases of unramified extensions and totally ramified extensions separately.

Proposition 2.23 ([Neu99, II.7.12])**.** *Let K be a local field with residue field $\mathbb{F}_{p^r}$ and let n be an integer, prime to p. Consider the extension $L = K(\zeta_n)$ for some primitive n-th root of unity. The extension is unramified of degree d, where d is the smallest positive integer such that $p^{dr} \equiv 1 \mod n$. The Galois group is canonically isomorphic to the Galois group of κ_L/κ_K and is generated by $\zeta_n \mapsto \zeta_n^{p^r}$. The ring of integers is given by $\mathcal{O}_L = \mathcal{O}_K[\zeta_n]$.*

Corollary 2.24. *The unique unramified extension of degree d over K is given by $K(\zeta_{q^d-1})$, where $q = \#\kappa_K$. Any uniformizer of K is also a uniformizer of $K(\zeta_{q^d-1})$.*

Proof. The first follows immediately by picking $n = q^d - 1$ in the proposition.

To prove the second statement, we take any uniformizer π of K, i.e. an element $\pi \in K$ such that $\kappa_K = \mathcal{O}_K/\pi\mathcal{O}_K$. Let $L = K(\zeta_{q^d-1})$ and note that by Proposition 2.23 we have that $\mathcal{O}_L/\pi\mathcal{O}_L$ equals

$$\mathcal{O}_K[\zeta_{q^d-1}]/\pi\mathcal{O}_K[\zeta_{q^d-1}] \cong (\mathcal{O}_K/\pi\mathcal{O}_K)[\zeta_{q^d-1}] \cong \kappa_K[\zeta_{q^d-1}] \cong \mathbb{F}_{q^d-1} \cong \kappa_L.$$

This shows that π is a uniformizer for L as well. □

Proposition 2.25 ([Neu99, II.7.13])**.** *The extension $\mathbb{Q}_p(\zeta_{p^r})/\mathbb{Q}_p$ is totally ramified of degree $\varphi(p^r) = (p-1)p^{r-1}$, the Galois group is isomorphic to $(\mathbb{Z}/r\mathbb{Z})^*$. The element $\pi = 1 - \zeta_{p^r}$ is a uniformizer and the ring of integers is given by $\mathbb{Z}_p[\pi] = \mathbb{Z}_p[\zeta_{p^r}]$.*

For both Proposition 2.23 and 2.25, Neukirch uses Nakayama's Lemma to describe the ring of integers. The same argument applies in a more general setting in Lang's book.

Proposition 2.26 ([Lan94, I.8.23])**.** *Let A be a discrete valuation domain, K its quotient field, L a finite separable extension over K and B the integral closure of A in L. Let $\mathfrak{p}$ be the maximal ideal of A and assume $\mathfrak{q}$ is the only ideal of B above it. Let $\beta \in B$ be a generator of $B/\mathfrak{q}$ over $A/\mathfrak{p}$ and let $\pi \in \mathfrak{q} \setminus \mathfrak{q}^2$. Then $B = A[\beta, \pi]$.*

Corollary 2.27. *Let L/K be a Galois extension of local fields. Let π_L be any uniformizer of L and set $q = \#\kappa_K$ and $f = f(L/K) = [\kappa_L : \kappa_K]$. Then $\mathcal{O}_L = \mathcal{O}_K[\zeta_{q^f-1}, \pi]$, for a root of unity ζ_{q^f-1} of order $q^f - 1$.*

Proof. We shall apply Proposition 2.26 with

$$(A, B, \mathfrak{p}, \mathfrak{q}, \beta, \pi) := (\mathcal{O}_K, \mathcal{O}_L, \mathfrak{p}_K, \mathfrak{p}_L, \zeta_{q^f-1}, \pi_L).$$

To do this, we first need to show that these choices satisfy the criteria of the proposition. Because π_L is a uniformizer, we indeed have $\pi_L \in \mathfrak{p}_L \setminus \mathfrak{p}_L^2$. Also, we know that $\kappa_L \cong \mathbb{F}_{q^f} \cong \mathbb{F}_q[\zeta_{q^f-1}]$ is generated by ζ_{q^f-1}. We only have to prove that $\zeta_{q^f-1} \in \mathcal{O}_L$.

Note that L contains the maximal unramified subextension $T_{L/K}$. By Proposition 2.22 $T_{L/K}$ is the unique unramified extension of K of degree f. By Proposition 2.23, this extension is given by $K(\zeta_{q^f-1})$ and so $\zeta_{q^f-1} \in L$. Clearly, the valuation of ζ_{q^f-1} is zero and so it is an element of $\mathcal{O}_L$. □

2.3 Local class field theory

One of the more complicated theories of this thesis is class field theory. As usual, we are primarily interested in the application of this theory. As such, we will only state the main results and refer to textbooks such as [Neu99] and [Mil13] for a more in-depth approach. See [Ser79] for a cohomological treatment of local class field theory. Also, we will only be considering the local version of class field theory and avoid ideles, which are needed to study the global version.

For the remainder of this section, we will fix a local field K. Its algebraic closure is denoted by $\bar{K}$ and the maximal abelian extension in $\bar{K}$ by K_{ab}.

Note that by the uniqueness of unramified extensions Proposition 2.23 gives all unramified extensions L/K. The Galois group of L/K is isomorphic to that of κ_L/κ_K. The latter is generated by the Frobenius morphism $\alpha \mapsto \alpha^q$. The corresponding generator for $\mathrm{Gal}(L/K)$ is called the *Frobenius element* $\mathrm{Frob}_{L/K}$.

One of the main results of local class field theory, the reciprocity law, can be formulated as follows.

Theorem 2.28 ([Mil13, Thm. 1.1])**.** *There exists a unique morphism*

$$\phi_K \colon K^* \to \mathrm{Gal}(K_{ab}/K),$$

satisfying the following properties:

- *For any unramified extension L/K and uniformizer $\pi \in K$, we have $\phi_K(\pi)|_L = \mathrm{Frob}_{L/K}$.*
- *For any abelian extension L/K, ϕ_K induces an isomorphism*

$$\phi_{L/K} \colon K^*/N_{L/K}(L^*) \to \mathrm{Gal}(L/K), \quad \bar{a} \mapsto \phi_K(a)|_L.$$

Among other things, the theorem allows us to describe $\mathrm{Gal}(L/K)$ using the norm subgroup $N_{L/K}(L^*)$ of K^*.

The other main ingredient for class field theory is the Existence Theorem. It tells us that that the norm subgroups are actually all subgroups of K^* of finite index.

Theorem 2.29 ([Mil13, Thm. 1.2])**.** *Let $N \subset K^*$ be a subgroup. Then there exists a finite extension L/K with $N = N_{L/K}(L^*)$ if and only if N has finite index.*

Remark 2.30. By Theorem 2.28 the index of N equals the degree of L/K.

Corollary 2.31. *The map $L \mapsto N_{L/K}(L^*)$ is an inclusion reversing bijection between the finite abelian extensions of K and the subgroups of finite index in K^*.*

One interesting case to look at is that of unramified extensions. By their uniqueness property they are often the easiest to work with.

Example 2.32. Let L/K be an unramified extension of degree d. Let π be a uniformizer of K. By Corollary 2.24, π is also a uniformizer in L. By Proposition 2.13 we have

$$\begin{aligned} N_{L/K}(L^*) &= N_{L/K}(\pi)^{\mathbb{Z}} \times N_{L/K}(\mathcal{O}_L^*) \\ &= \pi^{d\mathbb{Z}} \times N_{L/K}(\mathcal{O}_L^*). \end{aligned}$$

Because $N_{L/K}(L^*)$ has index d by Theorem 2.28, it must equal $\pi^{d\mathbb{Z}} \times \mathcal{O}_K^*$. This also shows that the norm is surjective when seen as a map on the units $\mathcal{O}_L^* \to \mathcal{O}_K^*$. By Corollary 2.31 these arguments also show the uniqueness of unramified extensions, which we stated in Proposition 2.19.

Corollary 2.33. *Any subgroup N of finite index in K^* that contains a uniformizer π of K, is the norm group of a totally ramified extension L/K.*

Proof. By Theorem 2.29, N is the norm group of some abelian extension L/K. If L/K is not totally ramified, it has an unramified subextension of degree $d \geq 2$. This unramified subextension corresponds to a subgroup $M \subset K^*$ containing N, because the assignment $L \mapsto N_{L/K}(L^*)$ is inclusion reversing. But by Example 2.32 $\pi \notin M$. This is a contradiction, so L/K must be totally ramified. □

3 Elliptic curves

While elliptic curves play an important role for our research question, this thesis mainly focuses on the discriminant of elliptic curves. The theory of elliptic curves is vast and these curves play an important role in virtually

any area of algebra. To see more than the bare minimum of the theory of elliptic curves that we will present in this thesis, the reader is advised to take a look at [Sil09] and [KM85].

We will define elliptic curves over fields and introduce Weierstrass equations of elliptic curves. Using Weierstrass equations, we also define the discriminant of an elliptic curve, the primary invariant we are concerned with. Finally we will give a definition of an elliptic curve over a the ring of integers of a local field.

Definition 3.1. Let K be a field. An elliptic curve over K is a pair (E, O), where E is a smooth curve of genus 1 over K and $O \in E(K)$ is a designated element. An isomorphism of elliptic curves (E, O) and (E', O') is an isomorphism of curves $E \xrightarrow{\sim} E'$ that sends O to O'.

Remark 3.2. As we are not focused on O in this thesis, we will often simply write E for the elliptic curve (E, O) and assume O is understood.

Using the Riemann-Roch theorem ([Sil09, II.5.4]), one can show that every elliptic curve over K is isomorphic to a curve given by a Weierstrass equation.

Definition 3.3. A *Weierstrass equation* is an equation of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{1}$$

If $a_i \in K$, such an equation defines a curve over K.

Remark 3.4. The only point (X, Y, Z) on the curve above with $Z = 0$ is $[0 : 1 : 0] \in \mathbb{P}^2$. Therefore, we often homogenize the curve to

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

remembering that there is one additional point outside this affine representation.

To a Weierstrass curve, we can associate a discriminant $\Delta \in K$ which indicates whether the curve is smooth or not.

Definition 3.5 ([Sil09, §III.1])**.** Let C be the curve defined by (1) over some field K. The *discriminant* of C is

$$\Delta(C) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where the b_i are defined by[3]

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6,$$
$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

[3]In some additions of Silverman's book, there is a typo in the definition of b_2.

Example 3.6. One often considers short Weierstrass equations:

$$y^2 = x^3 + ax + b.$$

The discriminant of such a curve is $\Delta = -16(4A^3 + 27B^2)$.

Actually, when the characteristic of K does not equal 2 or 3, any Weierstrass curve is isomorphic to a Weierstrass curve of this form with $a, b \in K$ and so this is one of the most important examples of a Weierstrass equation.

Example 3.7. Another important type of Weierstrass equations for us, is

$$y^2 + xy = x^3 - a.$$

The discriminant of such a curve is $\Delta = a + 16 \cdot 27a^2$.

As we have said, the discriminant indicates the smoothness of a Weierstrass curve. Furthermore, every elliptic curve is given by a (smooth) Weierstrass curve.

Lemma 3.8 ([Sil09, III.1.4])**.** *The curve C over K of a Weierstrass equation is smooth if and only if $\Delta(C) \in K^*$.*

Proposition 3.9 ([Sil09, III.3.1])**.** *Let (E, O) be an elliptic curve defined over K. Then there exists a curve C given by an equation of the form (1) so that E is isomorphic to C and O is mapped to $[0 : 1 : 0]$ by this isomorphism.*

If C' is another such curve, then C and C' are related by a change of variables

$$(X, Y) = (u^2X' + r, u^3Y' + su^2X' + t),$$

for some $u \in K^*$ and $r, s, t \in K$.

Corollary 3.10. *If E and E' are elliptic curves over a field K given by Weierstrass equations with discriminants Δ and Δ' respectively and $E \cong E'$, then there exists some $u \in K^*$ such that $\Delta = u^{12}\Delta'$. In other words, the discriminant of an elliptic curve defines an operation*

$$\Delta\colon \mathbf{Ell}_K \to K^*/(K^*)^{12},$$

where $\mathbf{Ell}_K$ denotes the isomorphism classes of elliptic curves over K.

3.1 Reduction of elliptic curves

If R is a principal ideal domain and K its field of fractions, any elliptic curve over K can be written in Weierstrass form (1) with $a_i \in R$. For any maximal ideal $\mathfrak{p}$ in R, we can consider the associated Weierstrass equation over $R/\mathfrak{p}$, where we reduce all the a_i modulo $\mathfrak{p}$. If the resulting equation still gives an elliptic curve, we say that it has *good reduction* modulo $\mathfrak{p}$.

Having good reduction depends on the choice of Weierstrass equation. Using a change of coordinates as in Proposition 3.9 we can map a curve of good reduction to a curve with bad reduction.

Example 3.11. Let $K = \mathbb{Q}_3$ and consider the elliptic curve given by

$$E\colon y^2 = x^3 + x.$$

This curve has good reduction as can be seen by looking at the discriminant $\Delta = -64 \in \mathbb{Z}_3$. It is also isomorphic to the curve

$$E'\colon v^2 = u^3 + 81u,$$

via the change of coordinates $(u, v) = (9x, 27y)$. This curve has discriminant $\Delta' = -64 \cdot 3^{12}$, which means it does not have good reduction.

A way to remove this ambiguity, is to agree on the type of curves we use the reduction step on. In the case where R is the ring of integers of a local field K, we can consider so-called minimal Weierstrass equations.

Definition 3.12. Let E be an elliptic curve over a local field K. A Weierstrass equation as in (1) for E is called *minimal* when the coefficients a_i are in $\mathcal{O}_K$ and the valuation of the discriminant $v_K(\Delta)$ is minimized with respect to this condition.

Remark 3.13. Let E be an elliptic curve. By Corollary 3.10, any Weierstrass equation for E with $a_i \in \mathcal{O}_K$ and $v_K(\Delta) < 12$ is minimal.

Also, if there exists a minimal Weierstrass equation for E with good reduction, then any other Weierstrass equation either has good reduction or is not minimal, depending on the valuation of $u \in K^*$ in Corollary 3.10.

Definition 3.14. Let K be a local field and $\mathcal{O}_K$ its ring of integers. An elliptic curve E over K is said to be *defined over* $\mathcal{O}_K$ if there is a minimal Weierstrass equation that has good reduction over $\mathfrak{p}_K$.

Remark 3.15. In general, the same definitions make sense when we replace $\mathcal{O}_K$ by an arbitrary discrete valuation domain R and K its field of fractions.

Remark 3.16. We have already mentioned that there is a general notion of an elliptic curve over a scheme. For this, one considers (minimal Weierstrass) models of elliptic curves. See [Liu02, §10] for more details.

4 Brauer groups

Now that we have dealt with the most important properties of local fields and elliptic curves, it is time to introduce the other major concept of this thesis, the Brauer group. As we have mentioned in the introduction, the Brauer group of a field K was originally introduced as a way to classify central division algebras over K, i.e. division algebras with centre K. By Wedderburn's Theorem it can also be used as a way to classify central simple

algebras. This is the approach that we will take. We will recall the definition of central simple algebras and state Wedderburn's Theorem. Then we consider the most important class of central simple algebras, the cyclic algebras. After this, we will define the Brauer group. In the next chapter, we will discuss how this group can be described by cohomology, which matches with most modern day definitions of the Brauer group. Proofs and more details can be found in [GS06, Ch.2].

Definition 4.1. Let K be a field. A central simple algebra over K is an algebra A over K satisfying the following two properties:

- The centre $Z(A)$ is equal to K.
- The only non-zero two-sided ideal of A is A.

Example 4.2. Any division algebra D is a central simple algebra over its centre $Z(D)$. One can also check that the matrix ring $M_n(K)$ is a central simple algebra over K for $n \geq 1$ (see [GS06, p.18]).

Wedderburn's Theorem shows that central simple algebras and central division algebras are interchangeable.

Theorem 4.3 ([GS06, 2.1.3])**.** *Let A be a finite dimensional central simple algebra over a field K. Then there exists an integer $n \geq 1$ and a division algebra $D \supset K$, unique up to isomorphism, so that $A \cong M_n(D)$.*

More importantly for us, we can use base changes to show that any central simple algebra can be moved to a matrix ring.

Theorem 4.4 ([GS06, 2.2.1])**.** *Let A be a finite dimensional K-algebra. Then A is central and simple if and only if there exists an integer $n \geq 1$ and a finite extension L/K such that $A \otimes_K L \cong M_n(L)$.*

Definition 4.5. The field L in the theorem above is called a *splitting field*. We also say that A is *split* by L.

Remark 4.6. The splitting field of a central simple algebra is not unique. In fact, a theorem by Noether and Köthe shows that among all the splitting fields, we can always pick a Galois extension of K ([GS06, 2.2.6]).

4.1 Cyclic algebras

We have already given some of the more trivial examples of central simple algebras. We will now devote some time to the introduction of cyclic algebras. These are one of the most prominent examples of central simple algebras.

Definition 4.7. Let L/K be a cyclic Galois extension of degree m, pick $b \in K^*$ and $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/m\mathbb{Z}$ a choice of isomorphism. If $\chi(\sigma) = \bar{1}$, the algebra

$$(\chi, b) := L\langle y\rangle/(y^m = b, \text{ and } xy = y\sigma(x)\ \forall x \in L),$$

is called a *cyclic algebra*.

Remark 4.8. Note that $(\chi, b) \cong (\chi, bc^m)$ by sending y to y'/c, where y and y' are the generators of (χ, b) and (χ, bc^m) respectively.

The pair (L, χ) in Definition 4.7 above can be seen as a surjective homomorphism

$$\chi\colon \mathrm{Gal}(K_s/K) \to \mathbb{Z}/m\mathbb{Z},$$

where K_s is the separable closure of K inside a fixed algebraic closure $\bar{K}$. The field L can be recovered as

$$L_\chi := \{a \in K_s \mid \sigma(a) = a\ \forall \sigma \in \ker(\chi)\}.$$

Clearly $\mathrm{Gal}(K_s/L_\chi) = \ker(\chi)$ and so $\mathrm{Gal}(L_\chi/K) = \mathrm{Im}(\chi) = \mathbb{Z}/m\mathbb{Z}$. We conclude that

$$\chi \mapsto (L_\chi, \chi|_{\mathrm{Gal}(L_\chi/K)}),$$

defines a bijection between $\hom(\mathrm{Gal}(K_s/K), \mathbb{Z}/m\mathbb{Z})$ and the set of pairs (L, χ) of Galois extensions L/K and injective homomorphisms $\mathrm{Gal}(L/K) \xrightarrow{\chi} \mathbb{Z}/m\mathbb{Z}$. Elements of $\hom(\mathrm{Gal}(K_s/K), \mathbb{Z}/m\mathbb{Z})$ are called (cyclic) *characters*. In the case that L_χ/K is an unramified extension of local fields, we call χ an *unramified character*.

If K contains a primitive m-th root of unity ζ_m and $\mu_m = \langle\zeta_m\rangle$ is the group of m-th roots of unity in K, we have the following map

$$K^* \to \hom(\mathrm{Gal}(K_s/K), \mu_m),\ a \mapsto (\sigma \mapsto \sigma(\alpha)/\alpha),$$

where α is any m-th root of a.

Proposition 4.9 ([GS06, 4.3.6])**.** *The map above is a surjective homomorphism with kernel* $(K^*)^m$ *and so* $\hom(\mathrm{Gal}(K_s/K), \mu_m) \cong K^*/(K^*)^m$.

This result is also known as Kummer Theory. It shows that for any field K containing a primitive m-th root of unity, its cyclic characters of degree m are parametrized by $K^*/(K^*)^m$. Any cyclic Galois extension L/K of degree m can be written as $K(\sqrt[m]{a})$ for some $a \in K^*$ and $K(\sqrt[m]{a}) = K(\sqrt[m]{b})$ if and only if $a = bx^m$ for some $x \in K^*$.

Example 4.10. If m is an odd prime and $K(\beta)/K$ is a cyclic Galois extension of degree m, we can always recover a such that $K(\beta) = K(\sqrt[m]{a})$ using the following steps. First, we set

$$\alpha = \sum_{j=0}^{m-1} \zeta_m^j \sigma^j(\beta),$$

where σ is a generator of $\mathrm{Gal}(K(\beta)/K)$. Note that $\sigma(\alpha) = \zeta_m^{-1}\alpha$ and so $K(\alpha) = K(\beta)$. Moreover, we have

$$N_{K(\beta)/K}(\alpha) = \prod_{j=0}^{m-1} \sigma^j(\alpha) = \prod_{j=0}^{m-1} \zeta_m^{-j}\alpha = \alpha^m.$$

And so we set $a := N_{K(\beta)/K}(\alpha) \in K^*$.

If we assume that $\zeta_m \in K$, we use Kummer theory to write any degree m cyclic Galois extension L/K as $L = K(\sqrt[m]{a})$ for $a \in K^*$. If $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/m\mathbb{Z}$ sends the map $\sqrt[m]{a} \mapsto \zeta_m \sqrt[m]{a}$ to $\bar{1}$, the cyclic algebra (χ, b) also has the following presentation:

$$(a, b)_{\zeta_m} := K\langle x, y\rangle/(x^m = a,\ y^m = b,\ xy = \zeta_m yx).$$

Remark 4.11. By the same argument as in Remark 4.8, we have that $(ac^m, b)_{\zeta_m} \cong (a, b)_{\zeta_m}$. By reversing x and y, we also get $(a, b)_{\zeta_m} \cong (b, a)_{\zeta_m^{-1}}$.

Example 4.12. Let $K = \mathbb{R}$, $m = 2$ and $a = b = -1$. The cyclic algebra $(-1, -1)_{-1}$ is the quaternion algebra

$$\mathbb{R}\langle i, j, k\rangle/(i^2 + 1,\ j^2 + 1,\ k^2 + 1,\ ijk + 1)$$

4.2 The Brauer group

We have defined central simple algebras and splitting fields and we looked at the important example of cyclic algebras. Now it is time to introduce the Brauer group. As mentioned before, the Brauer group will be a group that classifies central simple algebras over K. We also discussed the most trivial central simple algebras, the matrix algebras $M_n(K)$. This triviality is expressed by the following definition.

Definition 4.13. Let K be a field and let A and B be central simple K-algebras. We call A and B *Brauer equivalent* if there exist integers $n, m \geq 1$ such that $A \otimes_K M_n(K) \cong B \otimes_K M_m(K)$.

In other words, two central simple algebras are equivalent if they differ only by a (trivial) matrix algebra. To check that the definition above defines an equivalence relation, one only has to verify that

$$M_n(K) \otimes_K M_m(K) \cong M_{nm}(K).$$

Lemma 4.14 ([Mil13, IV.2.14],[GS06, 2.4.8])**.** *The equivalence classes form a set and the tensor product defines a group action on this set:*

$$[A][B] := [A \otimes_K B]$$

Remark 4.15. The neutral element of this group is of course $[K] = [M_n(K)]$. The inverse of $[A]$ is $[A^{op}]$, where A^{op} is the algebra with the same underlying set as A, but reverse multiplication, i.e. the multiplication $*$ on A^{op} is given by $a * b := ba$.

Definition 4.16. The resulting group is called the *Brauer group* of K and is denoted by $\mathrm{Br}(K)$.

Remark 4.17. Wedderburn's Theorem (Theorem 4.3) shows that each class in $\mathrm{Br}(K)$ is represented by a unique central division algebra (up to isomorphism). So $\mathrm{Br}(K)$ is also a way to classify central division algebras.

We have seen in Theorem 4.4 that every central simple K-algebra is split by some finite extension L/K. The elements of $\mathrm{Br}(K)$ that can be represented by an algebra split by L form a subgroup $\mathrm{Br}(L/K)$ of $\mathrm{Br}(K)$. These subgroups are called the *relative Brauer groups*. By Remark 4.6 we have

$$\mathrm{Br}(K) = \bigcup_{L/K} \mathrm{Br}(L/K),$$

where we take the union over all the Galois extensions L/K.

We are now in a position to understand the main construction we are concerned with. Consider any local field K and an elliptic curve E over K. To such a curve, we can associate a discriminant $\Delta(E) \in K^*$ that is uniquely defined modulo $(K^*)^{12}$. We consider the image of the cyclic algebra $(\chi, \Delta(E))$ in $\mathrm{Br}(K)$ for some $\chi \in \hom(\mathrm{Gal}(K_s/K), \mathbb{Z}/12\mathbb{Z})$.[4] A natural question to ask is which elements of $\mathrm{Br}(K)$ we can reach by only considering cyclic algebras of this form. A follow-up question is what happens when we restrict to elliptic curves over $\mathcal{O}_K$ rather than K. To answer these questions, we need some more tools.

5 Using cohomology

One of the main tools for studying Brauer groups is cohomology. The theory of cohomology is used extensively in modern day mathematics and translating any mathematical problem to one in cohomology, allows us to make use of many general statements that are sometimes hard to prove otherwise. We will give a short introduction on the main cohomological tools necessary for this thesis. Then, we shall identify some important groups we already looked at as cohomology groups. We close of with an illustration of how this theory can be used to explicitly describe the Brauer group of any local field.

Let us start with the definition of cohomology we will use.

[4] To assure that this cyclic algebra is well-defined, we can only consider cyclic extensions of degree dividing 12 because Δ is only defined up to 12-th powers.

Definition 5.1. Let G be a group and M a left $\mathbb{Z}[G]$-module. Consider a projective resolution of $\mathbb{Z}[G]$-modules

$$\cdots \xrightarrow{p_2} P_1 \xrightarrow{p_1} P_0 \to \mathbb{Z} \to 0.$$

This gives us the following sequence of $\mathbb{Z}[G]$-modules:

$$\hom(P_0, M) \xrightarrow{d_0} \hom(P_1, M) \xrightarrow{d_1} \hom(P_2, M) \xrightarrow{d_2} \cdots,$$

where $d_i(f) = f \circ p_{i+1}$. We now define $H^i(G, M) = \ker(d_i)/\operatorname{Im}(d_{i-1})$.

Remark 5.2. It is a routine check to verify that this definition does not depend on the choice of projective resolution $P_\bullet$ and satisfies the usual properties of cohomology, such as the long exact sequence ([GS06, Prop. 3.1.9]): given an exact sequence of $\mathbb{Z}[G]$-modules

$$0 \to A \to B \to C \to 0,$$

there exists a long exact sequence of abelian groups

$$\begin{aligned} 0 \to &H^0(G, A) \to H^0(G, B) \to H^0(G, C) \xrightarrow{\partial_0} H^1(G, A) \to \cdots \\ &\cdots \to H^i(G, A) \to H^i(G, B) \to H^i(G, C) \xrightarrow{\partial_i} H^{i+1}(G, A) \to \cdots \end{aligned}$$

The maps ∂_i are called the *connecting homomorphisms*.

Besides these connecting homomorphisms we usually use a few other maps between cohomology groups such as the restriction and corestriction maps.

Proposition 5.3 ([GS06, 3.3.7])**.** *Let G be a group, H a subgroup and A any $\mathbb{Z}[G]$-module. For any $i \geq 0$, there exist two natural morphisms*

$$\begin{aligned} \operatorname{res}\colon H^i(G, M) &\to H^i(H, M), \\ \operatorname{cor}\colon H^i(H, M) &\to H^i(G, M). \end{aligned}$$

Moreover, if the index $[G : H]$ is finite, their composite

$$\operatorname{cor} \circ \operatorname{res}\colon H^i(G, M) \to H^i(G, M),$$

is given by multiplication by $[G : H]$.

Corollary 5.4. *If G is a finite group of order n, A is any $\mathbb{Z}[G]$-module and $i > 0$ is an integer, the elements of $H^i(G, A)$ have order dividing n.*

Proof. Consider the subgroup $H = \{1\}$. By the proposition any element $x \in H^i(G, A)$ is mapped by $\operatorname{cor} \circ \operatorname{res}$ to nx. However, the image of res is $H^i(\{1\}, M) = \{0\}$ and so $nx = 0$. □

Another map that is important to us, is the cup-product map. Similar to the connecting homomorphism, we can use this map to describe elements of higher cohomology groups in terms of lower cohomology groups.

Proposition 5.5 ([GS06, 3.4.5])**.** *Let G be a group and let A and B be $\mathbb{Z}[G]$-modules. For any integers $i, j \geq 0$, there exists a group homomorphism, called the* cup-product map

$$H^i(G, A) \times H^i(G, B) \to H^{i+j}(G, A \otimes_{\mathbb{Z}} B),\ (a, b) \mapsto a \cup b.$$

Remark 5.6. The cup-product satisfies many properties that make it nice to work with (see [GS06, §3.4]). Instead of stating them one by one, we will state the one result we will make use of in the next section (see Proposition 5.14).

Let us finish with one example that shows how we can use an explicit projective resolution to describe cohomology groups.

Example 5.7 (inhomogeneous cochains)**.** Let G be a group and for each $i \geq 0$ consider the $\mathbb{Z}[G]$-module $\mathbb{Z}[G^{i+1}]$. For each $0 \leq j \leq i$ we define the map

$$s_{i,j} \colon \mathbb{Z}[G^{i+1}] \mapsto \mathbb{Z}[G^i],\ (\sigma_0, \ldots, \sigma_i) \mapsto (\sigma_0, \ldots, \sigma_{j-1}, \sigma_{j+1}, \ldots, \sigma_i).$$

The maps $p_i = \sum_{j=0}^{i} s_{i,j}$ give the projective resolution

$$\cdots \xrightarrow{p_3} \mathbb{Z}[G^3] \xrightarrow{p_2} \mathbb{Z}[G^2] \xrightarrow{p_1} \mathbb{Z}[G] \xrightarrow{p_0} \mathbb{Z} \to 0.$$

We can consider the non-standard basis of $\mathbb{Z}[G^{i+1}]$ given by elements of the form

$$[\sigma_1, \ldots \sigma_i] := (1, \sigma_1, \sigma_1\sigma_2, \ldots, \prod_{j=1}^{i} \sigma_j).$$

The maps p_i act on these elements as

$$\begin{aligned} p_i([\sigma_1, \ldots \sigma_i]) =& \sigma_1[\sigma_2, \ldots, \sigma_i] + \sum_{j=1}^{i} (-1)^j [\sigma_1, \ldots, \sigma_j\sigma_{j+1}, \ldots, \sigma_i] \\ &+ (-1)^{i+1}[\sigma_1, \ldots, \sigma_{i-1}]. \end{aligned}$$

Let A be a $\mathbb{Z}[G]$-module. Elements of $\hom(\mathbb{Z}[G^{i+1}], A)$ are of the form $[\sigma_1, \ldots, \sigma_i] \mapsto a_{\sigma_1,\ldots,\sigma_i}$ and the maps d_i between these homomorphism groups are given by

$$a_{\sigma_1,\ldots,\sigma_i} \mapsto \sigma_1 a_{\sigma_2,\ldots,\sigma_i} + \sum_{j=1}^{i} (-1)^j a_{\sigma_1,\ldots,\sigma_j\sigma_{j+1},\ldots,\sigma_1} + (-1)^{i+1} a_{\sigma_1,\ldots,\sigma_{i-1}}.$$

In particular, an element of $\ker(d_1)$ is a map $\sigma \mapsto a_\sigma$ satisfying the equality $a_{\sigma_1\sigma_2} = \sigma_1 a_{\sigma_2} + a_{\sigma_1}$. It is in $\mathrm{Im}(d_0)$ precisely when $a_\sigma = \sigma(x) - x$ for some $x \in A$. In particular, when G acts trivially on A, being in $\ker(d_1)$ is equivalent to $\sigma \mapsto a_\sigma$ being a group homomorphism. Furthermore, the image of d_0 is clearly trivial. We conclude that in this case $H^1(G, A) = \hom(G, A)$.

5.1 Cohomological identifications

We have now discussed some important properties of cohomology groups. In order to use this theory, we need to show that the groups we have so far looked at, appear as cohomology groups.

First, we have to note that in general one does not use Definition 5.1 to describe cohomology of profinite groups such as the Galois group of an infinite field extension. For this, we need continuous cohomology. Additional details can be found in [GS06, §4.2].

Definition 5.8. When G is a profinite group and A a continuous $\mathbb{Z}[G]$-module, we define the continuous cohomology groups $H^i_c(G, A)$ as the direct limit of $H^i(G_\alpha, A)$ with inflation maps.

Remark 5.9. For finite groups, the continuous cohomolgy groups and the cohomology groups defined in Definition 5.1 agree, i.e. $H^i(G, A) = H^i_c(G, A)$ for all i and A. In general the definitions do not agree. For the remainder of this thesis, we will only talk about continuous cohomology and whenever we use the notation $H^i(G, A)$, we mean continuous cohomology.

For any field K and group A, we can view A as a $\mathbb{Z}[\mathrm{Gal}(K_s/K)]$-module by using the trivial action on A.[5] We write $H^i(K, A)$ for the corresponding cohomology group $H^i(\mathrm{Gal}(K_s/K), A)$ and $H^i(L/K, A)$ for $H^i(\mathrm{Gal}(L/K), A)$. Such cohomology groups are sometimes called *Galois cohomology groups*. Example 5.7 shows that

$$H^1(K, A) \cong \varinjlim_{L/K} \hom(\mathrm{Gal}(L/K), A).$$

We have already seen in Section 4.1 that this group describes the pairs (L, χ), where L/K is a Galois extension with Galois group equal to a subgroup B of A and $\chi\colon \mathrm{Gal}(L/K) \to B$ a choice of isomorphism.

The Brauer group also appears as a cohomology group.

Theorem 5.10 ([Mil13, IV.3.13])**.** *Let L/K be any field extension. The relative Brauer group $\mathrm{Br}(L/K)$ is isomorphic to $H^2(L/K, L^*)$. For the absolute Brauer group we have $\mathrm{Br}(K) \cong H^2(K, K_s^*)$.*

Remark 5.11. Milne actually gives very explicit constructions for defining two inverse isomorphisms. The construction in [GS06] is very different and uses an intermediate identification $\mathrm{Br}(K) \cong H^1(G, \mathrm{PGL}_\infty)$ and a long exact sequence.

Corollary 5.12. *By Corollary 5.4, the group $\mathrm{Br}(L/K)$ is killed by the degree $[L : K]$ for any finite Galois extension L/K. This also shows that $\mathrm{Br}(K) = \bigcup_{L/K} \mathrm{Br}(L/K)$ is a torsion group.*

[5] Here K_s denotes the separable closure of K.

The theorem allows us to explicitly compute Brauer groups by choosing a projective resolution. We illustrate this by looking at cyclic Galois extensions.

Let G be a cyclic group of degree m generated by σ. Consider the operations $N = \sum_{i=0}^{m-1} \sigma^i$ and $\sigma - 1$ on any $\mathbb{Z}[G]$-module. These define the explicit projective resolution

$$\cdots \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\sigma-1} \mathbb{Z}[G] \xrightarrow{\sigma\mapsto 1} \mathbb{Z} \to 0.$$

This yields $H^2(G, M) = M^G/NM$. In particular, if L/K is a cyclic Galois field extension and $G = \mathrm{Gal}(L/K)$, we get

$$\mathrm{Br}(L/K) \cong H^2(G, L^*) = K^*/N_{L/K}(L^*). \tag{2}$$

Example 5.13. Let $K = \mathbb{R}$ be the field of real numbers. Its algebraic closure is given by the extension $\mathbb{C}/\mathbb{R}$. The corresponding Galois group is $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, where G acts on $\mathbb{C}^*$ by complex conjugation. We get

$$\mathrm{Br}(\mathbb{R}) \cong H^2(\mathbb{R}, \mathbb{C}^*) = (\mathbb{C}^*)^G/N(\mathbb{C}^*) = \mathbb{R}/\mathbb{R}_{>0} \cong \mathbb{Z}/2\mathbb{Z}.$$

The classes are given by the trivial class and the class of the quaternions: $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$.

Note that for each $\chi \in H^1(K, \mathbb{Z}/12\mathbb{Z})$ and $\Delta \in K^*$, the cyclic algebra (χ, Δ) induces an element of $\mathrm{Br}(L_\chi/K)$, which is in the 12-torsion subgroup of $\mathrm{Br}(K)$. In other words, this gives us the map

$$[(-, \Delta)] \colon H^1(K, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{Br}(K)[12],\ \chi \mapsto [(\chi, \Delta)]. \tag{3}$$

To deduce the image of this map, we will first prove that it is a group homomorphism. This way, we may consider the 2- and 3-primary part separately.

Let K be a field and consider the exact sequence

$$0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0.$$

This gives us the coboundary map $\partial \colon H^1(K, \mathbb{Z}/m\mathbb{Z}) \to H^2(K, \mathbb{Z})$ by the long exact sequence. Note that

$$K^* = (K_s^*)^{\mathrm{Gal}(K_s/K)} = H^0(K, K_s^*).$$

Consider the following sequence of group morphisms

$$H^1(K, \mathbb{Z}/m\mathbb{Z}) \times H^0(K, K_s^*) \to H^2(K, \mathbb{Z} \otimes K_s^*) = H^2(K, K_s^*) \xrightarrow{\sim} \mathrm{Br}(K),$$

where the first map sends a pair (χ, b) to $\partial(\chi) \cup b$, for any $b \in K^*$.

Proposition 5.14 ([GS06, 4.7.3])**.** *Consider the setup above. The image of the pair (χ, b) in $\mathrm{Br}(K)$ is the class represented by the cyclic algebra $[(\chi, b)]$.*

Remark 5.15. The isomorphism (2) can be induced by the map $b \mapsto [(\chi, b)]$ (see [GS06, 4.7.4]). Hence the cyclic algebra (χ, b) is trivial if and only if b is a norm of the extension L_χ/K. This also shows that cyclic algebras play a very special role in studying relative Brauer groups of cyclic extensions.

We now see that the map (3) is induced by the cup-product, so it is a group morphism. Using this fact, we can show that it is surjective onto $\mathrm{Br}(K)[12]$ if and only if it is surjective onto both $\mathrm{Br}(K)[3]$ and $\mathrm{Br}(K)[4]$. To do this, we need to know what $\mathrm{Br}(K)$ looks like when K is a local field.

5.2 The Brauer group of a local field

Until now, we only looked at the cohomology of Brauer groups associated to a general field K. In this thesis, we are only considering local fields. For these, it has been shown that the Brauer group is isomorphic to $\mathbb{Q}/\mathbb{Z}$, regardless of the local field. We will sketch the building blocks that go into proving this. Details can be found in [Mil13, §III.2].

Let L/K be a finite unramified extension of local fields. Consider the short exact sequence

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

By Corollary 5.4, $H^i(L/K, \mathbb{Q})$ is torsion, but because it is a $\mathbb{Q}$-module, it must be 0. The long exact sequence gives us an isomorphism

$$H^1(L/K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\partial} H^2(L/K, \mathbb{Z}).$$

Since we are dealing with an extension of local fields, we also have the short exact sequence

$$0 \to \mathcal{O}_L^* \to L^* \xrightarrow{v_L} \mathbb{Z} \to 0,$$

which is split by Proposition 2.13. We can use this to write $H^i(L/K, \mathcal{O}_L^*)$ as a direct summand of $H^i(L/K, L^*)$. Hilbert's theorem 90 shows that $H^1(L/K, L^*) = 0$ and so $H^1(L/K, \mathcal{O}_L^*)$ is trivial too. One can make use of the fact that the norm is surjective onto the units (see Example 2.32) to deduce that $H^0(L/K, \mathcal{O}_L^*) = 0$ as well. Using this, the long exact sequence associated to the short exact sequence above gives an isomorphism

$$H^1(L/K, L^*) \xrightarrow{\sim} H^1(L/K, \mathbb{Z}).$$

Using the discussion above we get the invariant map $\mathrm{inv}_{L/K}$:

$$\begin{aligned}\mathrm{Br}(L/K) \cong H^2(L/K, L^*) &\xrightarrow{\sim} H^2(L/K, \mathbb{Z}) \\ &\xrightarrow{\partial^{-1}} H^1(L/K, \mathbb{Q}/\mathbb{Z}) = \hom(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \xrightarrow{f \mapsto f(\mathrm{Frob}_{L/K})} \mathbb{Q}/\mathbb{Z}.\end{aligned}$$

Remark 5.16 ([Mil13, p. 82])**.** The construction above works also for infinite unramified extensions and gives a canonical isomorphism

$$\mathrm{inv}_K \colon \mathrm{Br}(K_{un}/K) \to \mathbb{Q}/\mathbb{Z},$$

where K_{un} is the maximal unramified extension. For each finite unramified extension L/K, this invariant map induces an isomorphism

$$\mathrm{Br}(L/K) \xrightarrow{\sim} [L:K]^{-1}\mathbb{Z}/\mathbb{Z}.$$

Until now, we have only looked at the relative Brauer groups of unramified extensions while ignoring all the ramified extensions. It turns out that the unramified extensions are the only ones we need in this case, since every element of $\mathrm{Br}(K)$ can be split by an unramified extension (see [Mil13, p. 109] or [CF10, VI.1.1.1]).

Corollary 5.17. *For every local field K, we have*

$$\mathrm{Br}(K) = \mathrm{Br}(K_{un}/K) \cong \mathbb{Q}/\mathbb{Z}.$$

Finally, we can return to the main question of this thesis. We now know that $\mathrm{Br}(K)[12] \cong \mathbb{Z}/12\mathbb{Z}$ and that for any $\Delta \in K^*$, the map

$$[(-,\Delta)] \colon H^1(K, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{Br}(K)[12] \cong \mathbb{Z}/12\mathbb{Z},\ \chi \mapsto [(\chi,\Delta)],$$

is a group homomorphism. Therefore, if we can find an elliptic curve E over K (or $\mathcal{O}_K$) and $\chi_1, \chi_2 \in H^1(K, \mathbb{Z}/12\mathbb{Z})$ so that $(\chi_1, \Delta(E))$ and $(\chi_2, \Delta(E))$ induce elements of $\mathrm{Br}(K)$ of orders 3 and 4 respectively, we can deduce that the map is surjective. This will be our method in the chapters to come.

We still need to be able to compute the order of a given cyclic algebra. For this, we will introduce our final tool in this thesis, the Hilbert symbol.

6 Hilbert symbols

To compute the order of a cyclic algebra, one can use the so-called Hilbert symbol. This symbol can be defined using both Kummer theory (Proposition 4.9) and local class field theory (Theorem 2.28). We will state some basic properties that we will use later in this thesis. A discussion on the most important formulas to compute Hilbert symbols is also included, although for our main purpose we will only need one. Finally, we will argue why we may use Kummer theory in the first place.

Neukirch uses a more general version of Kummer theory together with class field theory to define Hilbert symbols. We will define them using the Artin map of Theorem 2.28. Let μ_m denote the group of roots of unity of order dividing m in K.

Definition 6.1. Let K be a local field containing a primitive m-th root of unity. For any $a, b \in K^*$ the Hilbert symbol $(a,b)_m$ is equal to

$$(a,b)_m := \frac{\phi_{K(\sqrt[m]{b})/K}(a)(\sqrt[m]{b})}{\sqrt[m]{b}} \in \mu_m,$$

where $\phi_{K(\sqrt[m]{b})}$ is defined as in Theorem 2.28 and $\sqrt[m]{b}$ is any choice of root of $X^m - b$ in the algebraic closure of K.

Remark 6.2. Although Neukirch defines the Hilbert symbol slightly differently, he proves that this definition is equivalent ([Neu99, V.3.1]). He uses the notation $(\frac{a,b}{\mathfrak{p}})$ to denote a Hilbert symbol in a local field with prime ideal $\mathfrak{p}$. For us, the field K and maximal ideal $\mathfrak{p}$ are both clear from the context and instead we place emphasis on the degree m in our notation.

Hilbert symbols have the following key properties.

Lemma 6.3 ([Neu99, V.3.2])**.** *Let K be a local field containing a root of unity of order m. The Hilbert symbol has the following properties for any $a, b, x, y \in K^*$:*

- *bilinearity:* $(ax, by)_m = (a,b)_m(a,y)_m(x,b)_m(x,y)_m$.
- $(a,b)_m = 1$ *precisely when a is a norm of the extension $K(\sqrt[m]{b})$.*
- $(a,b)_m = (b,a)_m^{-1}$

Remark 6.4. Neukirch also shows some additional properties of the Hilbert symbol. These are, however, the only properties we will use for our computations.

Using these properties, we also see that the Hilbert symbol is a bilinear map

$$K^*/(K^*)^m \times K^*/(K^*)^m \to \mu_m.$$

Corollary 6.5. *If $m = 2$, the Hilbert symbol can be determined as follows: for $a, b \in K^*$, we have $(a,b)_2 = 1$ if and only if the equation*

$$ax^2 + by^2 = z^2$$

has no solution $(x,y,z) \in K^3 \setminus \{(0,0,0)\}$.

Proof. By the lemma we know that $(a,b)_2 = 1$ precisely when a is a norm of $K(\sqrt{b})$. This is the case when $a = Z^2 - bY^2$ for some $Y, Z \in K$ (not both zero). Multiplying by $x^2 \neq 0$ and setting $(y,z) = (Yx, Zx)$, gives us the desired equation. □

In some textbooks, the words cyclic algebra and Hilbert symbol are used interchangeably. Milne even states the following alternative definition of the Hilbert symbol without proving it is equivalent to the other definitions he uses:

$$(a,b)_m := \zeta_m^{n \operatorname{inv}_K([(a,b)_{\zeta_m}])}.$$

One argument why we do not distinguish between them is the following.

Corollary 6.6. *Let K be any local field containing a primitive m-th root of unity ζ_m. The order of the Hilbert symbol $(a,b)_m$ in μ_m is equal to the order of $[(a,b)_{\zeta_m}]$ in $\mathrm{Br}(K)$.*

Proof. Using the properties of the Hilbert symbol, Remark 5.15 and the fact that $[(-,b)]\colon K^*/(K^*)^m \to \mathrm{Br}(K)$ is a group homomorphism by Proposition 5.14 (and Kummer theory), we get

$$\begin{aligned}
(a,b)_m^n = 1 &\iff (b,a^n)_m = 1 \\
&\iff b \in N_{K(\sqrt[m]{a^n})/K}(K(\sqrt[m]{a^n})^*) \\
&\iff [(a^n,b)_{\zeta_m}] \text{ is trivial in } \mathrm{Br}(K) \\
&\iff [(a,b)_{\zeta_m}] \text{ has order dividing } n.
\end{aligned}$$

□

6.1 Formulas

The reason we translate the problem of finding the order of a cyclic algebra to computing a Hilbert symbol, is because there are formulas for the latter. We will state some of these formulas and discuss their application. Although not all formulas will be used to answer our main research question, they do allow explicit computations of Hilbert symbols and provide us with tools we can use for specific local fields. We will provide some examples in this section, as well as the next.

The formula that we will mainly use for computing the Hilbert symbol is also the one that is the easiest to use. Recall that for any local field K with residue field order $q = \#\kappa_K$, we can write any unit $u \in U_K$ as $u = \omega(u)\tilde{u}$ for $\tilde{u} \in U_K^{(1)}$ and $\omega(u) \in \mu_{q-1}$ such that $\omega(u) \equiv u \mod \mathfrak{p}_K$. Using this notation, we have the following formula for the Hilbert symbol.

Proposition 6.7 ([Neu99, V.3.4])**.** *Let K be a local field and set $q = \#\kappa_K$. Let $m \geq 1$ be an integer coprime to q. For $a, b \in K^*$, we have*

$$(a,b)_m = \omega\Big((-1)^{v_K(a)v_K(b)} \frac{b^{v_K(a)}}{a^{v_K(b)}}\Big)^{(q-1)/m}. \tag{4}$$

Note that this formula can only be used to compute Hilbert symbols for local fields over $\mathbb{Q}_p$ for p coprime to the degree m. Such a symbol is

also called a *tame* Hilbert symbol. Using this formula is relatively easy and for this reason we will mostly be interested in the case of the *wild* Hilbert symbol, where m is a power of p. Our question concerns extensions of degree 12 and therefore we will focus on local fields over $\mathbb{Q}_2$ and $\mathbb{Q}_3$, in which case Proposition 6.7 is not enough.

There are no formulas as nice as the one of Proposition 6.7 for the wild symbol. The most general formulas are given by Brückner (for p odd) and Henniart ($p = 2$). These are in general hard to use and we will not use them for explicit computations. The formulas can be found in [Neu99, V.3.7] and [Hen81, 7.5].

Another formula, that is more suited for explicit calculations is one by Artin and Hasse.

Proposition 6.8 ([AH28, p. 147])**.** *Let $K = \mathbb{Q}_p(\zeta_{p^n})$ for some p^n-th root of unity and let* Tr *be the trace of the extension. For any $a \equiv 1 \mod 1 - \zeta_{p^n}$, we have*

$$(\zeta_{p^n}, a)_{p^n} = ((-1)^{p+1}\zeta_{p^n})^{\mathrm{Tr}(\log(a))/p^n}.$$

Example 6.9. To see how this formula can be used for an explicit computation, we compute the Hilbert symbol $(2+i, i)_4$ in the local field $\mathbb{Q}_2(i)$. This example is inspired by [AM16, §8], where a similar Hilbert symbol is computed.

Since $(1+i)^2 = 2i$ and therefore $(1+i)^4 = -4$, we get the following formula for the trace of $(1+i)^j$:

$$\mathrm{Tr}((1+i)^{4k+\ell}) = \begin{cases} (-1)^k \cdot 2^{1+2k} & \text{for } \ell = 0, 1, \\ 0 & \text{for } \ell = 2, \\ (-1)^{k+1} \cdot 2^{2+2k} & \text{for } \ell = 3, \end{cases}$$

where we take $0 \leq \ell < 4$. This formula shows that $\mathrm{Tr}((1+i)^j)/j$ is divisible by 8 for $j > 8$. So modulo 8 we get

$$\begin{aligned} \mathrm{Tr}(\log(2+i)) = \mathrm{Tr}\Big(\sum_{j=1}^{\infty}(-1)^{j+1}\frac{(1+i)^j}{j}\Big) &\equiv \sum_{j=1}^{8}(-1)^{j+1}\frac{\mathrm{Tr}((1+i)^j)}{j} \\ &\equiv 2 - \frac{4}{3} + 2 - 4 \equiv -4 \mod 8. \end{aligned}$$

In other words, $\mathrm{Tr}(\log(2+i))/4$ is odd. Using Proposition 6.8 we compute

$$(i, 2+i)_4 = (-i)^{\mathrm{Tr}(\log(2+i))/4} = \pm i.$$

So the cyclic algebra $(i, 2+i)_i$ induces an element of order 4 in the Brauer group of $\mathbb{Q}_2(i)$.

An obvious downside to Proposition 6.8 is that we can only use this formula for fields of the given form and only when both arguments of the Hilbert symbol are of a specific form. A trade-off is achieved by Helou, who only computes Hilbert symbols for fields of the form $\mathbb{Q}_p(\zeta_p)$, but allows other elements as input into the Hilbert symbol.

Proposition 6.10 ([Hel02, Lemma 6])**.** *Let $u, v, x, y \in \mathbb{Z}_p$ be elements such that $p \nmid (u+v)(x+y)$. Let ζ_p be a p-th root of unity and set*

$$k = \frac{(uy - vx)^p - (u+v)y^p + v^p(x+y)}{p(u+v)(x+y)} \in \mathbb{Z}/p\mathbb{Z}.$$

For the p-th power Hilbert symbol in $\mathbb{Q}_p(\zeta_p)$ we have:

$$(u + v\zeta_p, x + y\zeta_p)_p = \zeta_p^k$$

6.2 Adding roots of unity

Both in writing a cyclic algebra (χ, b) as $(a, b)_{\zeta_m}$ and in defining the Hilbert symbol we need an m-th root of unity in K. In the literature this is often assumed without argument. Indeed, we would like to have a way to always reduce to the case where K includes the m-th roots of unity. The following argument is inspired by a small note by van der Kallen (see [Kal85, §3]).

To show the reduction step, we assume K does not contain a primitive m-th root of unity and let $\tilde{K} = K(\zeta_m)$. We consider the field extension $\tilde{K}/K$ of degree dividing $\varphi(m)$, where φ denotes the Euler totient function.[6]

Let L/K be a cyclic Galois extension of degree m and choose an isomorphism $\chi\colon \mathrm{Gal}(L/K) \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}$. We let $\tilde{K} = K(\zeta_m)$ as above and define $\tilde{L} := L(\zeta_m) = L \cdot \tilde{K}$. This induces an injective homomorphism

$$\tilde{\chi}\colon \mathrm{Gal}(\tilde{L}/\tilde{K}) \to \mathbb{Z}/m\mathbb{Z},\ \sigma \mapsto \chi(\sigma|_L). \tag{5}$$

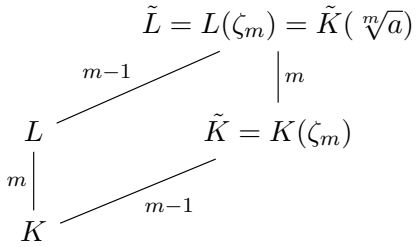
If m is prime, then $[\tilde{K} : K]$ divides $\varphi(m) = m-1$, and so it is coprime to m. In this case, we know that L does not contain any primitive m-th roots of unity because that would imply L/K has a subextension of degree dividing $m-1$. This means that $\tilde{L} = \bigoplus_{i=0}^{m-2} L\zeta_m^i$, so that to any $\sigma \in \mathrm{Gal}(L/K)$, we can associate $\tilde{\sigma}$:

$$\tilde{\sigma}\Big(\sum_{i=0}^{m-2} a_i\zeta_m^i\Big) = \sum_{i=0}^{m-2} \sigma(a_i)\zeta_m^i \quad \forall (a_i)_i \in L^{m-1}.$$

Note that $\tilde{\sigma}$ is an element of $\mathrm{Gal}(\tilde{L}/\tilde{K})$ such that $\tilde{\sigma}|_L = \sigma$, which means that $\tilde{\chi}$ is an isomorphism too. The following diagram gives a representation

[6] The degree is not always exactly $\varphi(m)$. Take for instance $m = 8$ and $K = \mathbb{Q}_3$: $\mathbb{Q}_3(\zeta_8)/\mathbb{Q}_3$ is the unramified degree 2 extension by Proposition 2.23.

of the field extensions we consider:



Since $\tilde{\chi}$ is an isomorphism, we can consider the cyclic algebra $(\tilde{\chi}, b)$ over $\tilde{K}$, which is isomorphic to $(\chi, b) \otimes \tilde{K}$. Kummer theory (Example 4.10) allows us to write this cyclic algebra as $(a, b)_{\zeta_m}$ for $a \in \tilde{K}$ such that $\tilde{L} = \tilde{K}(\sqrt[m]{a})$. We can compute the corresponding Hilbert symbol $(a, b)_m$ to see whether the algebra is trivial in $\mathrm{Br}(\tilde{K})$. If it is trivial, then $[(\chi, b)]$ is an $(m-1)$-torsion element in $\mathrm{Br}(K)$. Since it is an element of $\mathrm{Br}(L/K)$, it is also killed by m, so it must itself be trivial. We conclude that $(a, b)_m \in \mu_m$ has order n if and only if $[(\chi, b)] \in \mathrm{Br}(L/K)$ has order n.

Example 6.11. Let ζ_9 be a primitive 9-th root of unity and let $\zeta_3 = \zeta_9^3$. Consider the field extension $L = \mathbb{Q}_3(\zeta_9 + \zeta_9^{-1})$ over $K = \mathbb{Q}_3$ and fix an isomorphism $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/3\mathbb{Z}$. We want to find $b \in \mathbb{Q}_3$ such that the order of the cyclic algebra (χ, b) is 3.

Adjoining ζ_3 to both K and L yields

$$\tilde{L} = \mathbb{Q}_3(\zeta_9) = \mathbb{Q}_3(\sqrt[3]{\zeta_3}).$$

And so, using the same notation as in (5), the cyclic algebra becomes

$$(\chi, b) \otimes \tilde{K} = (\tilde{\chi}, b) = (\zeta_3, b)_{\zeta_3^j},$$

where $j \in \{1, 2\}$ is such that $\tilde{\chi}(\sqrt[3]{\zeta_3}) = \zeta_3^j \sqrt[3]{\zeta_3}$. The appropriate Hilbert symbol can be calculated using Proposition 6.10. We get $k = \frac{1-b^2}{3}$. Plugging in $b = 2$ gives $(\zeta_3, 2)_3 = \zeta_3^{-1}$. And so $[(\tilde{\chi}, 2)]$ has order 3 in $\mathrm{Br}(\mathbb{Q}_3(\zeta_3))$. By the main discussion of this section, we can conclude that $[(\chi, 2)]$ has order 3 in $\mathrm{Br}(\mathbb{Q}_3)$.

Instead of using Proposition 6.10, the final steps of this calculation can be done similarly to Example 6.9 (see [AM16, §8]). In both cases one uses the extension $\tilde{L}/\tilde{K}$.

Part II
Applying the theory

We have no dealt with all relevant theory for answering the three theorems we mentioned in the introduction. One by one, we will rephrase and specify them before providing a proof.

7 Elliptic curves over local fields

We have now dealt with all relevant theory for answering our main research question. In this section, we will prove Theorem 1.1. Let us rephrase the theorem using the notation we have discussed so far.

Theorem 7.1. *Let K be any local field. There exists an elliptic curve over K with discriminant $\Delta \in K^*$ such that the following map is surjective*

$$[(-,\Delta)]\colon H^1(K,\mathbb{Z}/12\mathbb{Z}) \to \mathrm{Br}(K)[12],\ \chi \mapsto [(\chi,\Delta)]. \tag{6}$$

By using Example 2.32, we will deduce conditions on Δ (depending on K) so that the map is surjective. For each local field K, we will give an explicit elliptic curve whose discriminant satisfies the given criterion. For local fields over $\mathbb{Q}_2$ we give an alternative proof which makes use of Proposition 7.3 and 6.7, as well as Section 6.2. This proof is harder to generalize to other local fields, but does allow for some observations that are easily overlooked when using the more general approach we start out with.

7.1 General approach

Let K be a local field with uniformizer π. As we have said, we will make use of Example 2.32 to deduce some sufficient conditions for (6) to be surjective.

Proposition 7.2. *Let $\Delta \in K^*$ such that $v_K(\Delta) \equiv \pm 1 \mod 6$. Then (6) is surjective.*

Proof. For the 3-primary part, we consider the unramified degree 3 extension K_3/K with a choice of isomorphism $\chi\colon \mathrm{Gal}(K_3/K) \to \mathbb{Z}/3\mathbb{Z}$. By Remark 5.15, the cyclic algebra (χ,Δ) induces a non-trivial element of $\mathrm{Br}(K)$ precisely when Δ is not a norm of the extension K_2/K. By Example 2.32 this is precisely when

$$\Delta \notin \pi^{3\mathbb{Z}} \times \mathcal{O}_K^*.$$

For $v_K(\Delta) \equiv \pm 1 \mod 6$ this is the case.

For the 2-primary part, we use a similar argument. If $\chi\colon \mathrm{Gal}(K_4/K) \to \mathbb{Z}/4\mathbb{Z}$ is a choice of isomorphism, the cyclic algebra (χ,Δ) is non-trivial when

Δ is not a norm of the extension K_4/K. In this case however, the cyclic algebra can still have order 2. In order to ensure that (χ, Δ) induces an element of order 4 in $\mathrm{Br}(K)$, we need that Δ is not a norm of the subextension K_2/K either. If $\chi'\colon \mathrm{Gal}(K_2/K) \to 2\mathbb{Z}/4\mathbb{Z}$ is an isomorphism, we have $2[(\chi, \Delta)] = [(\chi', \Delta)]$ in $\mathrm{Br}(K)$. By Example 2.32 again, we want that Δ is not in $\pi^{2\mathbb{Z}} \times \mathcal{O}_K^*$, which means $v_K(\Delta)$ must be odd. This is also ensured by picking $v_K(\Delta) \equiv \pm 1 \mod 6$.

We have shown that for $v_K(\Delta) \equiv \pm 1 \mod 6$, the map (6) is surjective on both the 2- and 3-primary part of $\mathrm{Br}(K)[12] \cong \mathbb{Z}/12\mathbb{Z}$ and so it must be a surjection. □

Using this proposition, we only need to find explicit elliptic curves over K whose discriminant Δ satisfies the condition of Proposition 7.2.

Proof of Theorem 7.1. Let $K/\mathbb{Q}_p$ be a local field with uniformizer π and ramification index $e = e(K/\mathbb{Q}_p) = v_K(p)$. Depending on p we consider different curves that have valuation equivalent to $\pm 1 \mod 6$ so that Proposition 7.2 ensures that we can reach $\mathrm{Br}(K)[12]$ entirely.

If $p = 2$, consider the elliptic curve

$$E\colon y^2 = x^3 + (3\pi - 3)x + 2.$$

Its discriminant is

$$\Delta(E) = -16(4(3\pi - 3)^3 + 27 \cdot 4) = 2^6 \cdot 3^3(\pi^3 - 3\pi^2 + 3\pi).$$

The valuation of $\Delta(E)$ is $6e + 1$.

If $p = 3$, we distinguish two cases. If e is odd, we take

$$E\colon y^2 = x^3 + 3\pi x + \pi.$$

Its discriminant has valuation $3e + 2 \equiv -1 \mod 6$:

$$\Delta(E) = -16(4 \cdot 27\pi^3 + 27\pi^2) = -2^4 \cdot 3^3\pi^2(1 + 4\pi).$$

If e is even, we consider the curve given by the Weierstrass equation

$$E\colon y^2 = x^3 + (3\pi - 3)x + 2\pi - 2.$$

Its discriminant has valuation equal to $3e + 1 \equiv 1 \mod 6$:

$$\Delta(E) = -16(4(3\pi - 3)^3 + 27 \cdot 4(1 - \pi)^2) = -2^6 \cdot 3^3 \cdot \pi(1 - \pi)^2.$$

If $p > 3$, we can also take this last elliptic curve. In this case, the valuation of the discriminant is equal to 1. □

7.2 Alternative approach to the 2-adic fields

In this section we consider local fields $K/\mathbb{Q}_2$ and use a different approach to find the condition $v_K(\Delta) \equiv \pm 1 \mod 6$ we found in Proposition 7.2. We will still deal with the 2- and 3-primary parts separately. For the 3-primary part, we will make use of Proposition 6.7. For dealing with the 2-primary part we use an explicit way to write the unramified extension of degree 4 in order to apply tools reminiscent of the study of Diophantine equations. This method allows for some quick observations that turn out to be useful later.

The 3-primary part Of course, we again consider the extenson K_3/K for the 3-primary part. In order to make use of the Hilbert symbol, we need that K contains a primitive third root of unity. Using the discussion of Section 6.2 we may move our study of the extension K_3/K to studying the extension $\tilde{K}_3/\tilde{K}$, where $\tilde{K} := K(\zeta_3)$.

Let $f = [\kappa_{\tilde{K}} : \mathbb{F}_2]$ be the residue field degree. Since we have $\zeta_3 \in \tilde{K}$, we know that f is even. By Proposition 2.13 $\tilde{K}$ contains a root of unity ζ of order $2^f - 1$. Since f is even, the order of ζ is divisible by 3. Any root of the polynomial $X^3 - \zeta$ must therefore have order $3(2^f - 1)$. Comparing this to the order of the residue field

$$\kappa_K = \mathbb{F}_2[\zeta] \cong \mathbb{F}_{2^f},$$

we see that κ_K does not contain a root of $X^3 - \zeta$. Therefore the extension $K(\sqrt[3]{\zeta})/K$ is unramified of degree 3.

We let $L = K(\sqrt[3]{\zeta})$ be the extension above and consider the isomorphism $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/3\mathbb{Z}$ sending $\sqrt[3]{\zeta} \mapsto \zeta_3\sqrt[3]{\zeta}$ to $\bar{1}$. For any choice of $\Delta \in K^*$, the cyclic algebra (χ, Δ) is isomorphic to $(\zeta, \Delta)_{\zeta_3}$. We can use Proposition 6.7 to compute the corresponding Hilbert symbol:

$$(\zeta, \Delta)_3 = \omega(\zeta^{-v_K(\Delta)})^{(2^f-1)/3} = (\zeta^{(2^f-1)/3})^{-v_K(\Delta)} = \zeta_3^{\pm v_K(\Delta)}.$$

For the last equality, we conclude that $\zeta^(2^f - 1)/3$ has order 3, hence equal to ζ_3 or ζ_3^{-1}. We conclude that the cyclic algebra (χ, Δ) induces an element of order 3 in $\mathrm{Br}(K)$ if and only if $v_K(\Delta) \not\equiv 0 \mod 3$.

The 2-primary part Similar to what we did above, we consider the unramified extension K_4/K of degree 4 with character χ and want to find conditions on Δ under which (χ, Δ) induces an element of order 4 in $\mathrm{Br}(K)$. As we did in Proposition 7.2, we can argue that (χ, Δ) has order 4 in $\mathrm{Br}(K)$ if and only if (χ', Δ) has order 2, where χ' is a character for K_2/K.

To translate the cyclic algebra (χ', Δ) to a Hilbert symbol, we need to write $K_2 = K(\sqrt{a})$ for some $a \in K$. For this, let $\zeta \in K$ be a root of unity of order $2^f - 1$, where $f = f(K/\mathbb{Q}_2)$ is the inertia degree of K. We claim

that $K_2 = K(\gamma)$, where γ is a root of $X^2 + X + \zeta$. To prove this, we show that $X^2 + X + \zeta$ is irreducible in the residue field $\mathbb{F}_2[\zeta]$ of K. Note that $\{\zeta^{2^i}\}_{0 \le i < f}$ forms a basis for $\mathbb{F}_2[\zeta]$ over $\mathbb{F}_2$ and since $\sum_{i=0}^{f-1} \zeta^{2^i}$ is invariant under the Frobenius morphism, this sum must be equal to 1 in $\mathbb{F}_2[\zeta]$. If $u \in \mathbb{F}_2[\zeta]$ is a root of $X^2 + X + \zeta$, then

$$1 \equiv \sum_{i=0}^{f-1} \zeta^{2^i} \equiv \sum_{i=0}^{f-1} u^{2^{i+1}} + u^{2^i} \equiv u^{2^f} + u \equiv 0 \mod 2.$$

This is a contradiction, so the polynomial is irreducible. We can write $K(\gamma) = K(\sqrt{1-4\zeta})$, because $(2\gamma+1)^2 = 1 - 4\zeta$. So the Hilbert symbol associated to the cyclic algebra (χ', Δ) is $(1 - 4\xi, \Delta)_2$.

It is not possible to use Proposition 6.7 to compute the Hilberts symbol in this case because the degree is not coprime to the order of the residue field. Since we are working over a general local field $K/\mathbb{Q}_2$ we cannot use Proposition 6.8 or 6.10 either. One thing we can consider in this case is Corollary 6.5.

Proposition 7.3. *Let $K/\mathbb{Q}_2$ be a local field with uniformizer π and inertia degree f. Let ζ be a root of unity of order $2^f - 1$ so that $\mathcal{O}_K = \mathbb{Z}_2[\pi, \zeta]$.*[7] *There are no non-trivial solutions $(x, y, z) \in K^3$ to the equation*

$$(1 - 4\zeta)x^2 + \pi y^2 = z^2. \tag{7}$$

Proof. If there is a non-trivial solution to the equation, we can use the fact that $\mathcal{O}_K$ is a discrete valuation ring to find a non-trivial solution $(x, y, z) \in \mathcal{O}_K^3$. Moreover, we may assume x, y and z are not all divisible by the same element of $\mathcal{O}_K$.

We claim that $y, z \pm x \in (2)$. We prove this by induction. We set $n = [K : \mathbb{Q}_2]/f$ so that $(\pi)^n = (2)$. Suppose $y \in (\pi)^k$ for some $k < n$. We write

$$\pi y^2 - 4\zeta x^2 = (z - x)(z + x).$$

Since the left hand side is in $(\pi)^{2k+1}$ and (π) is prime, we have that $z - x$ or $z + x$ is in $(\pi)^{k+1}$. Since $2x \in (2)$ too, both of $z \pm x \in (\pi)^{k+1}$. Using this, we deduce that $\pi y^2 \in (\pi)^{2k+2}$ and so $y \in (\pi)^{k+1}$. By induction we have thus proven that we can write $y = 2v$ and $z = x + 2w$ for some $v, w \in \mathbb{Z}_2[\pi, \zeta]$. We plug this into equation (7):

$$(1 - 4\zeta)x^2 + 4\pi v^2 = x^2 + 4xw + 4w^2.$$

Subtracting x^2 on both sides and dividing by 4 gives us

$$\pi v^2 - \zeta x^2 = (x + w)w.$$

[7] This is by Corollary 2.27.

We reduce this equation modulo π to get

$$\zeta x^2 + xw + w^2 = 0.$$

Since we assumed not all of x, y, z are divisible by π, we have that $x \not\equiv 0 \mod \pi$ and so we may define $\tilde{x} = w/x$. This gives

$$\tilde{x}^2 + \tilde{x} + \zeta = 0, \quad \text{in } \mathbb{F}_2[\zeta].$$

By the same arguments as before the proposition, this equation has no solutions. □

Remark 7.4. Note that during the proof we have only looked at the equation modulo 8. So we have actually shown that there are no solutions modulo 8. Also, the argument does not depend on the choice of uniformizer. Actually, the coefficients in the equation can be multiplied by squares to obtain the same result, so the coefficient in front of y^2 can be taken to be anything with odd valuation.

Corollary 7.5. *If we pick some Δ with odd valuation, the Hilbert symbol $(1 - 4\zeta, \Delta)_2$ equals -1. And so for such Δ the discussion before Proposition 7.3 shows that (χ, Δ) induces an element of order 4 in* $\mathrm{Br}(K)$.

Looking at the conditions we have obtained from considering the unramified extensions of degree 3 and 4 over K, we get back Proposition 7.2.

8 Elliptic curves over the ring of integers

In the previous chapter we have seen that the unramified extensions provided a simple answer to our problem. By considering norm groups associated to unramified extensions, we showed that if Δ has a valuation not divisible by 2 or 3, all elements of $\mathrm{Br}(K)[12]$ can be reached by only considering cyclic algebras associated to (unramified) cyclic Galois extensions of degree divisible by 12. However, when we only consider elliptic curves over the ring of integers $\mathcal{O}_K$, we see that we cannot use the same approach. Indeed, any elliptic curve over $\mathcal{O}_K$ has a minimal Weierstrass equation with discriminant of valuation 0. By Example 2.32, these discriminants clearly are elements of the norm groups associated to unramified extensions.

While the unramified extensions no longer give us the solution to our problem, we can use Lemma 6.3 to reverse the roles of the first and second argument of the Hilbert symbol. In other words, we consider the totally ramified extensions obtained by adding roots of a uniformizer and take $\Delta \in \mathcal{O}_K^*$ so that adding a root of Δ defines an unramified extension over K.

We will only consider the case where K is a local field over $\mathbb{Q}_2$ or $\mathbb{Q}_3$. For the other cases Proposition 6.7 can be used for all Hilbert symbol computations. In the case of local fields over $\mathbb{Q}_2$ and $\mathbb{Q}_3$ we make use of elliptic

curves of the form

$$y^2 + xy = x^3 - a. \tag{8}$$

As we saw in Example 3.7, the discriminant of such curves is

$$\Delta = a + 16 \cdot 27a^2.$$

We observe that modulo 8 or 27 we can get essentially any discriminant we want. This observation is important in our proof of Theorem 1.2 and 1.3. Another important part of these theorems is that for some local fields, we have some obstructions which make it impossible to find any unit $\Delta \in \mathcal{O}_K^*$ such that $[(-, \Delta)]$ is surjective onto $\mathrm{Br}(K)[12]$. We will deal with the 2-adic and 3-adic fields separately. In both cases we consider the 2- and 3-primary part as we did before. This time, we not only deduce sufficient conditions on Δ so that the map $[(-, \Delta)]$ is surjective, but also deduce some obstructions that show that surjectivity is impossible for some local fields.

8.1 The 2-adic fields

In this section, we will prove Theorem 1.2. Actually, we prove a slightly stronger result in which we can fix one discriminant Δ.

Theorem 8.1. *Let $K/\mathbb{Q}_2$ be a local field. There exists an elliptic curve over $\mathcal{O}_K$ so that the following hold:*

- *If K contains a primitive third root of unity, the following map is surjective*
$$[(-, \Delta)] \colon H^1(K, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{Br}(K)[12].$$
- *If K does not contain a primitive third root of unity, the image of the map above is $\mathrm{Br}(K)[4]$ and for any $\chi \in H^1(K, \mathbb{Z}/3\mathbb{Z})$ and $b \in \mathcal{O}_K^*$, the cyclic algebra (χ, b) is trivial.*

We will see that for local fields over $\mathbb{Q}_2$ some obstructions for surjectivity appear when we consider the 3-primary part of the map (6). We use Proposition 6.7 to show this. To prove surjectivity on the 2-primary part, we use the discussion of Section 2 and 7.2 in particular.

The 3-primary part The first obvious case to consider is the base case $K = \mathbb{Q}_2$. We already see an obstruction in this case. One can prove that there is no cyclic Galois extension of degree 3 over $\mathbb{Q}_2$ besides the unramified extension.[8] This means that the cyclic algebras (χ, Δ) for $\chi \in H^1(\mathbb{Q}_2, \mathbb{Z}/3\mathbb{Z})$ and $\Delta \in \mathbb{Z}_2^*$ are all trivial in $\mathrm{Br}(\mathbb{Q}_2)$ (see the discussion on the 3-primary part in Section 7.2).

[8] We can use local class field theory for this or use [LMFDB].

If $K/\mathbb{Q}_2$ has degree $d > 1$, we separate two cases. If K does not contain a primitive third root of unity ζ_3, we add it as per Section 6.2. This way, we get a local field $\tilde{K}$ with residue field $\mathbb{F}_{4^f}$, where $f = f(K/\mathbb{Q}_2)$ is the inertia degree of K. Using Proposition 6.7, we can see that for any $a \in \tilde{K}^*$ and $\Delta \in \mathcal{O}_K^*$, the Hilbert symbol equals

$$(a, \Delta)_3 = \omega(\Delta^{v_{\tilde{K}}(a)})^{(4^f-1)/3} = \omega(\Delta)^{v_{\tilde{K}} \sum_{j=0}^{f-1} 4^j} \in \omega(\Delta)^{\mathbb{Z}}.$$

Since $\Delta \in K^*$, we have $\omega(\Delta) \in \mu_{2^f-1}$ and so

$$(a, \Delta)_3 \in \mu_{2^f-1} \cap \mu_3 = \{1\}.$$

The equality comes from the assumption that K does not contain any primitive third roots of unity. We conclude that in this case the Hilbert symbol $(a, \Delta)_3$ is trivial for any choice of $a \in \tilde{K}^*$ and so for any $\chi \in H^1(K, \mathbb{Z}/3\mathbb{Z})$, the cyclic algebra (χ, Δ) is trivial.

If $\zeta_3 \in K$, there is no obstruction. For any choice of uniformizer $\pi \in K$ and any $\Delta \equiv \zeta_{2^f-1} \mod \mathfrak{p}_K$ we get for instance

$$(\pi, \Delta) = \omega(\Delta^{v_K(\pi)})^{(2^f-1)/3} = \zeta_{2^f-1}^{(2^f-1)/3} = \zeta_3^{\pm 1}.$$

We can consider any character χ for the extension $L = K(\sqrt[3]{\pi})$ over K to get a cyclic algebra that induces an element of order 3 in $\mathrm{Br}(K)$.

The 2-primary part In Section 7.2 we considered the extension L/K for $L = K(\sqrt{1-4\zeta})$ and took Δ to be a uniformizer. This time we do the converse. First, we need a totally ramified cyclic extension of degree 4. Theorem 2.29 and Proposition 2.15 give us an extension of degree 4 by considering the norm subgroup of K^* isomorphic to

$$\mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \oplus 4\mathbb{Z}_2 \oplus \mathbb{Z}_2^{d-1},$$

where q, d and a are defined as in Proposition 2.15. By Corollary 2.33, the associated extension is totally ramified. Finally, Theorem 2.28 shows that the extension is indeed cyclic because the quotient of the norm group is $\mathbb{Z}_2/4\mathbb{Z}_2 \cong \mathbb{Z}/4\mathbb{Z}$.

If we denote the extension defined above by L/K and pick a uniformizer τ of L, we can write $L = K(\tau)$. Indeed, we have $K(\tau) \subseteq L$ and since $K(\tau)$ has ramification index 4, it is not a strict subextension. The unique subextension is given by $K(\tau^2)/K$. Again, we observe that for any isomorphism $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/4\mathbb{Z}$, the cyclic algebra (χ, Δ) has order 4 in $\mathrm{Br}(K)$ if and only if (χ', Δ) has order 2 in $\mathrm{Br}(K)$, where $\chi'\colon \mathrm{Gal}(K(\tau^2)/K) \to \mathbb{Z}/2\mathbb{Z}$ is an isomorphism. The latter cyclic algebra is trivial precisely when the Hilbert symbol $(\tau^2, \Delta)_2$ equals 1.

Pick the uniformizer $\pi = \tau^2$ of K. If $\Delta = 1 - 4\zeta$, Proposition 7.3 shows that the Hilbert symbol $(\pi, 1-4\zeta)_2$ equals -1. In Remark 7.4 we observed that we only have to consider Δ modulo 8. Furthermore, since we only consider Δ up to squares, we can multiply with ζ, which is the square of some ζ^k because its order is odd. We conclude that $(\pi, \Delta)_2 = -1$ also for $\Delta \in \mathcal{O}_K^*$ with

$$\Delta \equiv \zeta - 4\zeta^2 \mod 8.$$

Lemma 8.2. *Let $K/\mathbb{Q}_2$ be a local field with inertia degree f and let $\Delta \in \mathcal{O}_K^*$ satisfy $\Delta \equiv \zeta - 4\zeta^2$, where ζ is a root of unity of order $2^f - 1$ in K.*

- *The map $[(-, \Delta)]\colon H^1(K, \mathbb{Z}/4\mathbb{Z}) \to \mathrm{Br}(K)[4]$ is surjective.*
- *The map $[(-, \Delta)]\colon H^1(K, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{Br}(K)[12]$ is surjective if and only if K contains a primitive third root of unity. This is precisely the case when f is even.*

Proof. The first statement follows immediately by the discussion on the 2-primary part above. The second follows by our discussion of the 3-primary part. The parity of f follows by the observation that $K(\zeta_3)/K$ defines the unramified degree 2 extension when $\zeta_3 \notin K$. □

In order to prove Theorem 8.1, we only need to find an elliptic curve whose discriminant Δ satisfies the condition of the lemma above. As we have mentioned, this is done by the elliptic curve

$$E\colon y^2 + xy = x^3 - \zeta + 4\zeta^2.$$

8.2 The 3-adic fields

In this section, we prove Theorem 1.3, the final main theorem of this thesis. As in the previous section, we show a slightly stronger result.

Theorem 8.3. *Let $K/\mathbb{Q}_3$ be a local field. There exists an elliptic curve over $\mathcal{O}_K$ so that the following hold:*

- *If K contains a primitive fourth root of unity, the following map is surjective*
$$[(-, \Delta)]\colon H^1(K, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{Br}(K)[12].$$
- *If K does not contain a primitive fourth root of unity, the image of the map above is $\mathrm{Br}(K)[6]$ and for any $\chi \in H^1(K, \mathbb{Z}/4\mathbb{Z})$ and $b \in \mathcal{O}_K^*$, the cyclic algebra (χ, b) does not induce an element of order 4 in $\mathrm{Br}(K)$.*

We use an approach similar to what we did for local fields over $\mathbb{Q}_2$. We try to find conditions on Δ to achieve surjectivity. This time we get possible obstructions by looking at the 2-primary part and use the symmetric property of the Hilbert symbol for the 3-primary part.

The 2-primary part In order for a map $[(-,\Delta)]$ to be surjective onto $\mathrm{Br}(K)[4]$, we want to find a cyclic Galois extension L/K of degree 4 so that $\Delta \in \mathcal{O}_K^*$ is not a norm of the extension. Moreover, we want that Δ is not a norm of the subextension either. By Example 2.32 this can only be the case when L/K is totally ramified. Otherwise, the subextension is unramified and the associated norm subgroup contains $\mathcal{O}_K^*$, including Δ. In other words, we want to find a subgroup $N \subset \mathcal{O}_K^*$ of index 4. By Proposition 2.15 this means finding a subgroup of index 4 in

$$\mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/3^a\mathbb{Z} \oplus \mathbb{Z}_3^d,$$

where $d = [K : \mathbb{Q}_3]$, $q = 3^f$ is the order of the residue field κ_K and a is such that $\mu_{3^a} \subset K$. Because any morphism from this group onto $\mathbb{Z}/4\mathbb{Z}$ must be trivial on the second and third summands, such a subgroup only exists if $q-1$ is divisible by 4.

If $i \notin K$, f is odd and so

$$q - 1 = 3^f - 1 = (3-1)\sum_{j=0}^{f-1} 3^j \equiv 2 \mod 4.$$

So in this case (χ, Δ) does not induce an element of order 4 in $\mathrm{Br}(K)$ for any $\chi \in H^1(K, \mathbb{Z}/4\mathbb{Z})$ and $\Delta \in \mathcal{O}_K^*$. We can still get an element of order 2 by letting χ be a character of $K(\sqrt{\pi})/K$ for some uniformizer $\pi \in K$. In this case we pick $\Delta \in \mathcal{O}_K^*$ with $\omega(\Delta) = \zeta_{q-1}$ for some root of unity of order $q-1$. Applying Proposition 6.7 to the corresponding Hilbert symbol $(\pi, \Delta)_2$ gives an element of order 2.

If $i \in K$, we can consider the cyclic Galois extension $K(\sqrt[4]{\pi})$ for any uniformizer $\pi \in K$. Picking $\Delta \equiv \zeta_{q-1} \mod \mathfrak{p}_K$ for some root of unity ζ_{q-1} of order $q-1$ and using Proposition 6.7 gives us

$$(\pi, \Delta)_4 = \omega(\Delta)^{v_K(\pi)(q-1)/4} = \zeta_{q-1}^{(q-1)/4} = \pm i.$$

So for any isomorphism $\chi\colon \mathrm{Gal}(K(\sqrt[4]{\pi})/K) \to \mathbb{Z}/4\mathbb{Z}$, we get that $[(\chi, \Delta)]$ has order 4.

The 3-primary part Different from our proof of Theorem 8.1 in the previous section, we will not give an explicit $\Delta \in \mathcal{O}_K^*$ such that $[(-,\Delta)]$ is surjective onto $\mathrm{Br}(K)[12]$ or $\mathrm{Br}(K)[6]$. Intead we show that such an element exists and is the discriminant of some elliptic curve over $\mathcal{O}_K$ of the form (8).

First, we let L/K be the extension corresponding to the norm subgroup N isomorphic to

$$\mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/3^a\mathbb{Z} \oplus 3\mathbb{Z}_3 \oplus \mathbb{Z}_3^{d-1},$$

by Proposition 2.15. We set $A = N \cap U_K^{(1)}$, so that[9]

$$A \cong \mathbb{Z}/3^a\mathbb{Z} \oplus 3\mathbb{Z}_3 \oplus \mathbb{Z}_3^{d-1}.$$

For any $b \in U_K^{(1)} \setminus A$ and character $\chi\colon \mathrm{Gal}(L/K) \to \mathbb{Z}/3\mathbb{Z}$ we have that the cyclic algebra (χ, b) has order 3 in $\mathrm{Br}(K)$ because by construction it is not a norm of L/K. Since the order of (χ, b) only depends on the class of b in $K^*/(K^*)^3$, we claim that we can also take $\Delta \equiv b\zeta_{q-1} \mod 27$. Since $q-1$ is coprime to 3, ζ_{q-1} is a cube and so $b \equiv b\zeta_{q-1}$ in $K^*/(K^*)^3$. The claim now follows by applying Corollary 2.12.

Lemma 8.4. *Let $K/\mathbb{Q}_3$ be a local field with inertia degree f and let $\Delta \in \mathcal{O}_K^*$ such that $\Delta \equiv b\zeta_{3^f-1}\mathfrak{p}_K$ with b as above.*

- *The map $[(-, \Delta)]\colon H^1(K, \mathbb{Z}/6\mathbb{Z}) \to \mathrm{Br}(K)[6]$ is surjective.*
- *The map $[(-, \Delta)]\colon H^1(K, \mathbb{Z}/12\mathbb{Z}) \to \mathrm{Br}(K)[12]$ is surjective if and only if K contains a primitive fourth root of unity. This is precisely the case when f is even.*

Proof. Both statements follow by our discussions on the 2- and 3-primary part. The parity of f in the last statement is because $K(i)/K$ defines an unramified extension of order 2 when K does not contain a primitive fourth root of unity. □

As we mentioned at the beginning of this section, such a discriminant $\Delta \in \mathcal{O}_K^*$ can be achieved by the elliptic curve

$$y^2 + xy = x^3 - b\zeta_{q-1}.$$

This proves Theorem 8.3.

9 Outlook

In this thesis we have solved the question of which elements of $\mathrm{Br}(K)$ can be reached by cyclic algebras of the form (χ, Δ), where Δ is the discriminant of an elliptic curve over a local field K or over the ring of integers of $K/\mathbb{Q}_p$ for $p \in \{2, 3\}$. There are some parts that have not been fully worked out and some others where one might hope to get a more general statement.

First of all, we have tried to find explicit sufficient conditions on Δ so that (χ, Δ) has the desired order for an appropriate choice of χ. In almost all cases we have found a very explicit curve that has a discriminant satisfying these

[9] To get A more explicitly, one needs to write down the explicit isomorphism of Proposition 2.15. This is somewhat troublesome as this depends on the choice of integral basis of $\mathcal{O}_K$ over $\mathbb{Z}_3$ and on the ramification index through the isomorphism $U_K^{(n)} \cong \mathfrak{p}_K^n$ for $n > e/(p-1)$.

conditions. One exception is Lemma 8.4, where we somewhat implicitly get an element $b \in U_K^{(1)}$. If we fix K, we can use the exponent map to write down an explicit isomorphism as in Proposition 2.15. This way we can get a more explicit expression for b.

For elliptic curves over a local field K, we have shown that the unramified extensions always allow us to reach $\mathrm{Br}(K)[12]$ with cyclic algebras of the form (χ, Δ). In the case of elliptic curves over $\mathcal{O}_K$, we only considered local fields over $\mathbb{Q}_2$ and $\mathbb{Q}_3$. An interesting question is whether this approach can also be generalized to arbitrary local fields. For instance, the same obstruction that appears for $\mathbb{Q}_2$ also applies to $\mathbb{Q}_p$ for $p \equiv 1 \mod 4$. One difficulty is that elliptic curves of the form (8) are not as useful for $p > 3$. On the other hand, for larger p, we can use Proposition 6.7 for both the 2- and 3-primary part. This makes computations much simpler.

As we have said before, we have focused on finding sufficient conditions on Δ to get a surjective map $[(-, \Delta)]$ onto $\mathrm{Br}(K)[12]$. An interesting question is whether we can also find necessary conditions. When we restrict ourselves to unramified extensions for instance, we see that we need $v_K(\Delta) \equiv \pm 1 \mod 6$ to get a cyclic algebra of order 3. On the other hand, we have seen in Section 6.2 that for totally ramified extensions, we can also find Δ with valuation 0 so that (χ, Δ) is non-trivial. By considering every possible cyclic Galois extension of a given order, one can arrive at a list of conditions on Δ so that when Δ does not satisfy any of them, there are no cyclic algebras (χ, Δ) of the desired order. Can we arrive at such a list of necessary conditions for an arbitrary local field K?

Tying into this last question, we can also flip the main question we have answered in this thesis. Instead of choosing Δ and finding characters χ so that (χ, Δ) has the order we want, we can also fix χ and wonder what the order of cyclic algebras of the form (χ, Δ) is for a choice of discriminant. In other words, we can consider the image of the map

$$[(\chi, \Delta(-))] \colon \mathbf{Ell}_K \to \mathrm{Br}(K).$$

In general this question is much harder than the question we answered in this thesis. Different from the map $[(-, \Delta)]$, this map is not a group morphism and so we cannot consider the 2- and 3-primary part separately.

Finally, giving both sufficient and necessary conditions on Δ allows us to more easily consider a similar question for sets of numbers beside discriminants of elliptic curves. For any subset $A \subset K^*$ we can consider which elements of $\mathrm{Br}(K)$ can be reached by cyclic algebras of the form (χ, a) with $a \in A$. To compute the Brauer group of the moduli stack of elliptic curves, the question appears to be relevant for

$$A = \{\Delta \mid \Delta \equiv \Delta(E) \mod (K^*)^{12} \text{ for some elliptic curve } E \text{ over } K\}.$$

For other problems, one might be interested in the problem for a different choice of subgroup A.

References

[AM16] B. Antieau and L. Meier. *The Brauer group of the moduli stack of elliptic curves*. 2016. eprint: arXiv:1608.00851.

[AH28] E. Artin and H. Hasse. "Die beiden Ergänzungssätze zum Reziprozitätsgesetz der n-ten Potenzreste im Körper derl n-ten Einheitswurzeln". In: *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 6.1 (Dec. 1928), pp. 146–162. DOI: 10.1007/bf02940607. URL: https://doi.org/10.1007/bf02940607.

[CF10] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society with the Support of the International Mathematical Union*. London Mathematical Society, 2010. ISBN: 9780950273426.

[CS19] J.-L. Colliot-Thélène and A. N. Skorobogatov. *The Brauer–Grothendieck group*. Available at https://www.imo.universite-paris-saclay.fr/~colliot. 2019.

[GS06] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2006. ISBN: 9781139458726.

[Gro66] A. Grothendieck. *Le groupe de Brauer: II. Théories cohomologiques*. fr. Séminaire Bourbaki 9. Société mathématique de France, 1966.

[Hel02] C. Helou. "On the Hilbert symbol in cyclotomic fields". eng. In: *Acta Arithmetica* 105.1 (2002), pp. 35–49. URL: http://eudml.org/doc/278131.

[Hen81] G. Henniart. "Sur les lois de réciprocité explicites. I." In: *Journal für die reine und angewandte Mathematik* 329 (1981), pp. 177–203. URL: http://eudml.org/doc/183529.

[Kal85] W. van der Kallen. "The Merkurjev-Suslin theorem". English. In: *Lecture notes in Math.* 1142 (1985), pp. 157–168.

[KM85] NICHOLAS M. KATZ and BARRY MAZUR. *Arithmetic Moduli of Elliptic Curves. (AM-108)*. Princeton University Press, 1985. ISBN: 9780691083520.

[Lan94] S. Lang. *Algebraic Number Theory*. Graduate Texts in Mathematics. Springer, 1994. ISBN: 9780387942254.

[Liu02] Q. Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford graduate texts in mathematics. Oxford University Press, 2002. ISBN: 9780198502845.

[LMFDB] The LMFDB Collaboration. *The L-functions and Modular Forms Database*. http://www.lmfdb.org. [Online; accessed March 2020]. 2020.

[Mil13] J.S. Milne. *Class Field Theory (v4.02)*. Available at `www.jmilne.org/math/`. 2013.

[Neu99] J. Neukirch. *Algebraic Number Theory. Transl. from the German by Norbert Schappacher.* English. Vol. 322. Berlin: Springer, 1999. ISBN: 3-540-65399-6/hbk.

[Ser79] J.P. Serre. *Local Fields*. Graduate Texts in Mathematics. Springer-Verslag New York, 1979. ISBN: 0-387-90424-7.

[Sil09] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, 2009.

[Sko99] A.N. Skorobogatov. "Beyond the Manin obstruction". English. In: *Invent. Math.* 135.2 (1999), pp. 399–424. ISSN: 0020-9910; 1432-1297/e.