Honours Project in Mathematics

Local Class Field Theory

Arshay Nimish Sheth

Supervisor: Professor Gan Wee Teck

Department of Mathematics
National University of Singapore

2018/2019 Semesters 1 & 2

Acknowledgements

Firstly, I would like to thank my parents and my sister for their constant love, encouragement and support.

I would like to thank Professor Gan Wee Teck for agreeing to supervise me for the final year project. I thoroughly enjoyed and also learned a lot from the weekly meetings that I had with Prof.Gan. I would also like to thank Professor Chin Chee Whye for his very careful reading of an earlier draft of this thesis and for giving concrete suggestions to improve some parts of the thesis.

Last, but certainly not the least, I would like to thank all my friends.

Contents

1 Introduction **1**
- 1.1 Historical background 1
- 1.2 The two branches of class field theory 4

2 Statements of local class field theory **6**
- 2.1 Class field theory for finite fields 6
- 2.2 The main theorems of local class field theory 7

3 Background on local fields **9**
- 3.1 Definition of local fields 9
- 3.2 Hensel's lemma & its applications 12
- 3.3 Ramification theory of local fields 13
- 3.4 Multiplicative structure of local fields 16

4 The Brauer group **19**
- 4.1 Some background on non-commuative ring theory 19
- 4.2 Defining the Brauer group 20
- 4.3 Examples of the Brauer group 21
- 4.4 Relative Brauer group 22

5 Group cohomology **23**
- 5.1 Tate cohomology groups 23
- 5.2 Shapiro's Lemma & its applications 25
- 5.3 The standard resolution 27
- 5.4 Tate's theorem 30
- 5.5 Examples in low degrees 33

6 Applications of group cohomology **35**
- 6.1 Brauer group of a local field 35
- 6.2 Galois cohomology 40

6.3 Hilbert symbol 42

7 Proof of Local Class Field Theory **44**
7.1 Reciprocity theorem 45
7.2 Norm subgroups 46
7.3 Tate duality and universal norms 48
7.4 Applications and concluding remarks 50

Chapter 1

Introduction

The purpose of this chapter is to first motivate the desire and need for class field theory and then explain the reasons behind studying a particular version of the subject - local class field theory.

1.1 Historical background

The main theme of class field theory is to study abelian extenions of fields. Recall that a field extension L/F is said to be abelian if it is Galois and its Galois group is an abelian group. In this section, we give some historical background and motivation to explain why studying abelian extensions of fields is important and interesting.

Fermat is often regarded as the father of modern number theory and indeed the historical origins of class field theory can be traced back to Fermat as well. In a letter to Mersenne dated 25th December 1640, Fermat stated the following theorem.

Theorem 1.1.1 (Fermat)**.** A prime number p is a sum of two squares if and only if $p \equiv 1 \mod 4$.

From the modern perspective of algebraic number theory, we now know that this theorem essentially deals with the question of how prime numbers decompose in the ring $\mathbb{Z}[i]$. To be more precise, consider the following more general situation: let K be a quadratic number field and let $\mathcal{O}_K$ be its ring of integers. If we take a prime number p in $\mathbb{Z}$ and consider the ideal $p\mathcal{O}_K$ that p generates in $\mathcal{O}_K$, there are three possibilities:

- $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for distinct prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ of $\mathcal{O}_K$ (p is split)

- $p\mathcal{O}_K = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ (p is ramified)
- $p\mathcal{O}_K$ is itself a prime ideal (p is inert)

Using this terminology, Fermat's theorem can be rephrased as follows: in the ring $\mathbb{Z}[i]$, we have: p is split if and only if $p \equiv 1 \bmod 4$, p is ramified if and only if $p = 2$ and p is inert if and only if $p \equiv 3 \bmod 4$.

It turns out that similar phenomena arise for all quadratic fields; the table below provides more examples of these.

Field	totally decomposed prime numbers p	ramified prime numbers p
$\mathbb{Q}(\sqrt{-1})$	$p \equiv 1 \bmod 4$	$p = 2$
$\mathbb{Q}(\sqrt{2})$	$p \equiv 1, 7 \bmod 8$	$p = 2$
$\mathbb{Q}(\sqrt{-2})$	$p \equiv 1, 3 \bmod 8$	$p = 2$
$\mathbb{Q}(\sqrt{3})$	$p \equiv 1, 11 \bmod 12$	$p = 2, 3$
$\mathbb{Q}(\sqrt{-3})$	$p \equiv 1 \bmod 3$	$p = 3$
$\mathbb{Q}(\sqrt{5})$	$p \equiv 1, 4 \bmod 5$	$p = 5$
$\mathbb{Q}(\sqrt{-5})$	$p \equiv 1, 3, 7, 9 \bmod 20$	$p = 2, 5$
$\mathbb{Q}(\sqrt{6})$	$p \equiv 1, 5, 23, 19 \bmod 24$	$p = 2, 3$
$\mathbb{Q}(\sqrt{-6})$	$p \equiv 1, 5, 7, 11 \bmod 24$	$p = 2, 3$
$\mathbb{Q}(\sqrt{-15})$	$p \equiv 1, 2, 4, 8 \bmod 15$	$p = 3, 5$

Figure 1.1: Source: [KKS2011]

An inspection of the table reveals the following observations:

- There is a finite number of ramified primes and how a prime p splits is determined mod N for an integer N which is a product of the ramified primes with some multiplicities.
- The split primes form a subgroup of index 2 of $(\mathbb{Z}/N\mathbb{Z})^\times$. For instance, $(\mathbb{Z}/15\mathbb{Z})^\times = \{1, 2, 4, 7, 8, 11, 13, 14\}$ and $\{1, 2, 4, 8\}$ are the set of split primes by the table which do indeed form a subgroup of index 2.

  We now proceed to briefly explain how such phenomena are explained by class field theory. Class field theory had its origins in the quadratic reciprocity law of Euler, Gauss and Legendre. The next important milestone in class field theory was the Kronecker-Weber theorem which was in fact completely proved by David Hilbert in 1896. The theorem states that every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field:

  Theorem 1.1.2 (Kronecker-Weber theorem)**.** If $L/\mathbb{Q}$ is a finite abelian extension, then $L \subseteq \mathbb{Q}(\zeta_n)$ where $n \in \mathbb{N}$ is a natural number and ζ_n is a primitive nth-root of unity.

Let n be the smallest integer for which the theorem above holds; such an integer is known as a conductor. Now class field theory provides us with the following theorem:

Theorem 1.1.3. Let K be a number field.

1. Assume $K/\mathbb{Q}$ is abelian. Then:
   (a): A prime number p is ramified in K if and only if p divides the conductor.
   (b): If $K \subseteq \mathbb{Q}(\zeta_N)$, then whether or not p splits in K depends on p modulo N.
2. Conversely, if the conclusion of (b) holds, then $K \subseteq \mathbb{Q}(\zeta_N)$ and so $K/\mathbb{Q}$ is abelian

In summary, what we have is the following: whether or not a prime number p splits in $\mathbb{Q}(\zeta_N)$ is determined by p mod N. By the Kronecker-Weber theorem, every abelian extension (in particular, every quadratic extension) is contained in cyclotomic field. Thus, the key-point is this: whether or not a prime number p splits in a quadratic field is determined by p mod N for some $N \in \mathbb{N}$.

Let L/K be an abelian extension of number fields. What we have described above is essentially the theory when $K = \mathbb{Q}$; a natural question to ask would be: is there any analogous theory when K is an arbitrary number field? The answer provided by class field theory is a resounding yes: indeed corresponding to the extension $\mathbb{Q}(\zeta_N)$ over $\mathbb{Q}$, there is certain extension $K(\mathfrak{a})$ over K for which laws similar to the ones above hold. For instance, one can derive the following from class field theory:

Theorem 1.1.4 (One consequence of class field theory)**.** Let K be a number field and $\mathfrak{a}$ be an ideal of $\mathcal{O}_K$. Then:

1. There exists a unique finite extension $K(\mathfrak{a})$ of K having the following property: if $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_K$ not diving $\mathfrak{a}$, then $\mathfrak{p}$ is split in $K(\mathfrak{a})$ if and only if there exists a totally positive element $\alpha \in \mathcal{O}_K$ such that $\mathfrak{p} = (\alpha)$ and $\alpha \equiv 1 \bmod \mathfrak{a}$
2. (Analogue of the Kronecker Weber theorem): Moreover, $K(\mathfrak{a})$ is an abelian extension of K and every finite abelian extension of K is contained in $K(\mathfrak{a})$ for some $\mathfrak{a}$.

1.2 The two branches of class field theory

The last section gave a flavour of class field theory and motivated the study of abelian extensions of algebraic number fields. The study of abelian extensions of algebraic number fields constitutes what is known as global class field theory. There is another branch of class field theory known as local class field theory: this studies abelian extensions of special fields called local fields. Despite the fact that the motivation in the previous section pertained to global fields, this entire report will focus on local class field theory for reasons that we now proceed to explain.

During the study of number theory, a key insight that mathematicians had is that there exists deep analogies between number theory and certain functions such as polynomial rings. One such analogy is the following: the ring of integers $\mathbb{Z}$ and the polynomial ring in one variable over $k[T]$ are both principal ideal domains and hence also unique factorization domains. Kurt Hensel took the analogy between number theory and functions further in 1900. Hensel was motivated by the fact that every rational function with complex coeffcients can be expanded at each point $T = \alpha \in \mathbb{C}$ in the Laurent series $\sum_{n=m}^{\infty} c_n(T-\alpha)^n$ for $m \in \mathbb{Z}$ and $c_n \in \mathbb{C}$. Hensel realized that analogously for each prime number p, every rational number has a p-adic expansion; for instance when $p = 2$ we have $\frac{1}{6} = \frac{1}{2} - 1 + 2 - 2^2 + 2^3 - \cdots$. This led him to define, for each prime p, the p-adic numbers denoted by $\mathbb{Q}_p := \{\sum_{n=m}^{\infty} c_n p^n | m \in \mathbb{Z}, c_n \in \{0, 1, \ldots, p-1\}\}$. It can be shown that $\mathbb{Q}_p$ is a field and is one example of a local field. Local fields are very important in modern number theory because of the following philosophy:

> Local-Global principle: To solve a problem over $\mathbb{Q}$, first try to solve the problems over local fields such as $\mathbb{Q}_p$

As an example of the local-global principle, we present the following theorem.

Theorem 1.2.1 (Rational points on conics)**.** The conic $ax^2 + by^2 = c$ for $a, b, c \in \mathbb{Q}^\times$ has a rational solution if and only if has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.

Thus, in this chapter we briefly discussed the motivations behind studying abelian extensions of local fields. We end with a quotation which summarizes the whole essence of what class field theory aims to do [Neu1986]: "The

main goal of class field theory is to classify all algebraic extensions of a given field F. The law governing the constitution of extensions of F is hidden in the inner structure of the base field F itself, and should therefore be expressed in terms of entities directly associated with it."

Chapter 2

Statements of local class field theory

In this chapter, our goal will be to state the main theorems of local class field theory. We have not defined local fields as yet; nevertheless we encourage the reader to keep $\mathbb{Q}_p$ as an example in mind.

2.1 Class field theory for finite fields

The class field theory for finite fields is a toy example that also gives us a preview of what is to come later. Consider $\mathbb{F}_p$, the finite field with p elements.

Theorem 2.1.1 (Class field theory for finite fields)**.** Equip $\mathbb{Z}$ with the discrete topology. Then we have the following $1:1$ correspondence:
$\{\text{finite abelian extensions of } \mathbb{F}_p\} \overset{1:1}{\longleftrightarrow} \{\text{open subgroups of finite index of } \mathbb{Z}\}$

Proof. We know from Galois theory that for each $n \in \mathbb{N}_{\geq 1}$, there exists a unique extension of degree n which we denote by $\mathbb{F}_{p^n}$. Thus, the map $\mathbb{F}_{p^n} \mapsto n\mathbb{Z}$ is the required bijection. □

Note that the adjectives "open" and "of finite index" applied to subgroups of $\mathbb{Z}$ are not really necessary since all non-zero subgroups of $\mathbb{Z}$ are of this form: we could have written the right hand side as simply the set of all non-zero subgroups of $\mathbb{Z}$. But we have chosen to present the theorem in this form to mimic the corresponding statements of local class field theory. Also note that the theorem essentially tells us that understanding abelian extensions of $\mathbb{F}_p$ is equivalent to understanding $\mathbb{Z}$, which is a relatively simple group to study. The question arises: for a local field F, is there a corresponding group that is simple and somehow

	easy-to-understand side	**the Galois side**
finite field $\mathbb{F}_p$	$\mathbb{Z}$	$\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$
local field F	$F^\times$	$\mathrm{Gal}(L/F)$

also encapsulates information of all its abelian extensions? Local class field theory answers this question in the affirmative and we explain this in the next section. Nevertheless, we give the answer right away in the form of the above table.

2.2 The main theorems of local class field theory

There are essentially two main theorems of local class field theory: the Reciprocity theorem and the Existence theorem.

To explain the Reciprocity theorem, we first introduce the notion of a norm.

Definition 2.2.1 (Norms)**.** Let L/F be a finite extension of fields. For $\alpha \in L$, we have an F-linear multiplication map $m_\alpha : L \to L$ with $m_\alpha(x) = \alpha \cdot x$. The determinant of this map is called the norm of α and is denoted by N_α.

A norm satisfies some important properties: firstly $N_\alpha \in F^\times$ for all $\alpha \in L^\times$ and secondly, we also have multiplicativity: $N_\alpha \cdot N_\beta = N_{\alpha\beta}$ for all $\alpha, \beta \in L$.

Definition 2.2.2 (Norm subgroups)**.** By the last theorem, we get a group homomorphism $N_{L/F} : L^\times \to F^\times$ with $N_{L/F}(\alpha) = N_\alpha$ and call it the norm map. The subgroup $N_{L/F}(L^\times)$ of $F^\times$ is called the norm subgroup.

We are now ready to state the Reciprocity theorem.

Theorem 2.2.1 (Reciprocity theorem)**.** Let L/F be a finite Galois extension of local fields. Then $\mathrm{Gal}(L/F)^{\mathrm{ab}} \cong F^\times/N_{L/F}(L^\times)$ as groups, where $\mathrm{Gal}(L/F)^{\mathrm{ab}}$ is the abelianization of $\mathrm{Gal}(L/F)$.

Recall that our goal was to understand the arithmetic of abelian extensions of L/F by data internal to F. Using the Reciprocity theorem, one proves the existence theorem of local class field theory which acheives our goal. Note how this theorem parallels the corresponding version for finite fields:

Theorem 2.2.2 (Existence theorem of local class field theory)**.** Let F be a local field. Then:

$$\{\text{finite abelian extensions of } F\} \overset{1:1}{\leftrightarrow} \{\text{open subgroups of finite index of } F^\times\}$$

Moreover, this correspondence is inclusion reversing and is given by associating a finite abelian extension L of F to the subgroup $N_{L/F}L^\times$ of $F^\times$.

This report will be focused on proving these two main theorems. As a first step, we need to understand local fields better; this is the subject of the next chapter where we first define local fields in general and then explain some of their key properties.

Chapter 3

Background on local fields

3.1 Definition of local fields

In this section, we will define local fields. The prototypical example of local fields will be $\mathbb{Q}_p$, the p-adic numbers. We begin with the following definition:

Definition 3.1.1 (Valuations)**.** A valuation on a field F is a map $v : F \to \mathbb{R} \cup \{\infty\}$ such that:

1. $v(x) = \infty$ iff $x = 0$
2. $v(xy) = v(x) + v(y)$ for all $x, y \in F$
3. $v(x + y) \geq \min\,(v(x), v(y))$ for all $x, y \in F$.

The additive group $v(F^\times) \subseteq \mathbb{R}$ is called the valuation group of v and v is called discrete if the valuation group is of the form $\alpha\mathbb{Z}$ for some real number $\alpha \geq 0$.

Example 3.1.1 (p-adic valuation)**.** Let $K = \mathbb{Q}$ and let p be a prime number. For each $a \in \mathbb{Q}^\times$, write $a = p^m \frac{u}{v}$, where $m \in \mathbb{Z}$ and $p \nmid u$ and $p \nmid v$. Define $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ by setting $v_p(a) = m$ for a non-zero and $v_p(0) = \infty$. Then v_p is a discrete valuation and is called the p-adic valuation.

Definition 3.1.2 (Absolute values)**.** An absolute value on a field F is map $|| : F \to \mathbb{R}$ such that

1. $|x| \geq 0$ for all $x \in F$ and $|x| = 0$ iff $x = 0$
2. $|xy| = |x||y|$ for all $x, y \in F$
3. $|x + y| \leq |x| + |y|$ for all $x, y \in F$.

If moreover, we have $|x+y| \leq \max(x|, |y|)$ for all $x, y \in F$, the absolute value is said to be non-archimedean.

The key point of a valuation is that it gives rise to a non-archimedean absolute value on the field F: for each $a \in F^\times$ define $|a|_v := \lambda^{v(a)}$, where $\lambda \in (0,1)$ and set $|0|_v = 0$. One checks using the Definition 3.1.2, that this indeed gives rise to a non-archimedean absolute value. Furthermore, this absolute value in turn gives rise to a metric: $d(a,b) := |a-b|_v$ for $a, b \in F$.

Example 3.1.2 (Absolute values arising from the p-adic valuation)**.** Let v_p be the p-adic valuation. Let $\lambda = \frac{1}{p}$. Then:

- $|p|_{v_p} = \frac{1}{p}$ and $|p^2|_{v_p} = \frac{1}{p^2}$.
- $d(p^2, p) = |p^2 - p|_{v_p} = |p(p-1)|_{v_p} = |p|_{v_p} \cdot |1-p|_{v_p} = \frac{1}{p}$

Having thus obtained a metric on the field F, it is natural to ask whether F is complete with respect to this metric. This motivates the following definition:

Definition 3.1.3 (Complete discrete valuation field)**.** A field F equipped with a discrete valuation v which is complete with respect to the metric induced by the valuation is called a complete discrete valuation field.

One can show that $\mathbb{Q}$ is not complete with respect to the p-adic valuation; see [Gov1993, Lemma 3.2.3] for an explicit example of a Cauchy sequence in $\mathbb{Q}$ which does not converge with repsct to the p-adic absolute value. More generally, if F is not complete with respect to an absolute value, we can 'complete' it just as we construct $\mathbb{R}$ from $\mathbb{Q}$. More precisely, we have:

Theorem 3.1.1 (Completion of a field)**.** Let F be a field equipped with an absolute value $||$. Then there exists a field $\hat{F}$ also equipped with an absolute value $||'$ and a map $\iota : F \to \hat{F}$ such that:

1. $\hat{F}$ is complete
2. ι is an isometry with dense image
3. Every embedding of F into a complete field L can be uniquely extended to an embdedding $\hat{F}$ into L.

Proof. See [KKS2011, Chapter 6 section (c)]. □

Definition 3.1.4 (The p-adic numbers)**.** The completion of $\mathbb{Q}$ with respect to the p-adic absolute value is called the field of p-adic numbers and is denoted by $\mathbb{Q}_p$.

Definition 3.1.5. The set $\mathcal{O}_F = \{x \in F : v(x) \geq 0\}$ is called the ring of integers of F.

Using to the properties of a valuation, one checks that O_F is indeed a ring.

Definition 3.1.6 (p-adic integers)**.** When $F = \mathbb{Q}_p$, the ring of integers of F is called the ring of p-adic integers and is denoted by $\mathbb{Z}_p$.

Example 3.1.3 (Localization at a prime)**.** When $F = \mathbb{Q}$ under the p-adic valuation, $\mathcal{O}_F = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$. This ring is denoted by $\mathbb{Z}_{(p)}$ and is called the localization of $\mathbb{Z}$ at p.

Also note that $x \in F \implies xx' = 1$ for some $x' \in F \implies v(xx') = v(1) \implies v(x) + v(x') = 0 \implies v(x) = -v(x')$. Thus both x and $x' \in \mathcal{O}_F^\times$ if and only if $v(x) = v(x') = 0$. Thus, it follows that O_F has unique maximal ideal $\mathfrak{p} = \{x \in F : v(x) > 0\}$; in other words, $\mathcal{O}_F$ is a local ring. The resulting field $\mathbb{F} := \mathcal{O}_F/\mathfrak{p}$ is called the residue field of F. It can be shown that the residue field of $\mathbb{Q}$ with respect to the p-adic valuation is $\mathbb{Z}/p\mathbb{Z}$. We now have all the ingredients ready to define a local field.

Definition 3.1.7 (Local fields)**.** A local field is complete discrete valuation field with finite residue field. We also require the valuation to be non-trivial.

Example 3.1.4. By our remarks above, $\mathbb{Q}_p$ is a local field.

The next proposition gives us more information about $\mathcal{O}_F$ and the maximal ideal $\mathfrak{p}$. We first note that if $v(F^\times) = \alpha\mathbb{Z}$, we can always normalize the valuation on F by replacing v with $v' = \frac{1}{\alpha}v$, so that $v'(F^\times) = \mathbb{Z}$.

Proposition 3.1.1. We have that $\mathcal{O}_F$ is a PID. Moreover,any non-zero element of F can be written uniquely in the form $\pi^n u$ with $n \in \mathbb{Z}$ and u a unit.

Proof. Without loss of generality, we can assume that the valaution is normalized. Pick $\pi \in \mathcal{O}_F$ such that $v(\pi) = 1$. Let I be any ideal and let $n = \min(v(x) : x \in I)$. Then $\pi^{-n}I \subseteq \mathcal{O}_F$ and is still an ideal. However, $\pi^{-n}I$ also contains units, so $\pi^{-n}I = \mathcal{O}_F$. Thus, $I = \pi^n\mathcal{O}_F = (\pi^n)$.
For $x \in F^\times$, let $n \in \mathbb{Z}$ be the valuation of x. Then we thus have $v(\pi^{-n}x) = 0$. Thus, $u := \pi^{-n}x$ is a unit and $x = \pi^n u$. For uniqueness, assume $\pi^n u = \pi^m v$ and suppose $n > m$. Then $\pi^{n-m} = vu^{-1}$ which implies that $(\pi^{n-m}) = \mathcal{O}_F$, a contradiction. Thus $n = m$ and cancelling on both sides yields $u = v$. □

We end this section by giving a complete characterization of local fields.

Theorem 3.1.2 (Classification of local fields)**.** Every local field is isomorphic to either: 1) a finite extension of $\mathbb{Q}_p$ or 2) a finite extension of $\mathbb{F}_p((t))$, where $\mathbb{F}_p((t))$ is the fields of formal Laurent series over $\mathbb{F}_p$.

Proof. See [Fre2017, Proposition 3.5]. □

We remark that, for simplicity and the desire to work in characteristic 0, all our local fields from this point on will be either $\mathbb{Q}_p$ or finite extensions of $\mathbb{Q}_p$; we will sometimes call them p-adic fields for emphasis.

3.2 Hensel's lemma & its applications

The purpose of this section will be to state Hensel's lemma, which is an important tool to develop the theory of local fields further. The essence of Hensel's lemma is that relatively prime factorizations in the residue field lift:

Theorem 3.2.1 (Hensel's lemma)**.** Let F be a local field and let $f \in \mathcal{O}_F[X]$ be a polynomial such that $\overline{f} = f_1 f_2$ in $\mathbb{F}[X] \setminus \{0\}$ with $f_1, f_2 \in \mathbb{F}[X]$ relatively prime. Then there is a factorization $f = gh$ in $\mathcal{O}_F[X]$ with $g, h \in \mathcal{O}_F[X]$ satisfying $\overline{g} = f_1$, $\overline{h} = f_2$ and $\deg g = \deg \overline{g}$.

Proof. See [Gui2018]. □

We now present some applications of Hensel's lemma.

Example 3.2.1 (Roots of unity in $\mathbb{Q}_p$)**.** Let $f(X) = X^{p-1} - 1 \in \mathbb{Z}_p[X]$. By Lagrange's theorem, we have $\alpha^{p-1} = 1$ for all $\alpha \in \mathbb{F}_p^\times$. Thus, $\overline{f} \in \mathbb{F}_p[X]$ factors as a product of distinct linear factors in $\mathbb{F}_p[X]$. Since the factors are distinct, we can apply Hensel's lemma to conclude that f has $p-1$ distinct roots in $\mathbb{Z}_p$ *i.e.* the $(p-1)$st roots of unity are in $\mathbb{Z}_p \subseteq \mathbb{Q}_p$.

Proposition 3.2.1 (Two-in implies all-in property)**.** Let F be a local field and suppose $f = a_0 + a_1 x + \cdots + a_n x^n \in F[X]$ is an irreducible polynomial with coefficients in F. If a_0 and a_n both lie in $\mathcal{O}_F$, then in fact $f \in \mathcal{O}_F[X]$.

Proof. Let $k \in \mathbb{N}$ be the smallest natural number such that $\pi^k f \in \mathcal{O}_F[X]$. Suppose for contradiction that $k > 0$. Then the first and the last coefficients of the polynomial $P = \pi^k f$ are in the ideal $\mathfrak{p}$, so $\deg(\overline{P}) < \deg(P)$ and X divides $\overline{P}$. Write $\overline{P} = X^m Q$ where $0 < m < n$ and X does not divide Q. By Hensel's lemma, there exists a polynomial $g(X) \in \mathcal{O}_F[X]$ of degree m which divides P in $F[x]$ and so $\pi^{-k} g(X)$ divides f in $F[X]$. This contradicts the fact that f is irreducible, so $k = 0$ as desired. □

The following theorem is important and will be used in later chapters.

Theorem 3.2.2 (Extending valuations)**.** Let F be a local field and suppose K/F is an extension with $[K : F] = n$. Then there exists a unique discrete valuation v_K on K extending the valuation v on F. It is given by the rule $v_K(\alpha) = \frac{1}{n}v(N_{L/K}(\alpha))$, where $N_{L/K}$ is the norm map.

Proof. For $x \in F$, $v_K(x) = \frac{1}{n}v(N_{K/F}(x)) = \frac{1}{n}v(x^n) = v(x)$. Hence v_K extends v. We proceed to show that v_K is indeed a valuation. It follows from the axioms of a valuation that $v_K(\alpha\beta) = v_K(\alpha)+v_K(\beta)$ for all $\alpha, \beta \in L$ and that $v_K(\alpha) = \infty$ iff $\alpha = 0$. We need some more work to show that $v_K(\alpha + \beta) \geq \min(v_K(\alpha), v_K(\beta))$. Note that this is equivalent to proving the statement that $v_K(1+\alpha) \geq 0$ if $v_K(\alpha) \geq 0$. To prove this, let $P = X^m + \cdots + a_0 \in F[X]$ be the minimal polynomial of α over F. Note that, by linear algebra, it can be shown that $v_K(\alpha) = \frac{1}{m}v(a_0)$. We can thus apply Proposition 3.2.1 to conclude that $P \in \mathcal{O}_F[X]$. The minimal polynomial of $1+\alpha$ is $P(X-1) \in \mathcal{O}_F[X]$ and looking at the constant coefficient, we see that $v_K(1 + \alpha) \geq 0$ as needed.
For the uniqueness, see [Gui2018]. □

Corollary 3.2.2.1 (Galois action preserves valuations)**.** Now suppose further that K/F is Galois. Then $v_K(\sigma(x)) = v_K(x)$ for all $x \in K$ and for all σ in $\mathrm{Gal}(K/F)$.

Proof. One can check, by definition of a valuation, that $x \mapsto v_K(\sigma(x))$ is valuation extending v. Then by the uniqueness assertion in the previous theorem, $v_K(\sigma(x)) = v_K(x)$. □

3.3 Ramification theory of local fields

For a local field, F, we have seen that the ring of integers $\mathcal{O}_F$ is a principal ideal domain with unique maximal ideal $\mathfrak{p}$. Since every principal ideal domain is a Dedekind domain, we have the property of unique factorization of an ideal into prime ideals. In other words, if K/F is an extension of local fields, with $\mathfrak{P}$ being the unique maximal ideal of $\mathcal{O}_K$, we have $\mathfrak{p} \cdot \mathcal{O}_L = \mathfrak{P}^e$ for some $e \in \mathbb{N}$.

Definition 3.3.1 (Ramification index)**.** For the extension K/F of local fields, the natural number e above is called the ramification index of K/F.

Definition 3.3.2 (Inertial degree)**.** For the extension K/F of local fields, we define $f = [\mathbb{K} : \mathbb{F}]$ and call it the inertial degree of K/F.

Theorem 3.3.1. Let K/F be an extension of local fields with $n = [K : F]$. Then $n = ef$.

Proof. See [Gui2018, Theorem 2.38]. □

Now suppose that K/F is also Galois. Since the Galois group acts transitively on the set of prime ideals lying over $\mathfrak{p}$, we must have $\sigma(\mathfrak{P}) = \mathfrak{P}$ as sets. Thus σ induces an isomorphism of the residue field $\mathbb{K} = \mathcal{O}_K/\mathfrak{P}$ which fixes $\mathbb{F} = \mathcal{O}_F/\mathfrak{p}$. We thus get a homomorphism: $\mathrm{Gal}(K/F) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. To see when this homomorphism is an isomorphism, we introduce the following definition:

Definition 3.3.3 (Unramified extensions)**.** An extension K/F is said to be unramified when $e = 1$.

Theorem 3.3.2. Let F be a p-adic field. For any $n \geq 1$, there exists a unique (up to isomorphism) extension L/F which is unramified such that $[L : F] = n$. Moreover, this extension is Galois and the natural map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is an isomorphism.

Proof. From Galois theory, we know that the residue field $\mathbb{F}$ has a unique (up to isomoprhism) extension $\mathbb{L}$ such that $[\mathbb{L} : \mathbb{F}] = n$. Choose $a \in \mathbb{L}$ such that $\mathbb{L} = \mathbb{F}(a)$ and let h be the minimal polynomial of a over $\mathbb{F}$. Note that $\deg h = n$. Choose a monic polynomial $P \in \mathcal{O}_F[X]$ of degree n such that $\overline{P} = h$ in $\mathbb{F}[X]$. Define $L := F(\alpha)$ where α is any root of P; we now use a counting argument to show that L/F is unramified of degree n. First note that since $\deg P = n$ and since P is not necessarily irreducible over F, $[L : F] \leq n$. On the other hand, the inertial degree $f = [\mathbb{L} : \mathbb{F}] = n$. Thus, $n \geq [L : F] = ef = en$ which forces $e = 1$ and $[L : F] = n$; so L/F is unramified of degree n.
We now turn to uniqueness. The key step in proving the uniqueness is the following:
Claim: For any extension K/F such that n divides $[\mathbb{K} : \mathbb{F}]$, there are n distinct embeddings $L \to K$.
Proof of claim: By the theory of finite fields, we know that there is a unique subfield $\mathbb{L}' \subseteq \mathbb{K}$ such that $[\mathbb{L}' : \mathbb{F}] = n$ and there is a $\mathbb{F}$ isomoprhism between $\mathbb{L}$ and $\mathbb{L}'$. Thus, $P \in \mathcal{O}_F[X]$ splits over $\mathbb{L}'$ and we can write $\overline{P} = f = (X - a_1) \cdots (X - a_n)$ in $\mathbb{L}'[X]$. Note that all the a_i's are distinct since we are working over separable extensions; we can thus apply Hensel's lemma over the field K to show that P has n distinct roots $\alpha_1, \cdots \alpha_n$ in K. The desired embeddings are then: $F[\alpha] \to K$ given by $\alpha \mapsto \alpha_i$.
Now if K/F is unramified of degree n, then $[\mathbb{K} : \mathbb{F}] = n$ so there is an isomoprhism $L \cong K$ showing uniquenss.
Finally, for $L = K$, we now know that $[L : F]$ has n distinct automorphisms. However, $[L : F] = n$ as well and so the extension is Galois. Any element $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is determined by $\sigma(a)$, which must be one $a_1, \ldots, a_n$ (viewed as elements of $\mathbb{L}$), say $\sigma(a_i)$. The automorphism of L mapping α to α_i induces σ

so $\mathrm{Gal}(K/F) \to \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is surjective and it is also injective since both groups have the same size.

□

Once we fix an algebraic closure $\overline{F}$ of F, we have the following stronger statement:

Corollary 3.3.2.1. We have the following $1:1$ correspondence:
$\{\text{unramified extensions } L/F \text{ with } L \subseteq \overline{F}\} \xleftrightarrow{1:1} \{\text{finite extensions } \mathbb{L}/\mathbb{F} \text{ with } \mathbb{L} \subseteq \overline{\mathbb{F}}\}$ given by associating each unramified extension L to its residue field $\mathbb{L}$.

Proof. Suppose two unramified extensions L_1 and L_2 have the same residue field $\mathbb{L}$. We know from the previous theorem that $L_1 \cong L_2$ as fields. By the isomorphism extension theorem, there exists an automorphism σ of $\overline{F}$ such that $\sigma(L_1) = L_2$; however both L_1 and L_2 are Galois, so we must have $L_1 = L_2$. Surjectivity follows from our construction of unramified extensions. □

Corollary 3.3.2.2. Suppose that L/F is an unramified extension. Then $\mathrm{Gal}(L/F)$ is cyclic, generated by a canonical element ρ called the Frobenius element. This element is characterized by the congruence $\rho(x) \equiv x^q \bmod \mathfrak{P}$ for all $x \in \mathcal{O}_L$ where $\mathfrak{P}$ is the maximal ideal of $\mathcal{O}_L$ and q is the size of the residue field $\mathbb{L}$.

Proof. On one hand, we know that the Galois group of a finite extensions of finite fields is cyclic and generated by the Frobenius map $x \mapsto x^q$; on the other hand the theorem tells us that $\mathrm{Gal}(L/F) \cong \mathrm{Gal}(\mathbb{L}/\mathbb{F})$ as groups. The corollary thus follows. □

The next proposition tells us that in fact we have a very concrete way to construct unramified extensions:

Theorem 3.3.3. Let F be a p-adic field with residue field $\mathbb{F}$, let N be an integer with $(N, p) = 1$ and let $K = F(\zeta_N)$. Then K/F is unramified of degree f, where f is the smallest integer such that $q^f \equiv 1 \bmod N$ with $q = |\mathbb{F}|$.

Proof. See [Gui2018, Proposition 2.46]. □

Thus, we can now work backwards: starting with $n \in \mathbb{N}_{\geq 1}$, set $N = q^n - 1$ which thus does not divide $q^{n'} - 1$ for $n' < n$. Then $F(\zeta_N)$ is the unique unramified extension of degree n.

3.4 Multiplicative structure of local fields

Let F be a p-adic field. In this section, we will describe the structure of $F^\times$.

Definition 3.4.1 (Unit groups)**.** Define $U_F^{(0)} = \mathcal{O}_F^\times$ and for $s \geq 1$, define $U_F^{(s)} := \{x \in \mathcal{O}_F : x \equiv 1 \bmod \mathfrak{p}^s\}$.

Observe that we have an exact sequence of abelian groups:

$$1 \to \mathcal{O}_F^\times \hookrightarrow F^\times \twoheadrightarrow \mathbb{Z} \to 1$$

This sequence in fact splits: We can define a map $s : \mathbb{Z} \to F^\times$ by setting $s(n) = \pi^n$, where π is any element of valuation 1. By the splitting lemma, we thus have $F^\times \cong \mathcal{O}_F^\times \times \mathbb{Z}$.

We also have the following exact sequence:

$$1 \to U_F^{(1)} \hookrightarrow \mathcal{O}_F^\times \twoheadrightarrow \mathbb{F}^\times \to 1$$

This sequence also splits: the polynomial $f(X) = X^{q-1} - 1 \in \mathcal{O}_F[X]$ splits into distinct linear factors when reduced in $\mathbb{F}[X]$, so by Hensel's lemma f is split in $\mathcal{O}_F[X]$. Thus $\mathcal{O}_F^\times = U_F^{(1)} \times \mathbb{F}^\times$ and so $F^\times \cong U_F^{(1)} \times \mathbb{F}^\times \times \mathbb{Z} \cong U_F^{(1)} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}$, where q is the size of the residue field of $\mathbb{F}$. Thus, to describe the structure of $F^\times$, it remains to to describe the structure of $U_F^{(1)}$. The following proposition answers our question:

Proposition 3.4.1. The group $U_F^{(1)}$ is isomorphic to $\mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$, where $d = [F : \mathbb{Q}_p]$ and $a \in \mathbb{N}$ is some natural number.

Proof. See [Gui2018, Proposition 4.7]. □

As a result, we can give a description of the group $F^\times$ via the next theorem. Note that this theorem not only gives an isomorphism between groups but also a homeomorphism with the discrete topology employed on $\mathbb{Z}$ and the cyclic groups.

Theorem 3.4.1. The group $F^\times$ is topologically isomorphic to $\mathbb{Z} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$, where q is the size of the residue field $\mathbb{F}$, $a \in \mathbb{N}$ is some natural number and $d = [F : \mathbb{Q}_p]$. Moreover, under this identfication, we have:

- The map $v : F^\times \to \mathbb{Z}$ corresponding to the projection on the first factor is the normalized valuation
- The subgroup $\{0\} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ corresponds to $\mathcal{O}_F^\times$
- The subgroup $\{0\} \times \{0\} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d$ corresponds to $U_F^{(1)}$.

- The subgroup $\{0\} \times \mathbb{Z}/(q-1)\mathbb{Z} \times \mathbb{Z}/p^a \times \{0\}$ corresponds to the roots of unity contained in F.

Proof. See [Gui2018, Theorem 4.8]. □

We now use this result to obtain several results that will be useful later in the report when dealing with the proofs of local class field theory.

A special case of the above theorem is the following:

Proposition 3.4.2. When $F = \mathbb{Q}_p$ and p is odd, we have $a = d = 1$. As a result, $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/(q-1) \times \mathbb{Z}_p$. When $p = 2$, $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$.

Proof. See [Gui2018, Example 4.9]. □

The next result pertains to the index of the subgroup $(F^\times)^n \subseteq F^\times$.

Corollary 3.4.1.1. For any $n \in \mathbb{N}_{\geq 1}$, the subgroup $(F^\times)^n \subseteq F^\times$ has finite index in $F^\times$ and in fact, this index equals $n \cdot |\mu_n(F)| \cdot p^{dr}$, where $n = p^r m$ with $(m, p) = 1$, and $\mu_n(F)$ is the group of nth roots of unity contained in F.

Proof. By the theorem, we have $F^\times \cong \mathbb{Z} \times \mu(F) \times \mathbb{Z}_p^d$, where $\mu(F)$ is the group of all roots of unity contained in F. Note that it suffices to compute the relevant indices individually. Firstly, the index of $n\mathbb{Z}$ in $\mathbb{Z}$ is n. Secondly, the map $\mu(F) \to \mu(F)$ by setting $x \mapsto x^n$ has kernel $\mu_n(F)$. Thus, by the first isomoprhism theorem, the index of $\mu(F)^n$ is $|\mu_n(F)|$. Finally, since m is invertible in $\mathbb{Z}_p$, we have $m\mathbb{Z}_p = \mathbb{Z}_p$ and so $n\mathbb{Z}_p = p^r\mathbb{Z}_p$. Thus the index of $n\mathbb{Z}_p^d$ in $\mathbb{Z}_p^d$ is p^{dr}. □

Corollary 3.4.1.2. The following hold:

1. Any subgroup of finite index of $F^\times$ is closed, hence open.
2. Any open subgroup of $F^\times$ contains a subgroup $U_F^{(n)}$ for some n
3. Any subgroup of finite index in $F^\times$ contains a subgroup of the form $\langle \pi^m \rangle \times U_F^{(n)}$ for some $n, m \in \mathbb{N}$.

Proof. We only prove (1) and (3); the proof of (2) can be found in [Gui2018, Lemma 4.11].

1. We will use the fact that if H is a subgroup of the topological group G, and if H contains a closed subgroup U of finite index in G, then H is itself closed; indeed H is the union of finitely many cosets of U each of which are closed. Now let H be a subgroup of finite index in $F^\times$. Set $G = F^\times$ and put $U = (F^\times)^n$, so $U \subseteq H$. From the previous corollary, we know that U

has finite index in G and so to apply the fact, we need to show that U is closed in G. Since Z and $\mu(F)$ are both equipped with the discrete topology, multiplication by n has a closed image on $\mathbb{Z}$ and $\mu(F)$. Multiplication by n also has a closed image on $\mathbb{Z}_p$ due to compactness of $\mathbb{Z}_p$. Hence, by Theorem $3.4.1$, U is closed as desired. Finally, since U is closed and has finite index, U must be open.

2. Let H be a subgroup of finite index in $F^\times$. By (1), we know that H is open and by (2) it contains a subgroup of the form $U_F^{(n)}$ for some n. The image of H in the valuation group must be $m_0\mathbb{Z}$ for some $m_0 > 0$, since the index of H is finite. Thus, H contains some element of the form $\pi^{m_0}u$, where $u \in \mathcal{O}_F^\times$. Let k be an integer such that $u^k \in U_F^{(n)} \subseteq H$. Let $m = km_0$ and so H contains $(\pi^{m_0}u)^k = \pi^m u^k$. Thus, $\pi^m \in H$ and so H contains both $\langle \pi^m \rangle$ and $U_F^{(n)}$. By Theorem $3.4.1$, these subgroups intersect trivially, so H contains $\langle \pi^m \rangle \times U_F^{(n)}$.

□

Using the above corollary, we see that in the case of p-adic fields, the term "open" in the existence theorem of local class field theory (Theorem 2.2.2) is unnecessary; since in this report, we only focus on p-adic fields, we will thus prove the existence theorem in this version.

Corollary 3.4.1.3. If $A \subseteq F^\times$ is a divisible subgroup, then A is trivial.

Proof. One checks that a divisible subgroup of a cyclic group is trivial. The same is true for $\mathbb{Z}_p$ as an element infintely divisble by p must have infinite valuation and so must be 0. By Theorem 3.4.1, A is trivial since its various projections on the given factors are trivial. □

Chapter 4

The Brauer group

In this chapter we introduce the Brauer group, an object of great importance in modern number theory. To define the Brauer group, we need some concepts from non-commutative ring theory to which we turn now.

4.1 Some background on non-commuative ring theory

Throughout this chapter, rings are possibly non-commutative unless otherwise stated. We begin by introducing some definitions. Let A be any ring.

Definition 4.1.1. The center of A denoted $\mathcal{Z}(A) = \{z \in A | xz = zx \text{ for all } x \in A\}$.

Definition 4.1.2. Let F be a commutaive ring. We say that A is an algebra over F when there is a ring homomorphism $\iota : F \to A$ such that $\iota(F) \subseteq \mathcal{Z}(A)$

Definition 4.1.3. Let F be a field. We say that a ring A is a central algebra over F, when $\mathcal{Z}(A) \cong F$ and when A is finite dimensional over F as an F-vector space. We furthemore say that A is simple when it has no non-trivial two-sided ideals.

The next definition captures the notion of a "not necessarily commutative field".

Definition 4.1.4. A ring K is called a skewfield when every non-zero element of K has a two-sided inverse: for every $x \in K$ there exists an element $x^{-1} \in K$ such that $xx^{-1} = x^{-1}x = 1$.

Example 4.1.1. Every field is a skewfield. The quaternions, which we denote by $\mathbb{H}$, is another example of a skewfield.

We remark that if F is a local field and K is a skwefield containing F, Theorem 3.2.2 still holds by replacing $N_{K/F}(\alpha)$ by $\det(m_\alpha)$, where m_α is the multiplication by α map. We shall use this fact later on in the report.

Definition 4.1.5. Let A be a ring with multiplication written $a \cdot b$ for $a, b \in A$. The opposite ring A^{op} is the same underlying group endowed with a new multiplication $a \star b$, defined by $a \star b := b \cdot a$

Example 4.1.2. Note that A is commutative if and only if $A = A^{\mathrm{op}}$. We also have $M_n(F) \cong M_n(F)^{\mathrm{op}}$ as rings via the transpose map: $M \mapsto M^T$. However, the isomorphism is no longer true if we replace F by a skewfield K since the identity $(MN)^T = N^T M^T$ is not valid in a non-commutative setting.

Theorem 4.1.1 (Classification theorem for central simple F-algebras)**.** The following are equivalent:

1. A is a central simple F-algebra.
2. $A \cong M_n(K)$ where K is a skewfield finite dimensional over F and with $\mathcal{Z}(K) = F$.

Moreover, n and K are uniquely determined above.

Proof. See [Gui2018, Theorem 5.48] □

Definition 4.1.6 (Brauer equivalence)**.** We say that A is Brauer equivalent to a skewfield K when $A \cong M_n(K)$ for some $n \geq 1$. If B is another central simple finite dimensional F-algebra, we say that A is Brauer equivalent to B if both A and B are Brauer equivalent to the same K. Denote the Brauer equivlence class of A by $[A]$.

4.2 Defining the Brauer group

We are now eqiuipped to define the Brauer group for any field F:

- Underlying set: $\mathrm{Br}(F) = \{[A] : A \text{ finite dimensional central simple algebra over F}\}$
- Group operation: $[A] \cdot [B] = [A \otimes_F B]$

- Well-defined: Firstly, we need to check that $A \otimes_F B$ is indeed a central simple F-algebra; for this we refer to [Gui2018, Theorem 6.11 & Lemma 6.16]. Secondly, we need to check that the operation is independent of the choice of representatives of $[A]$ and $[B]$; for this we refer to [Gui2018, Lemma 6.18].

- Associativity: This follows from assoociativity of the tensor product.

- Identity: Note that $A \otimes_F F \cong A$ as F-algebras via the map $a \otimes_F f \mapsto fa$. Thus the isomorphism class $[F]$ is the identity element under this group operation.

- Inverses: To prove the existence of the inverse element, we will prove the following theorem:

  Theorem 4.2.1. Let K be a skewfield, let $F = \mathcal{Z}(K)$ and let $n = [K : F]$. Then $K \otimes_F K^{\mathrm{op}} \cong M_n(F)$.

  Proof. K acts on itself by both left and right multiplication, so K is both a left K-module and a right K-module. Moreover, note that the two operations commute and also that that the right action can be seen as a structure of a K^{op}-module. Thus, K is a $K - K^{\mathrm{op}}$ bimodule or, equivalently, a $K \otimes K^{\mathrm{op}}$ module. Since $F = \mathcal{Z}(K)$, each element of $K \otimes K^{\mathrm{op}}$ gives an F-linear map of the n-dimensional vector space K, hence an F-algebra homomorphism $f : K \otimes K^{\mathrm{op}} \to M_n(F)$. Now $K \otimes K^{\mathrm{op}}$ is simple (see [Gui2018, Theorem 6.11]) and so $\ker f$ must be zero. Thus f is injective and since the dimensions match, f is also surjetcive. □

  Now, if A is Brauer equivalent to K, then A^{op} is Brauer equivalent to K^{op}. Thus, the theroem yields $[A][A^{\mathrm{op}}] = [K][K^{\mathrm{op}}] = [K \otimes_F K^{\mathrm{op}}] = [F]$ and so $[A]^{-1} = [A^{\mathrm{op}}]$.

4.3 Examples of the Brauer group

In this section, we state the Brauer groups of well-known fields.

Theorem 4.3.1 (Brauer group of an algebraically closed field)**.** If F is algebraically closed, Br(F) is trivial.

Proof. Pick any $[A] \in \mathrm{Br}(F)$ and let K be the unique skewfield such that $[A] = [K]$. Pick any $x \in K$ and consider the subring $F[x]$ of K. Since $F[x]$ is an integral

domain, the multiplication map by any non-zero element $y \in F[x]$ is injective. Moreover, since $F[x]$ is finite dimensional over F, the map is also surjective. Thus $F[x]$ is a field. Morover, using the fact that $F[x]$ is finite dimensional over F, we see that $F[x]$ is algebraic over F. Since F is algebraically closed, $F[x] = F$ and so $x \in F$. Thus $K = F$ and $[A] = [K] = [F]$ in Br(F). □

Our next two examples are classical results and we state them without proof.

Theorem 4.3.2 (Wedderburn's little theorem)**.** If $F = \mathbb{F}_p$ is the finite field of p elements, then Br(F) is also trivial.

Proof. See [Gui2018, Theorem 6.32]. □

Theorem 4.3.3. If $F = \mathbb{R}$ is the field of real numbers, then Br(F) $= \{[\mathbb{R}], [\mathbb{H}]\}$ and so Br(F) $\cong \mathbb{Z}/2\mathbb{Z}$.

Proof. See [Gui2018, Example 7.23]. □

A natural question at this stage would be to compute the Brauer group of a local field. This computation is one of the key results in local class field theory. However, we will only be able to compute this group in Chapter 6 once we have developed the notions of group cohomology. We end this chapter by introducing an important subgroup of the Brauer group.

4.4 Relative Brauer group

Proposition 4.4.1 (Maps between Brauer groups)**.** Let E/F be any field extension. The operation $[A] \mapsto [A \otimes_F E]$ is well defined and is a group homomorphism from Br(F) to Br(E).

Proof. See [Gui2018, Lemma 6.24]. □

Definition 4.4.1 (Relative Brauer group)**.** Conisder the homomorphism defined in the lemma above. Its kernel is written Br(E/F) and is called the relative Brauer group of the extension E/F.

The next proposition gives us the connection between the Brauer group and the relative Brauer group:

Proposition 4.4.2. Fix an algebraic closure $\overline{F}$ of F. Then the Brauer group $\mathrm{Br}(F) = \varinjlim \mathrm{Br}(E/F)$, where the direct limit runs through all fields E such that $F \subseteq E \subseteq \overline{F}$ and E/F is finite Galois.

Proof. See [Gui2018, Theorem 6.42 & Example 7.33]. □

We now turn to introducing the theory of group cohomology which will shed further light on the Brauer and the relative Brauer groups.

Chapter 5

Group cohomology

In this chapter, we introduce the machinery of group cohomology. This chapter is one of the most technical parts of the report but nonetheless is very useful later on in the report.

5.1 Tate cohomology groups

In this section, we define the Tate cohomology groups which play an important role in class field theory. Standard homological algebra and particularly background on the Ext and Tor groups is assumed. Let G be a finite group and M be a $\mathbb{Z}[G]$-module. Let $\mathbb{Z}$ be the trivial $\mathbb{Z}[G]$-module i.e. $g \cdot r = r$ for all $g \in G$ and for all $r \in \mathbb{Z}$.

Definition 5.1.1. The cohomology groups of G with coeffcients in M are $H^n(G, M) = \mathrm{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, M)$.

Definition 5.1.2. The homology groups of G with coeffcients in M are $H_n(G, M) = \mathrm{Tor}^{\mathbb{Z}[G]}_n(\mathbb{Z}, M)$.

Thus, to compute the cohomology groups of G with coefficients in M, we need to take a projective resolution P_* of $\mathbb{Z}$ as a trivial $\mathbb{Z}[G]$-module and compute the cohomology groups of the cochain complex $\mathrm{Hom}_{\mathbb{Z}[G]}(P_*, M)$. To compute the homology groups of G with coefficients in M, we need to a projective resolution Q_* of M and then compute the homology groups of the chain-complex $\mathbb{Z} \otimes_{\mathbb{Z}[G]} Q_*$. However, there is an alternative option available for computing the homology groups of G with coefficients in M: we can take a projective resolution P_* of $\mathbb{Z}$ and compute the homology groups of the chain complex $P_* \otimes_{\mathbb{Z}[G]} M$.

We now proceed to motivate the definition of the Tate cohomology group. Let $G =: C_r = \{1, T, \ldots, T^{r-1}\}$ be a cyclic group of order r generated by an element T. One checks, see [Gui2018, Example 9.13] for details, that

$$\cdots \xrightarrow{1-T} \mathbb{Z}[C_r] \xrightarrow{N} \mathbb{Z}[C_r] \xrightarrow{1-T} \mathbb{Z}[C_r] \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0$$

is a projective resolution for $\mathbb{Z}$, where $N = 1 + T + \cdots + T^{r-1}$ and ϵ is the $\mathbb{Z}[G]$-module homomorphism such that $\epsilon(T) = 1$. In any degree of the projective resolution, the nth projective module P_n is just $\mathbb{Z}[C_r]$, so $\mathrm{Hom}_{\mathbb{Z}[G]}(P_n, M) \cong M$ as $\mathbb{Z}[G]$-modules. Thus, our cochain complex looks like:

$$0 \longrightarrow M \xrightarrow{1-T} M \xrightarrow{N} M \xrightarrow{1-T} \cdots$$

Thus, for $n > 0$, $H^{2n}(C_r, M) = M^G/N(M)$ with $M^G = \{m \in M | g \cdot m = m \text{ for all } g \in G\}$ and $N(M) = \{N \cdot m | m \in M\}$.

For the odd cohomology groups, we have for $n \geq 0$, $H^{2n+1}(C_r, M) = N_M/\mathrm{im}\ (1-T)$, where $N_M = \{m \in M | N \cdot m = 0\}$. We claim that $\mathrm{im}\ (1-T) = M'$ where $M' = \langle m - g \cdot m | m \in M, g \in G \rangle$. The containment "$\subseteq$" is easy to check; for the other containment pick $m - T^k m \in M'$. Then $(1-T)(m + T \cdot m + \cdots + T^{k-1}m) = m - T^k m$, so we have shown the other containment as well. Thus, $H^{2n+1}(C_r, M) = N_M/M'$.

We now proceed to compute the homology groups using the alternate method described above. Firstly, since $P_n = \mathbb{Z}[G]$ for all $n \in \mathbb{N}$, $P_n \otimes_{\mathbb{Z}[G]} M \cong M$. Thus, our chain complex is as follows:

$$\cdots \to M \xrightarrow{1-T} M \xrightarrow{N} M \xrightarrow{1-T} M \longrightarrow 0$$

Hence, for $n > 0$, $H_{2n}(C_r, M) \cong N_M/M'$ and for $n \geq 0$ $H_{2n+1}(C_r, M) \cong M^G/N(M)$.

The similarity between the homology and cohomology groups in the case of a cyclic group was the original motivation that led Tate to introduce the following definition:

Definition 5.1.3 (Tate cohomology groups)**.** Let M be a $\mathbb{Z}[G]$-module. The Tate cohomlogy groups of G with coefficients in M are denoted by $\hat{H}^n(G, M)$ for $n \in \mathbb{Z}$ and are defined by:

$$\hat{H}^n(G, M) = \begin{cases} H^n(G, M) & \text{if } n \geq 1 \\ M^G/N(M) & \text{if } n = 0 \\ N_M/M' & \text{if } n = -1 \\ H_{-(n+1)}(G, M) & \text{if } n \leq -2 \end{cases}$$

Here, as above, $N(M) = \{N \cdot m | m \in M\}$ and $N_M = \{m \in M | N \cdot m = 0\}$, where $N = \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$. Also, $M^G = \{m \in M | \sigma \cdot m = m \text{ for all } \sigma \in G\}$ and $M' = \langle m - \sigma \cdot m : m \in M, \sigma \in G \rangle$.

Our first observation about Tate cohomology groups is the following:

Proposition 5.1.1 (Periodicity of Tate cohomology when G is cyclic)**.** When G is cyclic, $\hat{H}^{2n}(G, M) = M^G/N(M)$ and $\hat{H}^{2n+1}(G, M) = N_M/M'$ for all $n \in \mathbb{Z}$.

Proof. This follows from the work done above. □

We conclude this section by remarking that we also have a version of the long-exact sequence for Tate cohomology:

Proposition 5.1.2 (Long exact sequences in Tate cohomology)**.** If : $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ is a short exact sequence of $\mathbb{Z}[G]$-modules, then we get the following long exact sequence of Tate cohomology groups:

$$\cdots \longrightarrow \hat{H}^n(G, A) \longrightarrow \hat{H}^n(G, B) \longrightarrow \hat{H}^n(G, C) \longrightarrow \hat{H}^{n+1}(G, A) \longrightarrow \hat{H}^{n+1}(G, B) \cdots$$

Proof. See [Gui2018, Proposition 10.21]. □

5.2 Shapiro's Lemma & its applications

In this section, we state a well-known lemma in group cohomology called Shapiro's lemma. We use this lemma to extract more knowledge about the Tate cohomology groups. The setting for this section is as follows: we let G be a finite group, $H \subseteq G$ a subgroup, M a $\mathbb{Z}[G]$-module and A a $\mathbb{Z}[H]$-module.

Definition 5.2.1. The induced $\mathbb{Z}[G]$-module written $\mathrm{Ind}_H^G(A)$ is the group $\mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)$. It is viewed as a $\mathbb{Z}[G]$-module, where the action of $\sigma \in G$ on $f \in \mathrm{Ind}_H^G(A)$ is given by $(\sigma \cdot f)(x) = f(x\sigma)$.

Lemma 5.2.1 (Alternative description of the induced group)**.** There is an isomorphism $\mathrm{Ind}_H^G(A) \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A$ with G action given by $\sigma \cdot (g \otimes a) = \sigma g \otimes a$.

Proof. See [Gui2018, Lemma 12.3]. □

Lemma 5.2.2. Let M be a $\mathbb{Z}[G]$-module and let H be a subgroup of G. Then there is an injective homomorphism $M \to \mathrm{Ind}_H^G(M)$ mapping $m \in M$ to $f : \mathbb{Z}[G] \to M$ with $f(\sigma) = \sigma \cdot m$.

Proof. The kernel of this homomorphism is trivial since for all $m \in M \setminus \{0\}$, $f(1) = m \neq 0$. □

Theorem 5.2.3 (Shapiro's lemma)**.** For each $n \in \mathbb{N}$, we have the following isomorphism of groups: $H^n(G, \mathrm{Ind}_H^G(A)) \cong H^n(H, A)$ and $H_n(G, \mathrm{Ind}_H^G(A)) \cong H_n(H, A)$.

Proof. See [Gui2018, Proposition 12.5]. □

The first statement that Shapiro's lemma allows us to make regarding Tate cohomology groups is the following:

Proposition 5.2.1. Let M be a $\mathbb{Z}[G]$-module which is induced from the trivial subgroup of G, that is, $M \cong \mathrm{Ind}_{\{e\}}^G(A)$ for some abelian group A. Then $\hat{H}^n(G, M) = 0$ for all $n \in \mathbb{Z}$.

Proof. By Shapiro's lemma, we have $H^n(G, M) \cong H^n(\{e\}, A)$; now $H^n(\{e\}, A) = 0$ for $n > 0$ and so for $n > 0$ we have that $H^n(G, M) = 0$ as well. Similarly, $H_n(G, M) = 0$ for $n > 0$. Thus, by definition of the Tate cohomology groups, we have shown that $\hat{H}^n(G, M) = 0$ for all n except $n = 0$ and $n = -1$. These two remaining cases are treated directly, see [Gui2018, Corollary 12.6] for details.
□

Proposition 5.2.2. Suppose G is a finite group and P is a projective $\mathbb{Z}[G]$-module. Then $\hat{H}^n(G, P) = 0$ for all $n \in \mathbb{Z}$.

Proof. Since P is projective, there exists a $\mathbb{Z}[G]$-module Q such that $P \oplus Q$ is free. Since $\hat{H}^n(G, P \oplus Q) \cong \hat{H}^n(G, P) \oplus \hat{H}^n(G, Q)$, it suffices to prove the proposition when P is free; moreover, for similar reasons we can assume $P = \mathbb{Z}[G]$ is the regular $\mathbb{Z}[G]$-module itself.
By Lemma 5.2.1, $\mathrm{Ind}_{\{e\}}^G(\mathbb{Z}) \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}[G] = P$. Thus, P is induced from the trivial subgroup of G and by the previous proposition, we have $\hat{H}^n(G, P) = 0$ for all $n \in \mathbb{Z}$. □

Proposition 5.2.3 (Dimension shifting)**.** Let M be a $\mathbb{Z}[G]$-module. Then:

1. We can embed M as a submodule of a module M' with trivial Tate cohomology and express M as a quotient of a module M'' with trivial Tate cohomology.

2. For any $k \in \mathbb{Z}$, we can find a $\mathbb{Z}[G]$-module $M(k)$ such that

$$\hat{H}^n(G, M) \cong \hat{H}^{n+k}(G, M(k))$$

.

Proof. We make use of the propositions above:

1. Let M' be the $\mathbb{Z}[G]$-module given by Lemma 5.2.2 with $H = \{e\}$; M' has trivial Tate cohomology by Proposition 5.2.1. Let M'' be the free $\mathbb{Z}[G]$-module on M; M'' has trivial Tate cohomology by Proposition $5.2.2$.

2. Conisder the short exact sequence of $\mathbb{Z}[G]$-modules:

$$0 \to M \hookrightarrow M' \twoheadrightarrow M'/M \to 0$$

which induces the following long exact sequence in Tate cohomology:

$$\begin{aligned} 0 \longrightarrow \cdots \longrightarrow \hat{H}^{n-1}(G, M) &\longrightarrow \hat{H}^{n-1}(G, M') \longrightarrow \hat{H}^{n-1}(G, M'/M) \\ \longrightarrow \hat{H}^{n}(G, M) &\longrightarrow \hat{H}^{n+1}(G, M') \quad \longrightarrow \hat{H}^{n}(G, M'/M) \to \cdots \end{aligned}$$

Since $\hat{H}^n(G, M') = 0$ for all $n \in \mathbb{Z}$ by (1), $\hat{H}^n(G, M) \cong \hat{H}^{n-1}(G, M'/M)$ for all $n \in \mathbb{Z}$. Similarly, if we consider the exact sequence $0 \to K \to M'' \to M \to 0$ where K is the kernel of the map $M'' \twoheadrightarrow M$, we obtain $\hat{H}^n(G, M) \cong \hat{H}^{n+1}(G, K)$ for all $n \in \mathbb{Z}$. Thus, we can shift indices both to the left and the right; by doing this $|k|$ times depending on the sign of k, we find our desired module $M(k)$. □

The next lemma is a refinement of the previous proposition and allows us to perform dimension shifting on all subgroups of G simaltaneosly.

Lemma 5.2.4. Suppose G is a finite group and M is $\mathbb{Z}[G]$-module. Let $r \in \mathbb{Z}$ be an integer. Then there exists a $\mathbb{Z}[G]$-module $M(-r)$ with $\hat{H}^n(S, M(-r)) = \hat{H}^{n+r}(S, M)$ for all $n \in \mathbb{Z}$ and any subgroup S of G.

Proof. Consider any subgroup S of G. Recall from the proof above that to shift to the left, we use the module $M' = \mathrm{Ind}_{\{e\}}^{G}(M)$. Using the fact (see [Gui2018, Corollary 12.31]) that M', when viewed as a $\mathbb{Z}[S]$-module, is a direct sum of $[G : S]$ copies of $\mathrm{Ind}_{\{e\}}^{S}(M)$, we have that $H^n(S, M') = 0$ for all $n \in \mathbb{Z}$ by Proposition 5.2.1. Thus, we can shift to the left for all subgroups at the same time. To shift to the right, we used M'', the free $\mathbb{Z}[G]$-module on M. This is also a free $\mathbb{Z}[S]$-module, so in this case as well, the shift works for all subgroups at the same time. □

5.3 The standard resolution

Let G be a finite group and M be a $\mathbb{Z}[G]$-module. In this section, our goal is to describe the standard resolution, a particular projective resolution of $\mathbb{Z}$ as

a trivial $\mathbb{Z}[G]$-module. As we proceed to show, the benefit of using the standard resolution is that it gives us alternative formulas for computing cohomology groups. First, set $R := \mathbb{Z}[G]$. Define $R^{\otimes n} := \underbrace{R \otimes \cdots \otimes R}_{\text{n times}}$. Next, define boundary maps $\partial_n^i : R^{\otimes n+1} \to R^{\otimes n}$ by setting $\partial_n^{(i)}(\sigma_0 \otimes \cdots \otimes \sigma_n) = \sigma_0 \otimes \cdots \otimes \hat{\sigma_i} \otimes \cdots \otimes \sigma_n$. Now set $\partial_n = \sum_{i=0}^{n}(-1)^i \partial_n^{(i)}$. A calculation shows that $\partial_{n-1} \circ \partial_n = 0$. We thus obtain a chain complex $(R^{\otimes *+1}, \partial_*)$. We introduce the notation: $[\sigma_1|\sigma_2|\cdots|\sigma_n] := 1 \otimes \sigma_1 \otimes \sigma_1\sigma_2 \otimes \cdots \otimes \sigma_1\sigma_2\cdots\sigma_n \in R^{\otimes n+1}$. Our next claim is the following:

Lemma 5.3.1. The elements $[\sigma_1|\cdots|\sigma_n]$ form a basis of the R-module $R^{\otimes n+1}$ which is free of finite rank $|G|^n$.

Proof. See [Gui2018, Lemma 10.9]. □

Lemma 5.3.2. The sequence

$$\cdots \to R \otimes R \otimes R \xrightarrow{\partial} R \otimes R \xrightarrow{\partial} R \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0,$$

where $\epsilon : R \to \mathbb{Z}$ is such that $\epsilon(\sigma) = 1$ for all $\sigma \in G$, is exact.

Proof. See [Gui2018, Lemma 10.8]. □

The previous two lemmas together show that we have constructed a projective resolution of $\mathbb{Z}$ which we call the standard resolution. To demonstrate the utility of the standard resolution, we note that it may be used to prove the following proposition:

Proposition 5.3.1. There is an isomorphism $H_1(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$, where G^{ab} is the abelianization of G.

Proof. See [Gui2018,Lemma 10.20]. □

As mentioned, we can also use this to give alternative ways of computing the cohomology groups. We first introduce the following definition:

Definition 5.3.1 (Homogeneous cochains)**.** Let M be a $\mathbb{Z}[G]$-module. For $n \geq 0$, define $C^n(G, M)$ to be the group of map of sets: $f : G^{n+1} \to M$ satisfying $f(\sigma\sigma_0, \ldots, \sigma\sigma_n) = \sigma \cdot f(\sigma_0, \ldots, \sigma_n)$. The elements of $C^n(G, M)$ are called homogeneous cochains for G of degree n with values in M. We also define $d^n : C^n(G, M) \to C^{n+1}(G, M)$ by:

$$d^n(f)(\sigma_0, \ldots, \sigma_{n+1}) = \sum_{i=0}^{n+1}(-1)^i f(\sigma_0, \ldots, \hat{\sigma_i}, \ldots \sigma_{n+1}).$$

Put $Z^n(G, M) = \ker\,(d^n)$ and $B^n(G, M) = \mathrm{Im}\,(d^{n-1})$ and call them the group of cocyles and coboundaries respectively.

Proposition 5.3.2. The quotient $Z^n(G,M)/B^n(G,M)$ is isomorphic to $H^n(G,M)$.

Proof. We compute the cohomology groups using the standard resolution. Our cochain complex looks like:

$$0 \to \cdots \to \mathrm{Hom}(R^{\otimes n}, M) \to \mathrm{Hom}(R^{\otimes n+1}, M) \to \cdots$$

Note that $\mathrm{Hom}(R^{\otimes n+1}, M) \cong C^n(G,M)$ since a map $f : R^{\otimes n+1} \to M$ is completely determined by the values $f(\sigma_0 \otimes \cdots \otimes \sigma_n)$ where $\sigma_i \in G$. Note that the boundary maps are also precisely the ones in the definition; the proposition thus follows. □

We can use the formulas that we obtained for group cohomology to deduce several functorial properties of the cohomology group.

When $h : M_1 \to M_2$ is a homomorphism of $\mathbb{Z}[G]$-modules, the map $h' : C^n(G,M_1) \to C^n(G,M_2)$ defined by $h'(c) = h \circ c$ is comptaible with the boundary operator and induces a map $H^n(G,M_1) \to H^n(G,M_2)$.

Similarly, when $\phi : H \to G$ is a homomorphism of groups then the map $\phi' : C^n(G,M) \to C^n(H,M)$ defined by $\phi'(c) = c \circ \phi$ is compatible with the boundary operator and induces a map $H^n(G,M) \to H^n(H,M)$.

We now give names to some special cases of the above:

Definition 5.3.2 (Restriction)**.** When H is a subgroup of G, the induced map $H^n(G,M) \to H^n(H,M)$ is called the restriction map and is denoted by Res.

We can also go in the reverse direction. Let H be a normal subgroup of G; then M^G can be equipped with a well-defined action from $G/H : \overline{g} \cdot m := g \cdot m$.

Definition 5.3.3 (Inflation)**.** The quotient homomorphism $G \twoheadrightarrow G/H$ induces a homomoprhism $H^n(G/H, M^G) \to H^n(G, M^G)$ which when composed with the map $H^n(G,M^G) \to H^n(G,M)$ yields the inflation map $\mathrm{Inf}\colon H^n(G/H,M^G) \to H^n(G,M)$.

Definition 5.3.4 (Corestriction)**.** Let H be a subgroup of G so that $M^G \subseteq M^H$. Let T be a transversal set of H in G *i.e.* $T \subseteq G$ is a subset of G such that G is the disjoint union of the cosets Ht for $t \in T$. Define a map $f : M^H \to M^G$ by $f(m) = \sum_{\sigma \in T} \sigma \cdot m$. This map is well defined (independent of the choice of the transversal set T) and is known as the corestriction map in degree 0. By dimension shifting (see [Gui2018, Definition 12.8] for details), we can extend this map to all degrees to get a map $\mathrm{Cores} : H^n(H,M) \to H^n(G,M)$.

We now proceed to state some important exact sequences concerning the above definitions.

Proposition 5.3.3 (Restriction-inflation exact sequence)**.** Let H be a normal subgroup of G. Let $n \in \mathbb{N}_{\geq 1}$ and suppose $H^i(H, M) = 0$ for all $1 \leq i \leq n-1$. Then we have an exact sequence:

$$0 \to H^n(G/H, M^H) \xrightarrow{\text{Inf}} H^n(G, M) \xrightarrow{\text{Res}} H^n(H, M)$$

Proof. See [Sha Proposition 1.8.11] . □

Lemma 5.3.3. When H is normal in G, there is an exact sequence:

$$\hat{H}^0(H, M) \xrightarrow{Cor} \hat{H}^0(G, M) \to \hat{H}^0(G/H, M^H) \to 0$$

Noting that $(M^H)^{G/H} = M^G$, the second map is defined to be the map induced by the identity.

Proof. See [Gui2018, Lemma 12.32]. □

5.4 Tate's theorem

In this section, our main goal will be to prove Tate's theorem; we will use this theorem later in the report to prove the Reciprocity theorem. Let us begin with the following definition:

Definition 5.4.1. A $\mathbb{Z}[G]$-module M is said to be cohomologically trivial if $\hat{H}^r(S, M) = 0$ for every subgroup S of G and every $r \in \mathbb{Z}$.

Our first goal will be to give a sufficient condition for M to be cohomlogically trivial. We begin with the following lemma:

Lemma 5.4.1. The following hold:

1. If $\hat{H}^0(S, M) = H^1(S, M) = 0$ for all subgroups S of G, then $H^2(S, M) = 0$ for all S.
2. If $H^1(S, M) = H^2(S, M) = 0$ for all subgroups S of G, then $\hat{H}^0(S, M) = 0$ for all S.

Proof. 1. Special case: First consider the problem where G is an l-group, for l a prime number. We prove by induction on the order of G. Assume the result holds for all l-groups of order lesss than $|G|$. If $|S|$ is such a subgroup with $|S| < |G|$, then $H^2(S, M) = 0$ by induction hypothesis. Thus, we only need to show that $H^2(G, M) = 0$. Choose a normal subgroup N of G of index l. The exact sequence from Lemma 5.3.3 is:

$$\hat{H}^0(N, M) \to \hat{H}^0(G, M) \to \hat{H}^0(G/N, M^N) \to 0 \quad (*)$$

By assumption, $\hat{H}^0(G, M) = 0$, so exactness yields that $\hat{H}^0(G/N, M^N) = 0$. Also note that G/N is cyclic, so by periodicity of Tate cohomology for cyclic groups (Proposition 5.1.1), we have that $\hat{H}^2(G/N, M^N) = 0$. Now since $H^1(G, M) = 0$ by assumption also, we can apply Proposition 5.3.3 to obtain the following exact sequence:

$$0 \to H^2(G/N, M^N) \to H^2(G, M) \to H^2(N, M) \quad (**)$$

By induction, $H^2(N, M) = 0$ and we have seen above that $H^2(G/N, M^N) = 0$ as well; so exactness yields that $H^2(G, M) = 0$.
Now consider the general case. Let $S \subseteq G$ be any subgroup and let S_l be a Sylow l subgroup of G. By the special case, $H^2(S_l, M) = 0$. Now $H^2(S, M) \hookrightarrow \oplus_{S_l} H^2(S_l, M)$ (see [Gui2018, Corollary 12.22] for a proof) and so $H^2(S, M) = 0$ as required.

2. The argument here is similar and so it suffices to prove that $\hat{H}^0(G, M) = 0$. By (**) above, we have $H^2(G/N, M^N) = 0$ and so $\hat{H}^0(G/N, M^N) = 0$ by periodicity. Since $\hat{H}^0(N, M)$=0 by induction, (*) shows that $\hat{H}^0(G, M) = 0$ as required.

□

We can now give the desired condition for detecting cohomological triviality; this criterion is called the Nakayama-Tate Lemma.

Theorem 5.4.2 (Nakayama-Tate)**.** Suppose there exists an integer $r \in \mathbb{Z}$ such that $\hat{H}^r(S, M) = \hat{H}^{r+1}(S, M) = 0$. Then M is cohomologically trivial.

Proof. Let S be any subgroup of G. We want to show that $\hat{H}^n(S, M) = 0$ for all $n \in \mathbb{Z}$. By Lemma 5.2.4, we can find a module $M(-r)$ such that $\hat{H}^n(S, M(-r)) = \hat{H}^{n+r}(S, M)$. Now, by hypothesis, $\hat{H}^0(S, M(-r)) = \hat{H}^1(S, M(-r)) = 0$ for all subgroups S. Thus, we can apply Lemma 5.4.1 to conclude that $\hat{H}^2(S, M(-r)) = 0$. Thus, what we have shown is that $\hat{H}^n(S, M) = 0$ for $n = r, r+1, r+2$. We can iterate this procedure to obtain that $\hat{H}^n(S, M) = 0$ for $n \geq r$. Similarly, we can use statement 2 of Lemma 5.4.1 to extend on the left as well and so $\hat{H}^n(S, M) = 0$ for $n \leq r$. □

We now propose another definition.

Definition 5.4.2. Let $f : M \to N$ be a homomorphism of $\mathbb{Z}[G]$-modules. We say that f is a cohomological equivalence if the induced map $f_r : \hat{H}^r(S, M) \to \hat{H}^r(S, N)$ is an isomorphism for each $r \in \mathbb{Z}$ and for every subgroup S of G.

Lemma 5.4.3. Let $f : M \to N$ be as above. Then there exists a $\mathbb{Z}[G]$-module Q and maps δ_* and g_* such that for any subgroup S of G, the following sequence is exact:

$$\cdots \longrightarrow \hat{H}^{r-1}(S,Q) \xrightarrow{\delta_{r-1}} \hat{H}^r(S,M) \xrightarrow{f_r} \hat{H}^r(S,N)$$
$$\xrightarrow{g_r} \hat{H}^r(S,Q) \xrightarrow{\delta_r} \hat{H}^{r+1}(S,M) \xrightarrow{f_{r+1}} \cdots$$

Proof. See [Gui2018, Lemma 13.8]. □

Theorem 5.4.4 (Tate's criterion)**.** A $\mathbb{Z}[G]$-module homomorphism $f : M \to N$ is a cohomological equivalence if and only if there exists an $r \in \mathbb{Z}$ such that for every subgroup S of G, we have:

1. $f_{r-1} : \hat{H}^{r-1}(S,M) \to \hat{H}^{r-1}(S,N)$ is surjective
2. $f_r : \hat{H}^r(S,M) \to \hat{H}^r(S,N)$ is an isomorphism
3. $f_{r+1} : \hat{H}^{r+1}(S,M) \to \hat{H}^{r+1}(S,N)$ is injective

Proof. Cohomological equivalence, by definition, certainly implies the three conditions. For the converse, we first make two reductions. Firstly, let Q be as in the previous lemma; then by exactness of the long exact-sequence, it suffices to show that Q is cohomlogically trivial. Secondly, by the Nakayama-Tate lemma, it further suffices to show that $\hat{H}^{r-1}(S,Q) = \hat{H}^r(S,Q) = 0$ for each subgroup S. By exactness, note that f_{r+1} injective $\implies \operatorname{im} \delta_r = 0 \implies \ker \delta_r = \hat{H}^r(S,Q) \implies \operatorname{im} g_r = \hat{H}^r(S,Q)$. On the other hand, f_r surjective $\implies \ker g_r = \hat{H}^r(S,N) \implies \operatorname{im} g_r = 0$. Thus, $\hat{H}^r(S,Q) = 0$ as desired. Similarly, by using the other conditions given, we have $\hat{H}^{r-1}(S,Q) = 0$. □

Lemma 5.4.5. Assume that for any subgroup $S \subseteq G$, $\hat{H}^0(S,M)$ is cyclic of order $|S|$ and $\hat{H}^{-1}(S,M) = 0$. Then there exists a $\mathbb{Z}[G]$-module homomorphism $f : \mathbb{Z} \to M$ which is a cohomological equivalence.

Proof. We use Tate's criterion with $r = 0$. Then $f_{-1} : \hat{H}^{-1}(S,\mathbb{Z}) \to \hat{H}^{-1}(S,M)$ is surjective since the codomain is zero by assumption. Also, $f_1 : \hat{H}^1(S,\mathbb{Z}) \to \hat{H}^1(S,M)$ is injective since the domain is $\hat{H}^1(S,\mathbb{Z}) = \operatorname{Hom}(S,\mathbb{Z}) = 0$, since S is finite. It remains to show that $f_0 : \hat{H}^0(S,\mathbb{Z}) \to \hat{H}^0(S,M)$ is an isomorphism; this is long and we refer the reader to [Gui2018, Proposition 13.10]. □

Theorem 5.4.6 (Tate's theorem)**.** Let G be a finite group and let M be a $\mathbb{Z}[G]$-module. Assume that for any subgroup $S \subseteq G$, $H^2(S,M)$ is cyclic of order $|S|$ and $H^1(S,M) = 0$. Then for any $r \in \mathbb{Z}$ and any subgroup $S \subseteq G$, we have an isomorphism of groups: $\hat{H}^{r-2}(S,\mathbb{Z}) \cong \hat{H}^r(S,M)$. In fact, we can find

a family of isomorphisms $\theta_{G,M,S,r} : \hat{H}^{r-2}(S,\mathbb{Z}) \xrightarrow{\cong} \hat{H}^r(S,M)$ satisfying the following compatibility condition: whenever $S' \subseteq S \subseteq G$, we have the following commutative diagram for $r \in \mathbb{Z}$:

$$\begin{array}{ccc} \hat{H}^{r-2}(S',\mathbb{Z}) & \xrightarrow{\theta_{G,M,S',r}} & \hat{H}^r(S',M) \\ \Big\downarrow{\scriptstyle \text{Cores}} & & \Big\downarrow{\scriptstyle \text{Cores}} \\ \hat{H}^{r-2}(S,\mathbb{Z}) & \xrightarrow{\theta_{G,M,S,r}} & \hat{H}^r(S,M) \end{array}$$

Proof. Pick any $r \in \mathbb{Z}$ and any subgroup $S \subseteq G$. By Lemma 5.2.4, we can find a module $M(-2)$ such that $\hat{H}^r(S,M) \cong \hat{H}^{r-2}(S,M(-2))$ for all $r \in \mathbb{Z}$ and all subgroups S of G. The hypotheses of the previous lemma thus hold for the group $\hat{H}^{r-2}(S,M(-2))$ and applying the lemma yields the isomorphisms $\hat{H}^{r-2}(S,M(-2)) \cong \hat{H}^{r-2}(S,\mathbb{Z})$. For the compatibility, see [Gui2018, Theorem 13.11]. □

5.5 Examples in low degrees

We conclude the chapter by giving yet another set of formulas for the cohomology groups which will be useful for us in the next chapter. These formulas are especially useful in low degrees.

Definition 5.5.1 (Inhomogeneous cochains)**.** Let M be a $\mathbb{Z}[G]$-module. For $n \geq 0$, define $\mathcal{C}^n(G,M)$ to be the group of map of sets: $f : G^n \to M$. The elements of $\mathcal{C}^n(G,M)$ are called inhomogeneous cochains of degree n, with values in M. Define boundary maps d^0: $\mathcal{C}^0(G,M) \to \mathcal{C}^1(G,M)$ by $d^0(m)(\sigma) = \sigma \cdot m - m$ and d^1: $\mathcal{C}^1(G,M) \to \mathcal{C}^2(G,M)$ by $d^1(f)(\sigma,\tau) = f(\sigma) + \sigma \cdot f(\tau) - f(\sigma\tau)$. For $n \geq 2$, d^n: $\mathcal{C}^n(G,M) \to \mathcal{C}^{n+1}(G,M)$ by:

$$\begin{aligned} d^n(f)(\sigma_1,\ldots,\sigma_{n+1}) &= \sigma_1 \cdot f(\sigma_2,\ldots,\sigma_{n+1}) \\ &+ \sum_{i=1}^{n} (-1)^i f(\sigma_1,\ldots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\ldots,\sigma_{n+1}) \\ &+ (-1)^{n+1} f(\sigma_1,\ldots,\sigma_n) \end{aligned}$$

Put $\mathcal{Z}^n(G,M) = \ker(d^n)$ and $\mathcal{B}^n(G,M) = \mathrm{Im}(d^{n-1})$ and call them the group of cocyles and coboundaries respectively.

Proposition 5.5.1. The quotient $\mathcal{Z}^n(G,M)$ is isomorphic to $H^n(G,M)$.

Proof. This can be proven via homogeneous cochains, see [Gui2018 Lemma 10.14]. □

Example 5.5.1. Via inhomogeneous cochains, we see that a one-cocyle is a map $f : G \to M$ such that $f(gg') = g \cdot f(g') + f(g)$ for all $g, g' \in G$ and a one-coboundary is a map $h : G \to M$ is called a 1-coboundary if there exists $m \in M$ such that $h(g) = g \cdot m - m$ for all $g \in G$. Moreover, we also note that if G has trivial M action, then $H^1(G, M) = \mathrm{Hom}(G, M)$.

Example 5.5.2. Similarly, a two-cocyle is a map $c : G \times G \to M$ such that for all $\sigma, \tau, \rho \in G$, $\sigma \cdot f(\tau, \rho) + f(\sigma, \tau\rho) = f(\sigma\tau, \rho) + f(\sigma, \tau)$ and a two coboundary is a map $c : G \times G \to M$ such that there exists a map $f : G \to M$ such that for all $\sigma, \tau \in G$, $c(\sigma, \tau) = f(\sigma) + \sigma \cdot f(\tau) - f(\sigma\tau)$.

We conclude this chapter by giving an important theorem concerning the second cohomology group.

Theorem 5.5.1. Let G be a finite cyclic group and let M be any G-module. Put $N(m) = \sum_{g \in G} g \cdot m$ and write $N(M)$ for the image of the map $N : M \to M$. Then there is an isomorphism: $H^2(G, M) \cong M^G / N(M)$. Moreover, for each generator ρ of G, one such isomorphism is induced by $\psi_\rho : \mathcal{Z}^2(G, M) \to M^G$ defined by $\psi_\rho(c) = \sum_{\tau \in G} c(\tau, \rho)$.

Proof. See [Gui2018, Proposition 7.18]. □

Note that we are already familiar with this isomorphism via the periodicity of Tate cohomology groups but the virtue of the theorem is that gives an explicit way of constructing the isomorphism.

Chapter 6

Applications of group cohomology

6.1 Brauer group of a local field

In this section, we shall see reformulate the Brauer group in terms of the second cohomology group. To do this, we first introduce the notion of a crossed product algebra. Let E/F be a finite Galois extension of fields and pick a two-cocycle $c \in \mathcal{Z}^2(G, E^\times)$, where $G = \mathrm{Gal}(E/F)$.

Definition 6.1.1 (Crossed product algebra)**.** For each $\sigma \in G$, let a_σ be a formal symbol. Define A_c to be the free vector space over E on the set of all a_σ's. Furthermore, define multiplication on A_c by $\left(\sum_\sigma e_\sigma a_\sigma\right) \cdot \left(\sum_\tau e'_\tau a_\tau\right) := \sum_{\sigma,\tau} e_\sigma \sigma(e'_\tau) c(\sigma,\tau) a_{\sigma\tau}$.

Theorem 6.1.1. The crosssed product algebra A_c is a central-simple F-algebra and $[A_c] \in \mathrm{Br}(E/F)$. The association $c \mapsto [A_c]$ induces an isomoprhism of groups: $H^2(\mathrm{Gal}(E/F), E^\times) \cong \mathrm{Br}(E/F)$.

Proof. See [Gui2018, Theorem 7.21 & Proposition 7.26]. □

Corollary 6.1.1.1. Suppose E/F is a finite Galois extension of fields with $\mathrm{Gal}(E/F)$ cyclic. Then $\mathrm{Br}(E/F) \cong F^\times / N_{E/F}(E^\times)$.

Proof. This follows from the above theorem and Theorem 5.5.1. □

Proposition 6.1.1. Suppose $F \subseteq E_0 \subseteq E$ with both E/F and E_0/F finite and Galois. We have the following commuative diagram:

$$\begin{array}{ccc} H^2(\mathrm{Gal}(E_0/F), E_0^\times) & \xrightarrow{\inf} & H^2(\mathrm{Gal}(E/F), E^\times) \\ \cong\downarrow & & \downarrow\cong \\ \mathrm{Br}(E_0/F) & \xrightarrow{\subseteq} & \mathrm{Br}(E/F) \end{array}$$

Proof. See [Gui2018, Proposition 7.28]. □

Recall that $\mathrm{Br}(F) \cong \varinjlim \mathrm{Br}(E/F)$ where the limit ranges through all fields $F \subseteq E \subseteq \overline{F}$ such that E/F finite Galois. Note that by Corollary 6.1.1 we have identified $\mathrm{Br}(E/F)$ with $H^2(\mathrm{Gal}(E/F), E^\times)$ and Proposition 6.1.1 tells us that we also have compatibility of the homomorphisms. Thus, $\mathrm{Br}(F) \cong \varinjlim H^2(\mathrm{Gal}(E/F), E^\times)$, where the limit is taken over the same range. In fact, when F is a local field, we can make a stronger statement as we proceed to show.

Proposition 6.1.2. Let F be a local field and let K be a skewfield such that $\mathcal{Z}(K) = F$. There exists a field E with $F \subseteq E \subseteq K$ which is maximal and such that E/F is unramified. It follows that $[K] \in \mathrm{Br}(E/F)$.

Proof. See [Gui2018, Lemma 8.1 & Corollary 8.2]. □

As a result, $\mathrm{Br}(F) \cong \varinjlim \mathrm{Br}(E/F)$, where the limit ranges through all field $F \subseteq E \subseteq \overline{F}$ such that E/F unramified. We know from Corollary 3.3.2.1, there is a field $E_n \subseteq \overline{F}$ with E_n/F unramified of degree n and $E_n \subseteq E_m$ if and only if n divides m. As a result, if $[K : F] = n^2$, then the field E in the corollary is isomorphic to E_n.

Proposition 6.1.3. Let E_n be the unramified extension of degree n as above. Then $N_{E_n/F}(E_n^\times) = \{f \in F^\times : n \text{ divides } v(f)\}$.

Proof. See [Gui2018, Proposition 8.4] □

Corollary 6.1.1.2. The group Br(E_n/F) is a cyclic group of order n.

Proof. By the proposition above, the kernel of the composite map $F^\times \xrightarrow{v} \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ is $N_{E_n/F}(E_n^\times)$. Now by Corollary 6.1.1.1 , $\mathrm{Br}(E_n/F) \cong F^\times/N_{E_n/F}(E_n^\times) \cong \mathbb{Z}/n\mathbb{Z}$. □

Thus, the basic idea is starting to emerge: $\mathrm{Br}(F)$ is the union of the cyclic groups $\mathrm{Br}(E_n/F)$ and when n divides m, we know by the theory of cyclic groups that $\mathrm{Br}(E_n/F)$ is the unique order n subgroup of $\mathrm{Br}(E_m/F)$. In particular, $\mathrm{Br}(E_n/F)$ is the unique subgroup of order n in $\mathrm{Br}(F)$, for any $n \in \mathbb{N}_{\geq 1}$. It is now natural to conjecture that $\mathrm{Br}(F)$ must be isomorphic to $\mathbb{Q}/\mathbb{Z}$. We now describe how to explicitly construct a map $\mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$.

Let K be a skewfield such that $\mathcal{Z}(K) = F$. Choose a field E with $F \subseteq E \subseteq K$ which is maximal and with E/F unramified. The corresponding extensions $\mathbb{E}/\mathbb{F}$ of residue fields has a cyclic Galois group generated by the Frobenius map. Since E/F is unramified, $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(\mathbb{E}/\mathbb{F})$ thus also has a Frobenius element

which we call ρ. By the Skolem-Noether theorem, there exists $a_\rho \in K^\times$ such that $\rho(x) = a_\rho x a_\rho^{-1}$ for all $x \in E$. Also there exists a unique extension w to K of the valuation v defined on F. The number $w(a_\rho)$ is a priori not an integer but an element of $\mathbb{Q}$. We let $\mathrm{Inv}(K, E, a)$ denote the class of $w(a)$ in $\mathbb{Q}/\mathbb{Z}$. We proceed to show that this assignment is well-defined; first we state the following lemma.

Lemma 6.1.2. For any $\sigma \in G = \mathrm{Gal}(E/F)$, let $a_a \in K^\times$ be the element provided by Skolem-Noether such that $\sigma(x) = a_\sigma x a_\sigma^{-1}$ for all $x \in E$.

1. If $a'_\sigma \in K^\times$ is another such element, then there exists $e \in E^\times$ such that $a'_\sigma = e a_\sigma$.
2. There exists $c(\sigma, \tau) \in E^\times$ such that $a_\sigma a_\tau = c(\sigma, \tau) a_{\sigma\tau}$ for all $\sigma, \tau \in G$. Moreover, once we have fixed a_σ for all $\sigma \in G$, $c : G \times G \to E^\times$ is an inhomogeneous 2 cocycle.
3. K is isomorphic to the crossed product algebra A_c.

Proof. See [Gui2018, Proposition 7.18]. □

Proposition 6.1.4. The element $\mathrm{Inv}(K, E, a)$ does not depend on E or a and only depends on K up to isomoprhism of F algebras. It yields a map:

$$\mathrm{Inv} : \mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$$

Proof. First, we show that when E is chosen, the choice of a is not important. By the lemma above, another $a' \in K$ inducing the same automorphism of E would be of the form $a' = ea$ with $e \in E^\times$. However, $w(E^\times) = v(F^\times) = \mathbb{Z}$, since E/F is unramified and v can assumed to be normalized without loss of generality. Thus, $w(a') = w(ea) = w(e) + w(a) \equiv w(a)$ mod $\mathbb{Z}$. We can thus write $\mathrm{Inv}(K, E)$ instead of $\mathrm{Inv}(K, E, a)$; our next task is to show that the invaraint is independent of the choice of E as well. To do this, we make the following claim:
Claim: If $\theta : K \to L$ is an isomoprhism of F-algebras, then $\mathrm{Inv}(K, E, a) = \mathrm{Inv}(L, \theta(E), \theta(a))$ (so $\mathrm{Inv}(K, E) = \mathrm{Inv}(L, \theta(E))$) .
Proof of claim: First we show that the right hand side is well-defined. By the Frobenius condition, $axa^{-1} \equiv x^q$ mod $\mathfrak{P}$, where $\mathfrak{P}$ is the maximal ideal of $\mathcal{O}_E$. Applying θ to this congruence, we conclude that $\theta(a)\theta(x)\theta(a)^{-1} \equiv \theta(x)^q$ mod $\theta(\mathfrak{P})$. Note that θ induces an isomoprhism $\mathcal{O}_E \to \mathcal{O}_{\theta(E)}$ and that $\theta(\mathfrak{P})$ is the maximal ideal of $\mathcal{O}_{\theta(E)}$. The last congruence characterizes the Frobenius automorphism of $\mathcal{O}_{\theta(E)}$, so the right hand side is well-defined. Now, by uniqueness of extensions, $w_K(a) = w_L(\theta(a))$ and so $\mathrm{Inv}(K, E, a) = \mathrm{Inv}(L, \theta(E), \theta(a))$, proving the claim.
Finally, if $E' \subseteq K$ is another choice for the role of E, then by the Skolem Noether

theorem, there is an automorphism θ of K with $\theta(E) = E$. By the claim, $\mathrm{Inv}(K, E) = \mathrm{Inv}(K, E')$; we may thus use the notation $\mathrm{Inv}(K)$. The claim also implies that $\mathrm{Inv}(K) = \mathrm{Inv}(L)$ when K and L are isomoprhic. □

We can now finally compute the Brauer group of a local field; the idea behind the proof is to combine all the facts of the Brauer group that we have obtained earlier.

Theorem 6.1.3. The invariant $\mathrm{Inv}{:}\mathrm{Br}(F) \to \mathbb{Q}/\mathbb{Z}$. is an isomoprhism of groups which induces an isomoprhism betwen $\mathrm{Br}(E_n/F)$ and $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$.

Proof. For $n \geq 1$, let K be a skewfield with $[K] \in \mathrm{Br}(E_n/F)$ and suppose that $[K]$ does not belong to a subgroup $\mathrm{Br}(E_d/F)$ for any proper divisor d of n. Thus, $[K : F] = n^2$ (see [Gui2018, Lemma 8.6]) and we may choose E such that $F \subseteq E \subseteq K$ with E/F unramified and $[E : F] = n$. The skewfield K is then isomorphic to a crossed product algebra A_c for some $c \in \mathcal{Z}^2(\mathrm{Gal}(E/F), E^\times)$ by Lemma 6.1.2. Also note that E is isomorphic to E_n and since Inv depends only on its isomorphism class, we may assume that $K = A_c$ and $E = E_n$.
Let $e_1, \ldots, e_n$ be a basis for E_n over F and denote the elements of $\mathrm{Gal}(E_n/F)$ by $1, \rho, \ldots, \rho^{n-1}$, where ρ is the Frobenius map. Thus, $e_i a_{\rho^j}$ is a basis for K over F. Our goal is to compute $\mathrm{Inv}(K)$ which is the class of $w(a_\rho)$ in $\mathbb{Q}/\mathbb{Z}$. Note that $w(a_\rho) = \frac{1}{n^2} v(N_{K/F}(a_\rho))$ by Theorem 3.2.2. Multiplication by a_ρ is given in this basis by: $e_i a_{\rho^j} a_\rho = c(\rho^j, \rho) e_i a_{\rho^{j+1}}$. Thus, the matrix of m_{a_ρ} in this basis has only one non-zero coefficient in each row. Since we would like to compute $v(\det(m_{a_\rho}))$, we may freely permute the rows and columns to get a diagnol matrix whose determinant is $(\prod_{0 \leq i < n} c(\rho^i, \rho))^n$. We now apply Theorem 5.5.1 to obtain a map $\psi_\rho : \mathcal{Z}^2(\mathrm{Gal}(E_n/F), E_n^\times) \to F^\times$ with $\psi_\rho(c) = \prod_{0 \leq i < n} c(\rho^i, \rho)$. Thus, $w(a_\rho) = \frac{1}{n^2} v(\psi_\rho(c)^n) = \frac{1}{n} v(\psi_\rho(c))$. The same theorem also gives us an isomorphism $H^2(\mathrm{Gal}(E_n/F), E_n^\times) \cong F^\times / N_{E_n/F}(E_n^\times)$ via ψ_ρ.
On the other hand, by Proposition 6.1.3, v induces an isomorphism $F^\times / N_{E_n/F}(E_n^\times) \cong \mathbb{Z}/n\mathbb{Z}$ and so $\frac{1}{n} v$ induces an isomorphism $F^\times / N_{E_n/F}(E_n^\times) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Thus the composition:

$$I'_n : H^2(\mathrm{Gal}(E_n/F), E_n^\times) \xrightarrow{\psi_\rho} F^\times / N_{E_n/F}(E_n^\times) \xrightarrow{\frac{1}{n}v} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is an isomorphism of groups. Denote $\gamma_n : \mathrm{Br}(E_n/F) \to H^2(\mathrm{Gal}(E_n/F), E_n^\times)$ to be the isomorphism obtained by Theorem 6.1.1 and so $I_n := I'_n \circ \gamma_n$ is an isomorphism between $\mathrm{Br}(E_n/F)$ and $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Since $K = A_c$ corresponds to the cocycle c and since we have shown above that $w(a_\rho) = \frac{1}{n} v(\psi_\rho(c))$, we see that $\mathrm{Inv}(K) = I_n(K)$. Thus, $\mathrm{Inv} : \mathrm{Br}(E_n/F) \to \mathbb{Q}/\mathbb{Z}$ takes its values in $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$

and agrees with the isomorphism I_n when one restricts to those elements $[K]$ generating $\mathrm{Br}(E_n/F)$. To prove the theorem, consider the diagram:

$$\begin{array}{ccccccc}
\mathrm{Br}(E_d/F) & \xrightarrow{\gamma_d} & \mathrm{H}^2(\mathrm{Gal}(E_d/F), E_d^\times) & \xrightarrow{\varphi_\rho} & F^\times/\mathrm{N}_{E_d/F}(E_d^\times) & \xrightarrow{\frac{1}{d}v} & \frac{1}{d}\mathbb{Z}/\mathbb{Z} \\
\subset\downarrow & & \inf\downarrow & & f\mapsto f^{\frac{n}{d}}\downarrow & & \subset\downarrow \\
\mathrm{Br}(E_n/F) & \xrightarrow{\gamma_n} & \mathrm{H}^2(\mathrm{Gal}(E_n/F), E_n^\times) & \xrightarrow{\varphi_\rho} & F^\times/\mathrm{N}_{E_n/F}(E_n^\times) & \xrightarrow{\frac{1}{n}v} & \frac{1}{n}\mathbb{Z}/\mathbb{Z}
\end{array}$$

The arguments above, applied with replacing n by d, establish that when $[K] \in \mathrm{Br}(E_d/F)$ has order d, then in order to compute $\mathrm{Inv}(K)$, one may use the compositions of the isomorphisms on the first line of the diagram, which is I_d. If the diagram commutes, we would know that the restriction of I_n to $\mathrm{Br}(E_d/F)$ is I_d, so Inv coincides with I_n on all $\mathrm{Br}(E_n/F)$ making it an isomorphism. Thus, it suffices to check that the diagram commutes.

It is easy to see that the right-most square commutes. For the inner square, this requires a check; see [Gui2018, Example 7.28] for details. Finally, the left-most square commutes by Theorem 6.1.1.

□

Theorem 6.1.4 (Naturality)**.** If F'/F is a finite extension of local fields, we have the following commutative diagram: If F'/F is a finite extension of local fields, we have the following commutative diagram:

$$\begin{array}{ccc}
\mathrm{Br}(F) & \xrightarrow{\cong} & \mathbb{Q}/\mathbb{Z} \\
\downarrow & & \downarrow{\scriptstyle x\mapsto[F':F]x} \\
\mathrm{Br}(F') & \xrightarrow{\cong} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

Proof. See [Gui2018, Theorem 8.9 & Theorem 8.10]. □

Corollary 6.1.4.1. Let F'/F be any finite extension of local fields. Then $\mathrm{Br}(F'/F)$ is cyclic of order $[F' : F]$.

Proof. Let $n = [F' : F]$. By definition, $\mathrm{Br}(F'/F)$ is the kernel of the map $\mathrm{Br}(F) \to \mathrm{Br}(F')$. The naturality statement in the previous theorem allows us to identify this homomoprhism with multiplication by n on $\mathbb{Q}/\mathbb{Z}$ whose kernel is $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$. □

6.2 Galois cohomology

In this section, we introduce Galois cohomology; this is a specialized version of group cohomology where we take G to be a Galois group. In what follows, the basics of topological group theory and Infinite Galois theory are assumed. In this section, we let $\overline{F}$ to be the separable closure of $\mathbb{F}$.

Definition 6.2.1. Let G be a profinite group, M be a $\mathbb{Z}[G]$-module. If the map $G \times M \to M$ by $(\sigma, m) \mapsto \sigma \cdot m$ is continuous with respect to the discrete topology on M, we say that M is a discrete G-module.

When dealing with discrete G-modules, we henceforth insist that all maps in $C^n(G, M)$ and $\mathcal{C}^n(G, M)$ should be continuous. The same process as in the previous chapter shows that we get cohomology groups, which we also denote by $H^n(G, M)$ by abuse of notation.

Lemma 6.2.1. Let G be a profinite group and M be a discrete G-module. Then $H^n(G, M) \cong \varinjlim H^n(G/U, M^U)$, where the direct limit is taken over all open subgroups U.

Proof. See [Gui2018, Lemma 10.25]. □

Definition 6.2.2. Let F be a field and $\overline{F}$ be its separable closure. For any discrete $\mathrm{Gal}(\overline{F}/F)$-module M, define $H^n(F, M) := H^n(\mathrm{Gal}(\overline{F}/F), M)$ and call it the Galois cohomology group of F with coefficients in M.

Example 6.2.1. Let $M = \overline{F}^\times$. Then by Lemma 6.2.1, $H^n(F, \overline{F}^\times) = \varinjlim H^n(\mathrm{Gal}(E/F), E^\times)$ where the direct limit runs through all finite Galois extensions E/F contained in a fixed algebraic closure. In particular, $H^2(F, \overline{F}^\times) \cong \mathrm{Br}(F)$ by Theorem $6.1.1$ and Proposition 6.1.1. As another example, $H^0(F, \overline{F}^\times) = F^\times$.

The first important result in Galois cohomology is the following:

Theorem 6.2.2 (Hilbert 90)**.** Let L/F be any finite Galois extension. Then $H^1(Gal(L/F), L^\times) = 0$. As a result, $H^1(F, \overline{F}^\times) = 0$.

Proof. We work with inhomogeneous cochains. Let $G = \mathrm{Gal}(L/F)$. Pick any one cocycle $\psi \in \mathcal{Z}^1(G, L^\times)$ *i.e.* $\psi(\tau\sigma) = (\tau \cdot \psi(\sigma))\psi(\tau) = \psi(\tau)\tau(\psi(\sigma))$ for all $\tau, \sigma \in G$. We want to show that $\psi \in \mathcal{B}^1(G, L^\times)$ is a one coboundary i.e. we need $\psi(\tau) = \tau(a)a^{-1}$ for some $a \in L^\times$. By Dedekind's lemma on the independence of characters, $\sum_{\sigma \in G} \psi(\sigma)\sigma \neq 0$ as a map from L to L. Hence, there exists $c \in L^\times$ such that $b := \sum_{\sigma \in G} \psi(\sigma)\sigma(c) \neq 0$ in $L^\times$. Then $\psi(\tau)\tau(b) = \sum_{\sigma \in G} \psi(\tau)\tau(\psi(\sigma))\tau(\sigma(c)) = \sum_{\sigma \in G} \psi(\tau\sigma)\tau(\sigma(c))) = b$. Thus, $\psi(\tau) = \tau(b)^{-1}b = \tau(a)a^{-1}$ with $a = b^{-1}$. The fact that $H^1(F, \overline{F}^\times) = 0$ now follows from Lemma 6.2.1. □

Lemma 6.2.3 (Kummer exact sequence)**.** Let F be any field. Suppose that F is either perfect or the integer n is coprime to the characteristic of F. Then there is a short exact sequence of $\mathrm{Gal}(\overline{F}/F)$-modules:

$$1 \longrightarrow \mu_n(\overline{F}) \longrightarrow \overline{F}^\times \stackrel{x\mapsto x^n}{\longrightarrow} \overline{F}^\times \to 1$$

Proof. By definition, $\mu_n(\overline{F})$ is the kernel of $x \mapsto x^n$. When F is perfect, then $\overline{F}$ is an algebraic closure of F, so the equation $x^n - a = 0$ has solutions in $\overline{F}$. When the characteristic of F is coprime to n, then the equation has no multiple roots and so the equation also has a solution in $\overline{F}$. In either case, we have proven the desired surjectivity of $x \mapsto x^n$. □

Theorem 6.2.4. Suppose that F is either perfect or the integer n is coprime to the characteristic of F.

1. We have an isomorphism of groups $H^1(F, \mu_n) \cong F^\times / F^{\times n}$.
2. We have another isomoprhism $H^2(F, \mu_n) \cong$ the n-torsion in $H^2(F, \overline{F}^\times)$.

Proof. The key idea is to consider the Kummer exact sequence, write out the long exact sequence in cohomology and then use the vanishing guranteed by Hilbert 90.

1. : To prove this statement, the relevant portion of the long exact sequence is:

   $$H^0(F, \overline{F}^\times) \longrightarrow H^0(F, \overline{F}^\times) \longrightarrow H^1(F, \mu_n) \longrightarrow H^1(F, \overline{F}^\times)$$

   By Hilbert 90 , $H^1(F, \overline{F}^\times) = 0$. Also as noted in Example 6.2.1, $H^0(F, \overline{F}^\times) = F^\times$. Thus, our exact sequence is really:

   $$F^\times \stackrel{x\mapsto x^n}{\longrightarrow} F^\times \longrightarrow H^1(F, \mu_n) \longrightarrow 0$$

   and so $H^1(F, \mu_n) \cong F^\times / F^{\times n}$.
2. To prove this statement, the relevant portion of the long exact sequence is:

   $$H^1(F, \overline{F}^\times) \longrightarrow H^2(F, \mu_n) \longrightarrow H^2(F, \overline{F}^\times) \stackrel{x\mapsto x^n}{\longrightarrow} H^2(F, \overline{F}^\times)$$

   Again, Hilbert 90 implies $H^1(F, \overline{F}^\times) = 0$ and so by exactness $H^2(F, \mu_n) \cong$ the n-torsion in $H^2(F, \overline{F}^\times)$.

□

We remark that if F contains a primitive n-th root of unity ω, then we have an isomoprhism of discrete $\mathrm{Gal}(\overline{F}/F)$-modules $\mathbb{Z}/n\mathbb{Z} \to \mu_n$ given by $k \mapsto \omega^k$. So we can replace μ_n by $\mathbb{Z}/n\mathbb{Z}$ in the theorem above and in particular, we note for future use that $H^1(F, \mathbb{Z}/n\mathbb{Z}) \cong F^\times/F^{\times n}$. In fact, it possible to give an explicit description of this isomorphism:

Proposition 6.2.1. Suppose F contains a primitive n-th root of unity. Define a map $f : F^\times \to H^1(F, \mu_n)$ by $f(a) = \chi_a$ where χ_a is defined by $\chi_a(\sigma) = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}}$ for any nth root $\sqrt[n]{a}$ of a. Then f induces a group isomorphism $F^\times/F^{\times n} \cong H^1(F, \mu_n)$ and thus also $F^\times/F^{\times n} \cong H^1(F, \mathbb{Z}/n\mathbb{Z})$.

Proof. See [Sha, Lemma 2.5.8]. □

6.3 Hilbert symbol

Let F be any field and let $\overline{F}$ be a separable closure. Let $b \in F^\times$ and $\chi \in H^1(F, \mathbb{Q}/\mathbb{Z})$ i.e. $\chi : \mathrm{Gal}(\overline{F}/F) \to \mathbb{Q}/\mathbb{Z}$ is a continuous group homomorphism, where $\mathbb{Q}/\mathbb{Z}$ is equipped with the discrete topology. Thus, the kernel of χ is open and by infinite Galois theory is of the form $\mathrm{Gal}(\overline{F}/E)$ for some finite Galois extension E/F. Thus, the image of χ has finite order $d := [E : F]$, so $\chi(G) \cong \frac{1}{d}\mathbb{Z}/\mathbb{Z}$. The Galois group $\mathrm{Gal}(E/F)$ is hence cyclic and has a canonical generator $\rho \in \mathrm{Gal}(E/F)$ such that $\chi(\rho) = \frac{1}{d}$. By Theorem $5.5.1$, we have an explicit isomorphism $\psi_\rho : H^2(\mathrm{Gal}(E/F), E^\times) \to F^\times/N_{E/F}(E^\times)$. The element of $H^2(Gal(E/F), E^\times)$ mapping to the class of b under ψ_ρ is written (χ, b).

Proposition 6.3.1. The symbol (χ, b) is bilinear *i.e.* $(\chi, bb') = (\chi, b)+(\chi, b')$ and $(\chi + \chi', b) = (\chi, b) + (\chi', b)$. Moreover, the kernel of $F^\times \to H^2(\mathrm{Gal}(E/F), E^\times)$ defined by $b \mapsto (\chi, b)$ is $N_{E/F}(E^\times)$.

Proof. $(\chi, bb') \in H^2(\mathrm{Gal}(E/F), E^\times)$ is such that $\psi_\rho((\chi, bb')) = \overline{bb'} = \overline{b}\ \overline{b'} = \psi_\rho((\chi, b))\psi_\rho((\chi, b')) = \psi_\rho((\chi, b)+(\chi, b'))$. By injectivity, $(\chi, bb') = (\chi, b)+(\chi, b')$. Proving that $(\chi + \chi', b) = (\chi, b) + (\chi', b)$ is longer and we refer the reader to [Gui2018, Lemma 11.11 & Corollary 11.12] for the argument. Finally, consider the composite $F^\times \xrightarrow{b\mapsto(\chi,b)} H^2(\mathrm{Gal}(E/F), E^\times) \xrightarrow{\psi_\rho} F^\times/N_{E/F}(E^\times)$. Then $\ker$ ($\mathsf{F}^\times \to H^2(\mathrm{Gal}(E/F), E^\times)) = \{b \in F^\times | \psi_\rho((\chi, b)) = 0 \text{ in } F^\times/N_{E/F}(E^\times)\} = \{b \in F^\times | b \in N_{E/F}(E^\times)\} = N_{E/F}(E^\times)$. □

Now assume that F contains a primitive nth root of unity ω . Next, we turn our attention to (χ_a, b), where χ_a is defined as in 6.2.1.

Lemma 6.3.1. The fixed field of $\ker(\chi_a)$ is $F(\sqrt[n]{a})$ and $(\chi_a, b) = 0$ happens precisely when b is a norm from $F(\sqrt[n]{a})$.

Proof. See [Gui2018, Lemma 11.13]. □

Lemma 6.3.2. The element $(\chi_a, b) \in H^2(F, \overline{F^\times})$ is n-torsion.

Proof. See [Gui2018, Lemma 11.13]. □

Thus the above lemma combined with statement (2) in Theorem $6.2.4$ shows that we can view (χ_a, b) as an element of $H^2(F, \mu_n)$. Since we have assumed that F contains a primitive nth-root of unity, by the remark after Theorem $6.2.4$, we can in fact view (χ_a, b) as an element of $H^2(F, \mathbb{Z}/n\mathbb{Z})$. We are now ready to define the Hilbert symbol:

Definition 6.3.1 (Hilbert symbol)**.** For $a, b \in F^\times$, the element of $H^2(F, \mathbb{Z}/n\mathbb{Z})$ corresponding to (χ_a, b) under the above identifications is written as (a, b) and is called the Hilbert symbol of a and b.

The Hilbert symbol can be thought of as a bilinear map $F^\times/F^{\times n} \times F^\times/F^{\times n} \to H^2(F, \mathbb{Z}/n\mathbb{Z})$. Using Theorem 6.2.4 and the subsequent remark, we may replace $F^\times/F^{\times n}$ by $H^1(F, \mathbb{Z}/n\mathbb{Z})$.

Example 6.3.1 (Hilbert symbol for local fields)**.** When F is a local field, $H^2(F, \overline{F^\times}) \cong \mathrm{Br}(F) \cong \mathbb{Q}/\mathbb{Z}$. The n-torsion subgroup of $\mathbb{Q}/\mathbb{Z}$ is $\frac{1}{n}\mathbb{Z}/\mathbb{Z}$ which is a cyclic group of order n. Thus $H^2(F, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. Thus for a local field F, the Hilbert symbol is a bilinear map $H^1(F, \mathbb{Z}/n\mathbb{Z}) \times H^1(F, \mathbb{Z}/n\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$.
Now consider the case when $n = 2$. By Lemma 6.3.1, we see that $(a, b) \in \mathbb{F}_2$ and:

$$(a, b)_F = \begin{cases} 0 & \text{if } b \text{ is a norm from } F(\sqrt{a}) \\ 1 & \text{otherwise} \end{cases}$$

Thus, $(a, b)_F = 0$ exactly when $x^2 - ay^2 = b$ has a solution with $x, y \in F$.

Chapter 7

Proof of Local Class Field Theory

In this chapter, we will employ all the tools developed previously to prove the two main theorems of local class field theory- the existence theorem and the reciprocity theorem. Recall that the existence theorem of local class field theory yields the following 1-1 correspondence:

Theorem 7.0.1 (Existence theorem of local class field theory)**.** Let F be a p-adic field. Then:

$\{\text{finite abelian extensions of } F\} \overset{1:1}{\leftrightarrow} \{\text{subgroups of finite index of } F^\times\}$

Moreover, this correspondence is inclusion reversing and is given by associating a finite abelian extension L of F to the subgroup $N_{L/F}(L^\times)$ of $F^\times$.

Notation: When the base field F is understood, we write N_L for $N_{L/F}(L^\times)$.

Since this correspondence is inclusion reversing, we have the following as immediate corollaries once we have proven the existence theorem:
a) $N_{L_1L_2} = N_{L_1} \cap N_{L_2}$ as subgroups of $F^\times$.
b) $N_{L_1 \cap L_2} = N_{L_1} N_{L_2}$ as subgroups of $F^\times$.

Now, let us recall the Reciprocity theorem:

Theorem 7.0.2 (Reciprocity theorem)**.** Let L/F be a finite Galois extension of p-adic fields. Then $\mathrm{Gal}(L/F)^{\mathrm{ab}} \cong F^\times / N_{L/F}(L^\times)$ as groups.

Our strategy to prove these statements will be to work backward: we will first prove the Reciprocity theorem, then prove statement a) and finally prove the existence theorem. In more detail, the strategy can be broken down into the following five parts:

1. We first prove the Reciprocity theorem by using Tate's theorem.

2. Using the Reciprocity theorem, we prove statement a) above.
3. Next, we prove injectivity in the existence theorem: i.e. we prove a weaker version of the Existence theorem where we replace subgroups of finite index by subgroups of the form N_L.
4. We then prove a result known as Tate-duality.
5. Finally, we prove the Existence theorem in its full generality: *i.e.* we prove surjectivity of the correspondence in the Existence theorem.

7.1 Reciprocity theorem

In this section, we prove the Reciprocity theorem and deduce some consequences of it. The key ingredients used in the proof are: Tate's theorem and the facts that $H^1(\mathrm{Gal}(L/K), L^\times) = 0$ (Hilbert 90) and $H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathrm{Br}(L/K)$.

Theorem 7.1.1 (Reciprocity theorem)**.** Let L/F be a finite Galois extension of local fields. Then $\mathrm{Gal}(L/F)^{\mathrm{ab}} \cong F^\times/N_{L/F}(L^\times)$ as groups.

Proof. Set $G = \mathrm{Gal}(L/F)$, $M = L^\times$. By Galois theory, any subgroup S of G is of the form $\mathrm{Gal}(L/K)$. By the Hilbert 90 theorem, $H^1(\mathrm{Gal}(L/K), L^\times) = 0$. We also know $H^2(\mathrm{Gal}(L/K), L^\times) \cong \mathrm{Br}(L/K)$, which is cyclic of order $|\mathrm{Gal}(L/K)|$ by Corollary 6.1.4.1. We can thus apply Tate's theorem. For $S = G$ and $r = 0$, the theorem gives an isomorphism $\hat{H}^0(\mathrm{Gal}(L/F), L^\times) \cong \hat{H}^{-2}(\mathrm{Gal}(L/F), \mathbb{Z})$. However,$\hat{H}^0(\mathrm{Gal}(L/F), L^\times) = F^\times/N_{L/F}(L^\times)$ by definition of Tate cohomology and $\hat{H}^{-2}(\mathrm{Gal}(L/F), \mathbb{Z}) = H_1(\mathrm{Gal}(L/F), \mathbb{Z}) = \mathrm{Gal}(L/F)^{\mathrm{ab}}$ by definition of Tate cohomology and Proposition 5.3.1. □

Definition 7.1.1 (Artin symbol)**.** Consider the composite map $F^\times \to F^\times/N_{L/F}(L^\times) \to \mathrm{Gal}(L/F)^{\mathrm{ab}}$ where the first arrow is the natural quotient map and the second arrow is the isomorphism obtained from the Reciprocity theorem. We denote it by $x \mapsto (x, L/F)$ and we call it the Artin symbol of x.

Lemma 7.1.2. Suppose $F \subseteq K \subseteq L$ with L/F finite and Galois. Then we have the following commutative diagram:

$$\begin{array}{ccc} K^\times & \xrightarrow{x\mapsto(x,L/K)} & \mathrm{Gal}(L/K)^{\mathrm{ab}} \\ {\scriptstyle N_{K/F}}\downarrow & & \downarrow \\ F^\times & \xrightarrow{x\mapsto(x,L/F)} & \mathrm{Gal}(L/F)^{\mathrm{ab}} \end{array}$$

where the vertical right arrow is the natural map obtained by the universal property of abelianization.

Proof. We need to check that the right vertical arrow is indeed given by corestriction; the lemma then follows by the compatibility statement in Tate's theorem. □

Lemma 7.1.3. Suppose $F \subseteq K \subseteq L$ with L/F and K/F both finite and Galois. Then the two homomorphisms $F^\times \to \mathrm{Gal}(K/F)^{\mathrm{ab}}$ in the diagram below have the same kernel.

$$\begin{array}{ccc} F^\times & \xrightarrow{x\mapsto(x,L/F)} & \mathrm{Gal}(L/F)^{\mathrm{ab}} \\ {\scriptstyle =}\downarrow & & \downarrow \\ F^\times & \xrightarrow{x\mapsto(x,K/F)} & \mathrm{Gal}(K/F)^{\mathrm{ab}} \end{array}$$

Proof. Since both homomorphisms are surjective and $\mathrm{Gal}(K/F)^{\mathrm{ab}}$ is finite, we only need to prove an inclusion between the kernels. Going down and then right, we see that the kernel of $x \mapsto (x, K/F)$ is N_K. By the previous lemma, the group N_K is taken to that subgroup of $\mathrm{Gal}(L/F)^{\mathrm{ab}}$ which is the the image of $\mathrm{Gal}(L/K)^{\mathrm{ab}} \to \mathrm{Gal}(L/F)^{\mathrm{ab}}$; elements in that subgroup restrict to the identity of $\mathrm{Gal}(K/F)^{\mathrm{ab}}$. Hence, N_K is included in the kernel of the homomoprhism going right and then down. □

7.2 Norm subgroups

We begin this section by stating an important property of norms that we will repeatedly use many times from now:

Proposition 7.2.1 (Transitivity of norms)**.** If $F \subseteq K \subseteq L$ are local fields, then for all $x \in L$, $N_{K/F}(N_{L/K}(x)) = N_{L/F}(x)$. As a result, we have $N_L \subseteq N_K$.

Proof. See [Gui2018, Appendix pp281]. □

Lemma 7.2.1 (Norm subgroups can be obtained from abelian extensions)**.** Let L/F be a finite Galois extension and let L^{ab}/F be the largest abelian extension contained in L. Then $N_L = N_{L^{ab}}$.

Proof. Consider the diagram in Lemma 7.1.3 with $K = L^{\mathrm{ab}}$ and note that, by Galois theory, $\mathrm{Gal}(L/F)^{\mathrm{ab}} \cong \mathrm{Gal}(L^{\mathrm{ab}}/F)$. Thus, the kernel of the map by going right and then down is precisely N_L. Now applying the lemma 7.1.3 yields $N_L = N_{L^{\mathrm{ab}}}$. □

We now complete Step 2 of the proof; namely we prove statement that we labelled (a) in the first section.

Lemma 7.2.2. Let L_1 and L_2 be finite abelian extensions of F. Then $\mathrm{N}_{L_1L_2} = N_{L_1} \cap N_{L_2}$.

Proof. Since $L_i \subseteq L_1L_2$ for $i \in \{1,2\}$, we have by transitivity of norms $N_{L_1L_2} \subseteq L_i$ i.e. $N_{L_1L_2} \subseteq N_{L_1} \cap N_{L_2}$.
Conversely, suppose $x \in N_{L_1} \cap N_{L_2}$. Consider the diagram in Lemma 7.1.3 with $L = L_1L_2$ and $K = L_i$ for $i \in \{1,2\}$. Since L_1L_2/F is abelian, $(x, L_1L_2/F)$ restricts to the trivial element of $\mathrm{Gal}(L_i/F)$ for all $i \in \{1,2\}$. However, an element of $\mathrm{Gal}(L_1L_2/F)$ is determined by its action on L_1 and L_2, so $(x, L_1L_2/F) = 1$. It follows from Lemma 7.1.3 that $x \in N_{L_1L_2}$. □

Now we prove Step 3 which is the injectivity in the existence theorem:

Theorem 7.2.3. We have the following $1:1$ order reversing correspondence:
$\{$finite abelian extensions of F $\} \overset{1:1}{\leftrightarrow} \{$norm subgroups of $F^\times\}$

Proof. From Lemma 7.2.1, $L \mapsto N_L$ is surjective. A key step in proving injectivity is the following claim:
Claim: When, L_1 and L_2 are abelian extensions of F, $N_{L_2} \subseteq N_{L_1}$ implies $L_1 \subseteq L_2$.
Proof of claim: Using the previous lemma and the hypothesis, we have $N_{L_1L_2} = N_{L_1} \cap N_{L_2} = N_{L_2}$. Thus, $x \mapsto (x, L_1L_2/F)$ and $x \mapsto (x, L_2/F)$ have the same kernel. Apply Lemma 7.1.3 with $L = L_1L_2$ and $K = L_2$ to conclude that the restriction map $\mathrm{Gal}(L_1L_2/F) \to \mathrm{Gal}(L_2/F)$ is injective; however, the kernel of this map is $\mathrm{Gal}(L_1L_2/L_2)$. Thus, by Galois theory, $L_1L_2 = L_2$ and so $L_1 \subseteq L_2$ thus proving the claim.
Thus, by switching the roles of L_1 and L_2, we see that $N_{L_1} = N_{L_2}$ implies $L_1 = L_2$ *i.e.*, we have proven injectivity. □

Corollary 7.2.3.1. Any subgroup of $F^\times$ containing a norm subgroup N_L is a norm subgroup.

Proof. We may assume that L/F is abelian by Lemma 7.2.1. Then:

$$\begin{aligned}\{\text{subgroups of } F^\times \text{ containing } N_L\} &\overset{1:1}{\leftrightarrow} \{\text{subgroups of } F^\times/N_L\} \\ &\overset{1:1}{\leftrightarrow} \{\text{subgroups of } \mathrm{Gal}(L/F)\} \\ &\overset{1:1}{\leftrightarrow} \{\text{subfields } F \subseteq K \subseteq L\}\end{aligned}$$

Thus, the groups containing N_L are exactly the various groups N_K for $F \subseteq K \subseteq L$.

□

7.3 Tate duality and universal norms

We will use the notation of Chapter 6.3 in this section.We will prove the Tate duality theorem which will allow us to complete the proof of the existence theorem.

Lemma 7.3.1. If $(\chi, f) = 0$ for all $f \in F^\times$, then χ is the trivial character.

Proof. By proposition $6.3.1$, we see that $N_L = F^\times$ where L is the field corresponding to the kernel of χ. However, we also have that $N_F = F^\times$. By Theorem 7.2.3, $L = F$ so the kernel of χ is all of $\mathrm{Gal}(\overline{F}/F)$. □

Theorem 7.3.2 (Tate duality)**.** Let F be a local field containing a primitive lth root of unity. The pairing $H^1(F, \mathbb{F}_l) \times H^1(F, \mathbb{F}_l) \to \mathbb{F}_l$ given by $([a], [b]) \mapsto (a, b)$ is non-degenerate. Here, we write $[a]$ for the image of $F^\times$ under $F^\times \twoheadrightarrow F^\times/F^{\times l} \cong H^1(F, \mathbb{F}_l)$.

Proof. Given $[a] \in H^1(F, \mathbb{F}_l)$ which is a non-zero class, we need to show that there exists $[b] \in H^1(F, \mathbb{F}_l)$ such that $(a, b) \neq 0$. Suppose for contradiction that this is not true; then for all $b \in F^\times$, $(a, b) = (\chi_a, b) = 0$. By the previous lemma, χ_a must be trivial character and examining the definition of χ_a, we see that this implies $\sigma(\sqrt[l]{a}) = \sqrt[l]{a}$ for all $\sigma \in \mathrm{Gal}(\overline{F}/F)$. Then, by Galois theory, $\sqrt[l]{a} \in F^\times$ which implies that $[a] = 0$, a contradiction. □

Definition 7.3.1 (Universal norms)**.** The group of universal norms of a local field F is the subgroup D_F of $F^\times = \cap N_L$ where the intersection runs through all finite extensions L/F.

Our goal is to prove that D_F is the trivial group. For this, we need:

Lemma 7.3.3. For any finite extension E/F, we have $N_{E/F}(D_E) = D_F$

Proof. Let $x \in D_E$ and let $y = N_{E/F}(x)$. For any finite extension L/F, consider the compositum EL. Then $x = N_{EL/E}(z)$ for some $z \in EL$ which implies, by transitivity of norms, that $y = N_{EL/F}(z)$. Since $L \subseteq EL$, by transitivity of norms again, we see that y is norm from L. Thus, $y \in D_F$.
Converseley, pick $a \in D_F$. For any finite extension L/E, set $K(L) := N_{L/E}(L^\times) \cap N_{E/F}^{-1}(a)$. To prove this inclusion, it suffices to show that the intersection of $K(L)$ as L runs through all finite extensions L/E is non-empty. The crucial observation is the following:
Claim: $K(L)$ is compact with respect to the topology on $E^\times$.
Proof of claim: For $n \in \mathbb{Z}$, let $F_n \subseteq F^\times$ consist of all elements of valuation n; then $\{F_n\}_{n \in \mathbb{Z}}$ forms an open cover of $F^\times$. If f_n is any element of valuation n, we have $F_n = f_n \mathcal{O}_F^\times$; thus each F_n is also compact. Similarly, each subset $N_{E/F}^{-1}(F_n)$

is either empty or a translate of $\mathcal{O}_E^\times$, so it is always compact. Now if C is a compact subspace of $F^\times$, then it is covered by finitely many F_n's and we see that $N_{E/F}^{-1}(C)$ is closed and contained in a compact subspace, so it is itself compact. We have thus shown that $N_{E/F}$ is a proper map. Thus, $N_{E/F}^{-1}(a)$ is compact. We now use a result from the theory of metric spaces: a proper map $f : X \to Y$ between metric spaces must have a closed image. Applying this to $f = N_{L/E}$, we see that $N_{L/E}(L^\times)$ is closed in $E^\times$. Thus, $K(L)$ is compact and we have proven the claim.
Now suppose for contradiction that the intersection of all the sets $K(L)$ were empty. Then the sets $K(E) \cap K(L)$ where L runs through the finite extensions of E, are closed subsets having empty intersection. By compactness, there must exist $L_1, \ldots, L_k$ such that $K(E) \cap K(L_1) \cap \cdots \cap K(L_k) = \emptyset$. Let L_0 be the compositum of $L_1, \ldots, L_k$. Since $K(L_0) \subseteq K(L_i)$ by transitivity of norms, it suffices to prove that $K(L_0)$ is non-empty to reach a contradiction. However, $K(L_0)$ is indeed non-empty since $a \in D_F$ is a norm from L_0.

□

Theorem 7.3.4. For a local field F, the group D_F of universal norms is trivial.

Proof. The key point is to show that D_F is a divisible subgroup of $F^\times$; then by Corollary 3.4.1.3, D_F must be trivial. We now proceed to show prove that D_F is divisible.
Let l be any prime number and let F_l be obtained by adjoining the lth roots of unity to F. Pick any $f \in D_F$ and choose a field E containing F_l. By the previous proposition, we have $f = N_{E/F}(b)$ for some $b \in D_E$. Then b is in the kernel of $e \mapsto (\chi, e)$ for any character χ since this kernel is a norm subgroup by Proposition 6.3.1. In particular, $(e, b) = 0$ for any $e \in E^\times$. Tate duality implies that $b = x^l$ for some $x \in E^\times$. Apply the norm map $N_{E/F}$ to the equation $b = x^l$ to obtain $f = y^l$ where $y = N_{E/F}(x)$. Set $K(E) := \{z \in F^\times : z^l = f\} \cap N_E$ which is thus non-empty and also finite. It follows that $K(E')$ is also finite for any $F \subseteq E' \subseteq E$, since $K(E) \subseteq K(E')$. An argument similar to the previous proof thus shows that the intersection of all the sets $K(E)$, where E runs over all finite extensions of F, is non-empty. Thus, $f = z^l$ for some $z \in D_F$. Since this is true for all primes, D_F is a divisible subgroup of $F^\times$ as desired. □

We now complete the proof of local class field theory by completing Step 5, namely we complete the proof of the existence theorem by showing surjectivity.

Theorem 7.3.5 (Existence theorem)**.** Let A be a subgroup of finite index in $F^\times$. Then there exists an abelian extension L/F such that $A = N_L$.

Proof. First consider a special case when A contains $\mathcal{O}_F^\times$. Since $\mathcal{O}_F^\times$ is the kernel of the valuation map $v : F^\times \to \mathbb{Z}$, we see that A must be of the form $v^{-1}(n\mathbb{Z})$ for some $n \geq 1$. By Proposition 6.1.3, $A = N_{E_n}$ where E_n is the unique unramified extension of F of degree n. We have thus proven the theorem in the special case. To prove the general case, we first make the following claim:
Claim: We can find a norm subgroup N such that $N \cap \mathcal{O}_F^\times \subseteq A$.
Proof of claim: First note that $\bigcap N \cap \mathcal{O}_F^\times = \{1\}$, where the intersection is taken over all norm subgroups, since the left hand side is contained in D_F which is trivial by Theorem 7.3.4 . Since each norm subgroup has finite index by the Reciprocity theorem, we can apply corollary 3.4.1.2 to conclude that each norm subgroup is open and closed. The same corollary shows that A is open and closed. Let $C := F^\times \setminus A$; so C is closed and note that the various closed subsets $C \cap N \cap \mathcal{O}_F^\times$ of the space $\mathcal{O}_F^\times$ have empty intersection. Since $\mathcal{O}_F^\times$ is compact, there must exists finitely many norm subgroups $N_1, \cdots, N_r$ such that $C \cap N_1 \cdots \cap N_r \cap \mathcal{O}_F^\times = \emptyset$. Settting $N := N_1 \cap \ldots \cap N_r$, we note that N is a norm subgroup by Lemma 7.2.2 and that $N \cap \mathcal{O}_F^\times \subseteq A$, thus proving the claim.
Let N be the norm subgroup obtained from the claim. Let $A_N := (A \cap N) \cdot \mathcal{O}_F^\times$. Then A_N must have finite index since it contains $A \cap N$ and both A and N have finite index. By the special case, A_N is a norm subgroup. Now pick any $a \in N \cap A_N \subseteq A_N$. Then $a = a_1 a_2$, where $a_1 \in A \cap N$ and $a_2 \in \mathcal{O}_F^\times$. Then $a_2 = a a_1^{-1}$ lies in $N \cap \mathcal{O}_F^\times$; by the claim $a_2 \in A$ as well. Thus $a = a_1 a_2$ lies in A and so $N \cap A_N \subseteq A$. Finally, $N \cap A_N$ is a norm subgroup by Lemma 7.2.2 and so is A by Corollary 7.2.3.1.

□

7.4 Applications and concluding remarks

Class field theory has been one of the major achievements of 20th century algebraic number theory and the theorems of the subject can be seen as milestones in themselves for their sheer depth and profundity. Nevertheless, in this section we give some rather concrete results that class field theory allows us to make. Perhaps the most spectacular of all such statements is the Local-Kronecker Weber theorem which states that every abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension of $\mathbb{Q}_p$.

We first state the following lemma as a preparation. Its proof is rather long and computational, so we do not include it here. The unit groups $U_{\mathbb{Q}_p}^{(n)}$ of $\mathbb{Q}_p$ are denoted $U^{(n)}$.

Lemma 7.4.1. Let $K = \mathbb{Q}_p(\zeta_{p^n})$ for some $n \in \mathbb{N}_{\geq 1}$. Then $N_K = \langle p \rangle \times U^{(n)}$.

Proof. See [Gui2018, Lemma 13.28]. □

Theorem 7.4.2 (Local Kronecker-Weber theorem)**.** If $L/\mathbb{Q}_p$ is a finite abelian extension, then $L \subseteq \mathbb{Q}_p(\zeta_n)$ where $n \in \mathbb{N}$ is a natural number and ζ_n is a primitive nth-root of unity.

Proof. Recall that by Corollary 3.4.1.2, N_L contains a subgroup of the form $\langle p^m \rangle \times U^{(n)}$ for some integers m, n. Write this as $\langle p^m \rangle \times U^{(n)} = (\langle p^m \rangle \times \mathbb{Z}_p^\times) \cap (\langle p \rangle \times U^{(n)}) = N_{L_1} \cap N_{L_2}$.
By Lemma 7.4.1 above, $\langle p \rangle \times U^{(n)} = N_{L_2}$, where $L_2 = \mathbb{Q}_p(\zeta_{p^n})$. Let $N = p^m - 1$ and let $L_1 = \mathbb{Q}_p(\zeta_N)$. Then by Theorem 3.3.3, we know that $L_1/\mathbb{Q}_p$ is unramified of degree m. By Proposition 6.1.3, $N_{L_2} = v_p^{-1}(m\mathbb{Z}) = \langle p^m \rangle \times \mathbb{Z}_p^\times$.
Thus, what we have shown is $N_{L_1} \cap N_{L_2} = \langle p^m \rangle \times U^{(n)}$. Thus, by local class field theory, we have $N_{L_1} \cap N_{L_2} = N_{L_1 L_2} \subseteq N_L$ and so $L \subseteq L_1 L_2 = \mathbb{Q}_p(\zeta_{(N \cdot p^n)})$. □

As a final application, we prove the following theorems:

Theorem 7.4.3. When p is odd, there exist $p + 1$ abelian extensions of $\mathbb{Q}_p$ of degree p.

Proof. By the existence theorem of local class field theory, the number of abelian extenions of degree p of $\mathbb{Q}_p$ is in one-to-one correspondence with subgroups of $\mathbb{Q}_p^\times$ of index p. Moreover, any subgroup of index p in $\mathbb{Q}_p^\times$ must contain $(\mathbb{Q}_p^\times)^p$ since elements here are zero in the quotient. The problem is thus reduced to finding the number of subgroups of index p in $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$.
We know from Proposition 3.4.2 that $\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$ and so $(\mathbb{Q}_p^\times)^p \cong p\mathbb{Z} \times p\mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}$; thus $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In this group, a subgroup of index p is a subgroup of order p. Any element $(a, b) \neq (0, 0)$ generates such a subgroup of order p and (ca, cb) generate the same subgroup for $c \in (\mathbb{Z}/p\mathbb{Z})^\times$. Hence, the number of subgroups of order p equals $\frac{p^2-1}{p-1} = p + 1$. □

Theorem 7.4.4. When p =2, there exist 7 abelian extensions of $\mathbb{Q}_2$ of degree 2.

Proof. The idea of the proof is similar to that of the previous theorem; we are thus reduced to finding the number of subgroups of index 2 in $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$. By Proposition 3.4.2, $\mathbb{Q}_2^\times \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ and so $(\mathbb{Q}_2^\times)^2 \cong 2\mathbb{Z} \times 2\mathbb{Z}_2$; thus

$$\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

. We can thus regard $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ as a dimension 3 vector space over $\mathbb{Z}/2\mathbb{Z}$ and so the problem is reduced to finding the number of 2-dimensional subspaces of this vector space. Any 2 dimensional subspace would have 2 linearly independent elements and so there are (8-1) × (8-2)=42 ways of picking 2 linearly independent elements. Each dimension 2 subspace has 3 × 2=6 number of bases and so the number of 2 dimensional subspaces of $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$= 42/6=7 as required. □

Bibliography

[Fre2017] J.Fresan, "Class Field Theory."[Online]. Available:https://metaphor.ethz.ch/x/2017/fs/401-3106-17L/nm/CFT1.pdf

[Gui2018] P.Guillot, *A Gentle Course in Local Class Field Theory: Local Number Fields, Brauer Groups, Galois Cohomology*. Cambridge University Press, 2018.

[Gou1991] F.Gouvea, *p-adic Numbers: An Introduction*. Springer Verlag Berlin Hiedelberg, 1991.

[KKS2000] K.Kato, N.Kurokawa, T.Saito, *Number Theory 1: Fermat's dream*, American Mathematical Society, Providence, Rhode Island, 2000.

[KKS2011] K.Kato, N.Kurokawa, T.Saito, *Number Theory 2: Introduction to Class Field Theory*, American Mathematical Society, Providence, Rhode Island, 2011.

[Neu1986] J.Neukirch, *Class Field Theory*. Springer Verlag Berlin Hiedelberg, 1986.

[Sha] R.Sharifi, "Group and Galois Cohomology". [Online]. Available: http://math.ucla.edu/~sharifi/groupcoh.pdf