Topics in Galois Cohomology

Lambert A'Campo
01570095

Supervised by Alexei Skorobogatov

2018/2019

Abstract

Group cohomology appears in many different number theoretic questions and has various interpretations which make the theory very versatile and give rise to surprising connections. We will see some general methods for working with group cohomology as shown in [9] and [21]. Central results are Hilbert's Theorem 90, restriction-corestriction and the inflation-restriction sequence.

These methods then accompany us throughout the rest of the text where we see how to use them in number theory. In most cases concrete consequences about diophantine equations, for example the weak Mordell-Weil theorem, can be derived from the theory. Further, we outline some of the connections between group cohomology, Galois Descent and central simple algebras, our main source being [9].

Moving on we prove local class field theory like in [16] and [5] and we state what carries over to the global case where we encounter certain local-global principles and Artin reciprocity which is a vast generalisation of the famous law of quadratic reciprocity. In particular, we show how these generalised reciprocity laws can be used to give restrictions on hypothetical solutions to the Fermat equation as in [15]. Finally we give an original proof of the Artin-Schreier theorem based on the much deeper Merkurjev-Suslin theorem.

Acknowledgements

I thank Alexei Skorobogatov for giving me so much freedom while working on this project, for suggesting great books and for spending many hours on finding a mistake I couldn't manage to find myself. I thank my parents for reading a draft of this thesis and offering constructive feedback. Finally, I owe my gratitude to Wojtek Wawrow who gave helpful comments on my text which simplified a few proofs and for suggesting how to elementarily prove that infinitely many primes split in a non-trivial extension of number fields.

Declaration

The work contained in this thesis is my own unless otherwise stated.

Contents

1 Introduction **4**

2 Group Cohomology **5**

2.1 Some Resolutions 5

2.2 Hilbert's Theorem 90 7

2.3 Cohomology of Cyclic Groups 10

2.4 Functorial Properties 11

2.5 The Cup Product 16

2.6 Profinite Group Cohomology 20

2.7 Galois Cohomology 26

2.8 Cohomological Dimension 29

3 Nonabelian Cohomology **33**

3.1 Galois Descent 34

3.2 Principal Homogeneous Spaces 38

4 Central Simple Algebras **41**

4.1 The Brauer Group 43

5 Local Class Field Theory **48**

5.1 The Cohomology of a Local Field 48

5.2 Abelian Extensions 53

5.3 ℓ-Extensions 60

6 Global Class Field Theory **63**

6.1 The Fundamental Exact Sequence 64

6.2 Global Norm Groups 69

6.3 The Power Residue Symbol 72

6.4 Application to Fermat's Last Theorem 75

7 The Structure of Absolute Galois Groups **78**

7.1 The Bloch-Kato Conjecture 78

1 Introduction

The starting point of this text are Diophantine equations, that is polynomial equations with integer coefficients for which we seek solutions in the integers or rational numbers. This is an ancient subject, and an almost endless supply of very different tools have been developed to study such equations. We will look at the subject from the perspective of homological algebra. Let us start with some simple examples.

Consider the equation $x^2 + y^2 = 1$. The rational solutions are precisely pairs of the form $x = \frac{a^2-b^2}{a^2+b^2}, y = \frac{2ab}{a^2+b^2}$ with $a, b \in \mathbb{Z}$. There is a simple geometric proof by choosing the rational point $(-1, 0)$ on the circle and then drawing lines with rational slopes through this point. But one can also see Galois Cohomology here. The equation can be rewritten as $N(x + iy) = 1$, where N is the norm of the extension $\mathbb{Q}(i)/\mathbb{Q}$ and solving the equation is equivalent to determining the kernel of $N : \mathbb{Q}(i)^\times \to \mathbb{Q}^\times$.

Here we reach the first theorem of Galois Cohomology: Hilbert's Theorem 90. It states that the kernel of $N_{K/\mathbb{Q}}$ where $K/\mathbb{Q}$ is a cyclic extension consists precisely of elements of the form $\alpha = \beta/\sigma(\beta)$, where σ is a generator of $\mathrm{Gal}(K/\mathbb{Q})$. One can use this to recover the parametrisation of Pythagorean triples. Hilbert's Theorem 90 itself has been generalised in many directions, in particular it can be interpreted as the vanishing of a certain cohomology group. Using this vanishing one can then easily derive the theory of Kummer and Artin-Schreier extensions which are a central ingredient in the proof that solvable Galois groups correspond to equations which can be solved by radicals.

Thus we are able to solve a Diophantine problem because there is more algebraic structure than in just a random equation. This is a general theme in this subject. One exploits certain algebraic structures and their interaction with Galois groups to solve number theoretic problems. Note that the negative answer to Hilbert's 10th problem by Yuri Matiyasevich shows that there is no theory of random equations so one has to study special classes of equations. A key example of using algebra to solve diophantine equations is Galois Descent. One has two structures over a field K, for example curves and a Galois extension L/K. If the structures are isomorphic over L they are not necessarily isomorphic over K but cohomology precisely classifies all possible obstructions. This can be used to answer whether certain curves have a rational point or not by studying an elliptic curve which is only isomorphic to the original curve over a larger field. For example that $3x^3 + 4y^3 + 5z^3 = 0$ has no rational points can be shown by studying the curve $x^3 + y^3 + 60z^3 = 0$ which has a rational point!

Probably the most impressive application of group cohomology to number theory is class field theory which in some sense classifies the abelian extensions of a local or global field. As a famous consequence we derive the Kronecker-Weber theorem which states that the maximal abelian extension of $\mathbb{Q}$ is given by adjoining all roots of unity to $\mathbb{Q}$. The modern way of proving class field theory is by first proving it for local fields and then deriving the global theory by studying what happens in all the completions. This gives rise to local-global principles like the Hasse Principle which states that a ternary quadratic form has a solution over $\mathbb{Q}$ if and only if it has solutions in $\mathbb{Q}_p$ for all p and in $\mathbb{R}$. One also recovers quadratic reciprocity and more generally for any monic polynomial $f \in \mathbb{Z}[x]$ whose splitting field is abelian over $\mathbb{Q}$ one can find congruence conditions to determine when f has roots modulo a prime p.

2 Group Cohomology

Galois Cohomology is a special case of group cohomology which we introduce in this section. To find solutions to diophantine equations is equivalent to finding solutions which are fixed under the action of a Galois group G. This is why it is natural to study the functor $A \mapsto A^G$ which sends an $\mathbb{Z}[G]$-module A to its G-invariants. This is a left exact functor and so homological algebra tells us that it is fruitful to study the right derived functors which will be exactly the group cohomology.

For example, taking mth powers is surjective in an algebraically closed field and so there is an exact sequence

$$1 \to \mu_m \to \overline{\mathbb{Q}}^\times \xrightarrow{m} \overline{\mathbb{Q}}^\times \to 1.$$

The corresponding sequence of $G_{\mathbb{Q}}$-invariants is not exact anymore but it can be extended to a long exact sequence in cohomology and so we get information about the mth powers in $\mathbb{Q}$. This leads to the theory of Kummer extensions and similar ideas give rise to a proof of the Mordell-Weil theorem on Elliptic Curves. In this chapter we outline the theory of group cohomology as presented in [9], [19] and [21].

2.1 Some Resolutions

Let G be a group and let $\mathbb{Z}[G] = \bigoplus_{g \in G} g\mathbb{Z}$ be its group ring with multiplication induced by the group operation in G. A $\mathbb{Z}[G]$-module is the same as an abelian group with an action of G by automorphisms. By letting G act trivially, any abelian group becomes an $\mathbb{Z}[G]$-module. For example we do this for $\mathbb{Z}$ in the following definition.

Definition 2.1.1. *Let A be a $\mathbb{Z}[G]$-module and $q \geq 0$ an integer, then we define the cohomology and homology groups by*

$$H^q(G, A) := \mathrm{Ext}^q_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$
$$H_q(G, A) := \mathrm{Tor}^{\mathbb{Z}[G]}_q(\mathbb{Z}, A).$$

$A \mapsto H^q(G,A)$ is the qth right derived functor of

$$A \mapsto A^G = \{a \in A : \mathrm{Stab}(a) = G\} = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A)$$

and $A \mapsto H_q(G,A)$ is the qth left derived functor of

$$A \mapsto A_G = A/\langle a - ga : a \in A, g \in G\rangle = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A.$$

See [4] for the theory of derived functors and in particular of Tor and Ext. We will almost exclusively study the cohomology groups $H^q(G,A)$ and homology will only briefly appear in our treatment of class field theory. To compute $H^q(G,A) = \mathrm{Ext}^q_{\mathbb{Z}[G]}(\mathbb{Z}, A)$ we need a projective resolution of $\mathbb{Z}$.

Lemma 2.1.2. *There is a free resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module with trivial action of G*

$$\cdots \to \mathbb{Z}[G^3] \xrightarrow{d} \mathbb{Z}[G^2] \xrightarrow{d} \mathbb{Z}[G] \xrightarrow{d} \mathbb{Z} \to 0,$$

with $d(g_0, \ldots, g_q) = \sum_{i=0}^q (-1)^i (g_0, \ldots, \hat{g}_i, \ldots, g_q)$ for $q > 0$ and $g_i \in G$, where the $\hat{g}_i$ indicates that we leave out this index. The map $d : \mathbb{Z}[G] \to \mathbb{Z}$ is defined by mapping $g \mapsto 1$ for all $g \in G$. Here G acts diagonally on $\mathbb{Z}[G^{q+1}]$.

Proof. Let S be a set of right coset representatives of $G < G^{q+1}$, then S is a $\mathbb{Z}[G]$ basis of $\mathbb{Z}[G^{q+1}]$ and so the resolution is free.

We have $d^2 = 0$ since

$$\begin{aligned} d^2(g_0, \ldots, g_q) &= \sum_{j<i} (-1)^{i+j} (g_0, \ldots, \hat{g}_j, \ldots, \hat{g}_i, \ldots, g_q) \\ &+ \sum_{i<j} (-1)^{i+j-1} (g_0, \ldots, \hat{g}_i, \ldots, \hat{g}_j, \ldots, g_q) \end{aligned}$$

and those sums cancel.

To show exactness we prove that the identity $\mathbb{Z}[G^\bullet] \to \mathbb{Z}[G^\bullet]$ is nullhomotopic. Such a nullhomotopy is given by $h_q : \mathbb{Z}[G^q] \to \mathbb{Z}[G^{q+1}] : (g_1, \ldots, g_q) \mapsto (1, g_1, \ldots, g_q)$, because then

$$\begin{aligned} (dh_{q+1} + h_q d)(g_0, \ldots, g_q) &= d(1, g_0, \ldots, g_q) + \sum_{i=0}^{q} (-1)^i h_q(g_0, \ldots, \hat{g}_i, \ldots, g_q) \\ &= (g_0, \ldots, g_q) + \sum_{i=1}^{q+1} (-1)^i (1, g_0, \ldots, \widehat{g_{i-1}}, \ldots, g_q) \\ &+ \sum_{i=0}^{q} (-1)^i (1, g_0, \ldots, \hat{g}_i, \ldots, g_q) = (g_0, \ldots, g_q). \end{aligned}$$ □

Definition 2.1.3. *We denote the resolution from the previous lemma by $P_\bullet(G) \to \mathbb{Z} \to 0$. The indexing is chosen such that $P_n(G) = \mathbb{Z}[G^{n+1}]$ for $n \geq 0$.*

Definition 2.1.4 (inhomogeneous cochains)**.** *Let G be a group and A a $\mathbb{Z}[G]$-module, then let $C^q(G,A)$ denote the abelian group of functions $G^q \to A$ for $q \geq 0$.*

Lemma 2.1.5. *There is an isomorphism $C^\bullet(G,A) \cong \mathrm{Hom}_G(P_\bullet(G),A)$ such that under this isomorphism the differential d becomes*

$$\begin{aligned}(df)(g_1,\dots,g_q) =& g_1 f(g_2,\dots,g_q)\\ &+\sum_{i=1}^{q-1}(-1)^i f(g_1,\dots,g_ig_{i+1},\dots,g_q) + (-1)^q f(g_1,\dots,g_{q-1}).\end{aligned}$$

Proof. Note that the elements

$$[g_1,\dots,g_q] := (1, g_1, g_1g_2,\dots,g_1g_2\dots g_q).$$

form a $\mathbb{Z}[G]$-basis of $\mathbb{Z}[G^{q+1}] = P_q(G)$. This choice of basis induces an isomorphism $C^q(G,A) \cong \mathrm{Hom}_G(P_q(G),A)$ and we have

$$d([g_1,\dots,g_q]) = g_1[g_2,\dots,g_q] + \sum_{i=1}^{q-1}(-1)^i[g_1,\dots,g_ig_{i+1},\dots,g_q] + (-1)^q[g_1,\dots,g_{q-1}],$$

as required. □

Corollary 2.1.6. *Let G be a group and A a $\mathbb{Z}[G]$-module, then*

$$H^1(G,A) = \{f : G \to A \mid f(gh) = gf(h) + f(g)\}/\{g \mapsto ga - a \mid a \in A\}.$$

Proof. We have $d : C^1(G,A) \to C^2(G,A) : f \mapsto df(g,h) = gf(h) - f(gh) + f(g)$ and $d : C^0(G,A) \to C^1(G,A) : a \mapsto (g \mapsto ga - a)$. □

Corollary 2.1.7. *In particular if the action of G on A is trivial, then $H^1(G,A) =$ $\mathrm{Hom}(G,A)$.*

2.2 Hilbert's Theorem 90

As a first application of group cohomology we discuss Hilbert's Theorem 90, an important result in Galois Theory. It can simply be interpreted as the vanishing of $H^1(\mathrm{Gal}(L/K), L^\times)$ where L/K is a finite Galois extension. It is a key building block of Galois Cohomology and we will apply it frequently in this text.

Lemma 2.2.1. *Let G be a group, L a field and S a finite set of homomorphisms $G \to L^\times$, then S is linearly independent in the L-vector space of functions $G \to L$.*

Proof. When $S = \{\tau\}$, then $a\tau(e) = 0$ implies $a = 0$. Now suppose the claim of the lemma is false. Then we take a counterexample where S has minimal cardinality which is > 1 since the case $|S| = 1$ has already been established. Suppose we have a nontrivial linear relation

$$\sum_{s \in S} a_s s \equiv 0,$$

for some $a_s \in L$. Since the relation was nontrivial and the $|S| = 1$ case is already proven there must be $\sigma \neq \tau \in S$ such that $a_\tau \neq 0, a_\sigma \neq 0$. Let $h \in G$ such that $\sigma(h) \neq \tau(h)$, then

$$\sum_{s \in S} a_s s(hg) = \sum_{s \in S} a_s s(h) s(g) = 0,$$

for all $g \in G$. Subtracting the first relation times $\tau(h)$ we get another linear relation with coefficients $a_s(s(h) - \tau(h))$ which is nontrivial since $\sigma(h) \neq \tau(h)$ and $a_\sigma \neq 0$. It is also shorter than the original relation since for $s = \tau$ we have $a_s(s(h) - \tau(h)) = 0$. This is a contradiction to the minimality of S. □

Theorem 2.2.2 (Hilbert's Theorem 90). *Let $K \subset L$ be a finite Galois extension with Galois group G, then $H^1(G, L^\times) = 0$, where we view $L^\times$ as a G-module in the natural way.*

Proof. Let $f \in C^1(G, L^\times)$ be a cocycle, i.e. $f(g_1 g_2) = (g_1 \cdot f(g_2)) f(g_1)$ for all $g_1, g_2 \in G$ (in multiplicative notation). The previous lemma applied to the group $L^\times$ shows that the homomorphism

$$\sum_{\tau \in G} f(\tau)\tau : L \to L$$

is non-zero since f takes non-zero values and G is a finite set of homomorphisms $L^\times \to L^\times$. Thus there is $\theta \in L$ such that

$$\beta := \sum_{\tau \in G} f(\tau)\tau(\theta) \neq 0.$$

Now we compute for any $\sigma \in G$

$$\sigma(\beta) = \sum_{\tau \in G} \sigma(f(\tau))\sigma\tau(\theta) = \sum_{\tau \in G} f(\sigma\tau) f(\sigma)^{-1} \sigma\tau(\theta) = \beta f(\sigma)^{-1}.$$

Hence $f(\sigma) = \beta / \sigma(\beta)$ is a coboundary. □

Corollary 2.2.3 (Original Hilbert's Theorem 90). *Let L/K be a finite Galois extension with cyclic Galois group generated by σ. Then every element $x \in L$ such that $N_{L/K}(x) = 1$ is of the form $y/\sigma(y)$, for some $y \in L^\times$.*

Proof. Let $x \in L$ such that $N_{L/K}(x) = 1$, then consider the map f given by $\sigma^n \mapsto \sigma^{n-1}(x)\sigma^{n-2}(x) \ldots x$. f is well defined since x is of norm one. It is a cocycle since for all integers m and k

$$f(\sigma^k \sigma^m) = \sigma^{k+m-1}(x) \ldots \sigma^k(x) \sigma^{k-1}(x) \ldots x = \sigma^k(f(\sigma^m)) f(\sigma^k).$$

By Hilbert's Theorem 90 there is a $y \in L$ such that $x = f(\sigma) = y/\sigma(y)$. □

Corollary 2.2.4. *Let $K \subset L$ be a finite Galois extension of degree d with Galois group generated by σ and let $\alpha_1, \dots, \alpha_d$ be a basis of L over K, then $V = \{x \in L : N_{L/K}(x) = 1\}$ is in bijective correspondance with $\mathbb{P}^{d-1}(K)$ via the map $\mathbb{P}^{d-1}(K) \to V$ given by*

$$[u_1, \dots, u_d] \mapsto \frac{\sum_{i=1}^d u_i\alpha_i}{\sum_{i=1}^d u_i\sigma(\alpha_i)}$$

Proof. By the original form of Hilbert's Theorem 90 the map is surjective. To show injectivity, let $z, w \in L^\times$ such that $z/\sigma(z) = w/\sigma(w)$ and set $\alpha = z/w$. Then $\sigma(\alpha) = \sigma(z)/\sigma(w) = \alpha$ is fixed by the Galois group, which is generated by σ. So $\alpha \in K$ and w and z have the same K-span i.e. are equivalent in $\mathbb{P}^{d-1}(K)$. □

Example 2.2.5. *There is a bijective map from $\mathbb{P}^1(\mathbb{Q})$ to the rational points on the circle $x^2 + y^2 = 1$ given by*

$$[a, b] \to \left(\frac{a^2 - b^2}{a^2 + b^2}, \frac{2ab}{a^2 + b^2}\right).$$

Proof. Let $(x, y) \in \mathbb{Q}^2$, then $x + iy \in \mathbb{Q}(i)$ has norm 1 if and only if $x^2 + y^2 = 1$. Since $\mathbb{Q}(i)/\mathbb{Q}$ is a cyclic Galois extension we conclude from the previous corollary that there is a bijection from $\mathbb{P}^1(\mathbb{Q})$ to the rational points on the circle given by

$$[a, b] \mapsto \frac{a + ib}{a - ib} = \frac{a^2 - b^2}{a^2 + b^2} + i\frac{2ab}{a^2 + b^2}.$$ □

Example 2.2.6. *There is a bijective map from $\mathbb{P}^2(\mathbb{Q})$ to the rational solutions of*

$$x^3 - xy^2 + 2y^3/3 + xz^2 - 2yz^2/3 + 4z^3/9 + 2x^2z - 2xyz = 1.$$

Proof. Let K be the splitting field of $f = x^3 - x - 2/3$ over $\mathbb{Q}$, then $K/\mathbb{Q}$ is a Galois extension of degree 3 (because $\operatorname{disc} f = 16$ is a square). Let α be a root of f, then

$$N_{K/\mathbb{Q}}(x + y\alpha + z\alpha^2) = x^3 - xy^2 + 2y^3/3 + xz^2 - 2yz^2/3 + 4z^3/9 + 2x^2z - 2xyz.$$

To actually compute the bijection we would have to express the other roots of f in terms of α. □

Example 2.2.7. *Let ω be a primitive 3rd root of unity. Then there is a bijective map from $\mathbb{P}^2(\mathbb{Q}(\omega))$ to the $\mathbb{Q}(\omega)$-solutions to the equation $x^3 + 2y^3 + 4z^3 = 6xyz + 1$.*

Proof. This follows from the fact that $N(x + y2^{1/3} + z4^{1/3}) = x^3 + 2y^3 + 4z^3 - 6xyz$ and that $\mathbb{Q}(2^{1/3}, \omega)/\mathbb{Q}(\omega)$ is a cyclic Galois extension. □

When we see profinite group cohomology, Hilbert's Theorem 90 will imply Kummer Theory and Artin-Schreier Theory and it plays an important role in the study of central simple algebras.

2.3 Cohomology of Cyclic Groups

With Hilbert's Theorem 90 we already saw a connection between cohomology and the norm map. This is a general phenomenon for cyclic groups.

Definition 2.3.1. *Let G be a finite group and A a $\mathbb{Z}[G]$-module, then we define the norm map as $N : A \to A : x \mapsto \sum_{g \in G} gx$.*

The reason that the cohomology of cyclic groups is simple is the following special resolution of $\mathbb{Z}$ which allows us to easily compute the cohomology of cyclic groups. For example this is used in later chapters to prove class field theory.

Lemma 2.3.2. *Let $G = \langle \sigma \rangle$ be a finite cyclic group, then*

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

is a free resolution of $\mathbb{Z}$, where the map $\mathbb{Z}[G] \to \mathbb{Z}$ is defined by mapping $g \mapsto 1$ for all $g \in G$.

Proof. Let $n = |G|$, then $\mathbb{Z}[G] \cong \mathbb{Z}[x]/(x^n - 1)$ and so clearly the kernel of the last map is the image of multiplication by $\sigma - 1$. The exactness at the other terms follows from the factorisation $(x-1)(1 + x + \dots + x^{n-1}) = x^n - 1$ and the fact that N is multiplication by $1 + x + \dots + x^{n-1}$. □

Corollary 2.3.3. *$H^{q+2}(G, A) \cong H^q(G, A)$ for $q \geq 1$ when G is a finite cyclic group and $H^q(G, A) \cong \ker N/(\sigma - 1)A$ if q is odd and $H^q(G, A) \cong A^G/N(A)$ if q is even.*

Example 2.3.4. *If L/K is a cyclic extension with group $G = \langle \sigma \rangle$, then by Hilbert's Theorem 90 $\ker N/(\sigma-1)L^\times = H^1(G, L^\times) = 0$ and we recover the original statement of Hilbert's Theorem 90.*

Example 2.3.5. *Let $G = \langle \sigma \rangle$ be a finite cyclic group of order n and A an abelian group viewed as $\mathbb{Z}[G]$-module with trivial G-action, then $N : \mathbb{Z} \to \mathbb{Z}$ is multiplication by $n = |G|$ and multiplication by $(\sigma - 1)$ is the zero map, hence $H^1(G, \mathbb{Z}) \cong A[n]$ and $H^2(G, A) = A/nA$.*

Definition 2.3.6 (Herbrand quotient)**.** *Let G be a finite cyclic group and A a $\mathbb{Z}[G]$-module, then we define*

$$h(A) = |H^2(G, A)|/|H^1(G, A)|$$

whenever both numerator and denominator are finite.

Lemma 2.3.7. *Let $0 \to A \to B \to C \to 0$ be a short exact sequence, then $h(B) = h(A)h(C)$.*

Proof. From the resolution 2.3.2 we get an exact hexagon

$$\begin{tikzcd}
& H^1(G,A) \arrow[r] & H^1(G,B) \arrow[dr] & \\
H^2(G,C) \arrow[ur] & & & H^1(G,C) \arrow[dl] \\
& H^2(G,B) \arrow[ul] & H^2(G,A) \arrow[l] &
\end{tikzcd}$$

and as a result

$$|H^2(G,A)||H^2(G,C)||H^1(G,B)| = |H^1(G,A)||H^1(G,C)||H^2(G,B)|$$

which implies $h(B) = h(A)h(C)$. □

Lemma 2.3.8. *If A is finite, then $h(A) = 1$.*

Proof. Let σ be a generator of G, then $H^1(G,A) = \ker N/(\sigma - 1)$ and $H^2(G,A) = \ker(\sigma - 1)/N$. Moreover, $|A| = |\ker N||N(A)| = |\ker(\sigma - 1)||(\sigma - 1)A|$ and the claim follows. □

2.4 Functorial Properties

A powerful method in group cohomology is 'dévissage' to the case of a cyclic group which, as shown above, have a very simple cohomology theory. The idea is that if G is solvable for example, then we have a normal subgroup $H < G$ and we would like to understand how $H^q(G,A)$ depends on $H^q(H,A)$ and $H^q(G/H,A^H)$. And even more generally, it is often useful to know what happens with a group homomorphism $G \to G'$ on cohomology. There are a few natural maps which we now define.

Definition 2.4.1 (Functorial Pair). *Let G and G' be groups, A a $\mathbb{Z}[G]$-module, A' a $\mathbb{Z}[G']$-module, $f : G \to G'$ a group homomorphism and $\psi : A' \to A$ a homomorphism of abelian groups which is compatible with f, i.e. $\psi(f(g)a') = g\psi(a')$ for all $g \in G$. There is a natural chain map $f_\# : P_\bullet(G) \to P_\bullet(G')$ induced by f. Now precomposing with ψ gives a chain map $\mathrm{Hom}(P_\bullet(G'), A') \to \mathrm{Hom}(P_\bullet(G), A)$. The induced map on cohomology is called the map associated to the functorial pair (f, ϕ).*

Definition 2.4.2 (Restriction). *Let $\iota : H \hookrightarrow G$ be a subgroup, then for any $\mathbb{Z}[G]$-module A, we get a functorial pair (ι, id_A) and the associated map, called restriction, is denoted by Res^G_H.*

Definition 2.4.3 (Inflation)**.** *Let $H < G$ be a normal subgroup and $\pi : G \to G/H$ the canonical surjection. Further let A be a G-module and $\iota : A^H \hookrightarrow A$ the inclusion, then the map associated to the functorial pair (π, ι) is called inflation and denoted by Inf_H^G.*

Definition 2.4.4. *Let $H < G$ be a subgroup and A a $\mathbb{Z}[H]$-module. Like in representation theory we define the induced module $\mathrm{Ind}_H^G(A) = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)$ and we view $\mathrm{Ind}_H^G(A)$ as a $\mathbb{Z}[G]$-module by setting $(gf)(y) = f(yg)$, for $f \in \mathrm{Ind}_H^G(A)$, $y \in \mathbb{Z}[G]$ and $g \in G$.*

Induction is adjoint to restriction in the sense that there is a natural isomorphism $\mathrm{Hom}_H(A, B) \cong \mathrm{Hom}_G(A, \mathrm{Ind}_H^G(B))$ for any $\mathbb{Z}[G]$-module A and $\mathbb{Z}[H]$-module B. This extends to a similar isomorphism on cohomology as shown in the next lemma.

Lemma 2.4.5 (Shapiro)**.** *Let G be a group, $H < G$ a subgroup and A a H-module, then the map*

$$H^q(G, \mathrm{Ind}_H^G A) \to H^q(H, A)$$

induced by the canonical map $\psi : \mathrm{Ind}_H^G A \to A : \phi \mapsto \phi(1)$ and the inclusion $\iota : H \hookrightarrow G$ is an isomorphism for each $q \geq 0$.

Proof. (ι, ψ) is a functorial pair since $\psi(\iota(h)\phi) = \phi(h) = h\phi(1) = h\psi(\phi)$.

First we prove the lemma for $q = 0$. Let $f \in \mathrm{Ind}_H^G(A)^G$, then since f is G-invariant, it is constant and $f(1) = f(h) = hf(1)$ for all $h \in H$, so $\psi : \mathrm{Ind}_H^G(A)^G \to A^H$ is an isomorphism.

Now suppose the lemma is true for q, then we prove that it holds for $q + 1$. Embed A in an injective $\mathbb{Z}[H]$-module I and set $B = I/A$. Then $0 \to A \to I \to B \to 0$ is exact and since $\mathbb{Z}[G]$ is a projective $\mathbb{Z}[H]$-module (it is even free), the sequence $0 \to A' \to I' \to B' \to 0$ is also exact, where $M' = \mathrm{Ind}_H^G(M)$ for $M = A, I, B$. Moreover $\mathrm{Hom}_G(-, \mathrm{Ind}_H^G(I)) = \mathrm{Hom}_H(-, I)$ and so I' is an injective $\mathbb{Z}[G]$-module. In particular $H^{q+1}(G, I') = H^{q+1}(H, I) = 0$ and since the maps $H^q(G, M') \to H^q(H, M)$ are induced by chain maps it commutes with the connecting homomorphisms in the long exact sequences, i.e. we have a commutative diagram

$$\begin{tikzcd}
H^q(G, I') \arrow[r] \arrow[d, "\alpha"] & H^q(G, B') \arrow[r] \arrow[d, "\beta"] & H^{q+1}(G, A') \arrow[r] \arrow[d, "\gamma"] & 0 \\
H^q(H, I) \arrow[r] & H^q(H, B) \arrow[r] & H^{q+1}(H, A) \arrow[r] & 0
\end{tikzcd}$$

where α, β are isomorphisms by inductive hypothesis and so γ is an isomorphism, too. □

Sometimes it is also useful to know the cohomology of the additive group of a field L which is much simpler than the multiplicative group as we can easily deduce now.

Corollary 2.4.6 (Additive Hilbert 90)**.** *Let $K \subset L$ be a finite Galois extension with Galois group G, then $H^q(G, L^+) = 0$ for all $q \geq 1$, where L^+ denotes the additive group of L.*

Proof. Using the normal basis theorem one can show that there is a G-module isomorphism $L^+ \cong K[G] = \operatorname{Ind}_1^G K$. Now the theorem follows from Shapiro's lemma since if G is the trivial group, $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$ is a projective resolution of $\mathbb{Z}$ and so all cohomology groups vanish for $q \geq 1$. However, we could also use the weaker statement from [9], that $L^n \cong L \otimes_K L \cong \operatorname{Ind}_1^G L$, where the G acts on $L \otimes_K L$ on the right factor. Then we get $H^q(G, L)^n \cong H^q(G, \operatorname{Ind}_1^G L) = 0$. □

Remark 2.4.7. *The method of reducing to the case $q = 0$ in the proof of Shapiro's Lemma is called dimension shifting and we will encounter it many more times since higher cohomology groups often don't have nice interpretations.*

Definition 2.4.8 (Corestriction)**.** *Let $H < G$ be a finite index subgroup, A a $\mathbb{Z}[G]$-module and R a set of coset representatives of G/H, then the maps $\mathrm{id} : G \to G$ and $\operatorname{Ind}_H^G(A) \to A : f \mapsto \sum_{r \in R} rf(r^{-1})$ form a functorial pair which induces a map on cohomology $H^q(G, \operatorname{Ind}_H^G(A)) \to H^q(G, A)$. This map composed with the isomorphism from Shapiro's Lemma is denoted $\operatorname{Cor}_H^G : H^q(H, A) \to H^q(G, A)$.*

In the previous definition we have to check that $f \mapsto \sum_{r \in R} rf(r^{-1})$ is a $\mathbb{Z}[G]$-homomorphism, independent of R. The independence of R is straightforward since f is a $\mathbb{Z}[H]$-homomorphism. Let $g \in G$, then for every $r \in R$ there is a unique $h_r \in H$ and $s_r \in R$ such that $r^{-1}g = h_r s_r^{-1}$. Now gf gets mapped to

$$\sum_{r \in R} rf(r^{-1}g) = \sum_{r \in R} rf(h_r s_r^{-1}) = \sum_{r \in R} g s_r h_r^{-1} f(h_r s_r^{-1}) = g \sum_{r \in R} s_r f(s_r^{-1}).$$

Since $r \mapsto s_r$ is a bijection, this shows that $f \mapsto \sum_{r \in R} rf(r^{-1})$ is G-equivariant.

Lemma 2.4.9. *Let $H < G$ be a finite index subgroup, then $\operatorname{Cor}_H^G \circ \operatorname{Res}_H^G$ is multiplication by $[G : H]$.*

Proof. For $q = 0$, we have that $\operatorname{Res} : A^G \to A^H$ is the inclusion and $\operatorname{Cor} : A^H = \operatorname{Ind}_H^G(A)^G \to A^G : f \mapsto \sum_{r \in R} rf(r^{-1}) = [G : H]f(1)$ and the result follows.

Assume the result has been proven for $q \geq 0$ and embed A in an injective module I. Then we have a short exact sequence $0 \to A \to I \to A' \to 0$ for $A' = I/A$. Since I is injective, we have $H^{q+1}(G, I) = 0$. Let $\alpha : H^q(G, \operatorname{Ind}_H^G(A)) \to H^q(H, A)$ be the isomorphism from Shapiro's Lemma, then we can split up $\operatorname{Cor} \circ \operatorname{Res} = (\operatorname{Cor} \circ \alpha) \circ \alpha^{-1} \circ \operatorname{Res}$. Now observe that $\operatorname{Cor} \circ \alpha$, α and Res are all induced by functorial pairs and hence by chain maps. As a result there is a commutative diagram

$$\begin{tikzcd}
H^q(G, I) \arrow[r] \arrow[d, "{[G:H]}"] & H^q(G, A') \arrow[r] \arrow[d, "{[G:H]}"] & H^{q+1}(G, A) \arrow[r] \arrow[d, "\operatorname{Cor} \circ \operatorname{Res}"] & 0 \\
H^q(G, I) \arrow[r] & H^q(G, A') \arrow[r] & H^{q+1}(G, A) \arrow[r] & 0
\end{tikzcd}$$

and the claim follows by induction. □

Corollary 2.4.10. *If G is finite, then $|G|$ kills $H^q(G,A)$ for $q \geq 1$.*

Proof. Let $H = \{\mathrm{id}\}$, then $H^q(H,A) = 0$ for $q \geq 1$, since $0 \to \mathbb{Z} \to \mathbb{Z} \to 0$ is a $\mathbb{Z}[H]$-projective resolution of $\mathbb{Z}$. Hence $0 = \mathrm{Cor}_H^G \circ \mathrm{Res}_H^G = |G|$. □

Corollary 2.4.11. *Let $H < G$ be a finite index subgroup such that $p \nmid [G:H]$, then Res_H^G is injective on p-primary components and Cor_H^G is surjective on p-primary components.*

Proof. Multiplication by $[G:H] = \mathrm{Cor} \circ \mathrm{Res}$ is bijective on p-primary components since $p \nmid [G:H]$. Thus Res is injective on p-primary components and Cor is surjective on p-primary components. □

Corollary 2.4.12. *Let G be a finite group, A a $\mathbb{Z}[G]$ module and $q \geq 1$, such that for every prime p, there is a p-Sylow subgroup $H < G$ with $H^q(H,A) = 0$, then $H^q(G,A) = 0$.*

Proof. By 2.4.11, all p-primary components of $H^q(G,A)$ vanish and since $H^q(G,A)$ is torsion by 2.4.10, this proves the claim. □

Lemma 2.4.13. *Let $H < G$ be a normal subgroup and A a $\mathbb{Z}[G]$-module, then the following sequence is exact.*

$$0 \to H^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} H^1(G,A) \xrightarrow{\mathrm{Res}} H^1(H,A).$$

Proof. We prove this by using the explicit description of H^1 from Corollary 2.1.6. First we show injectivity of Inf. Note that Inf is induced by the map

$$C^\bullet(G/H, A^H) \to C^\bullet(G,A) : f \mapsto f \circ \pi,$$

where $\pi : G \to G/H$ is the canonical surjection. Now let $f \in C^1(G/H, A^H)$ and suppose $\mathrm{Inf}[f] = 0$, i.e. there is $a \in A$ such that $f(gH) = ga - a$ for all $g \in G$, then for all $h \in H$ we have $ha - a = f(hH) = f(H) = a - a = 0$ and so $a \in A^H$. Thus $f(gH) = gHa - a$ for all $gH \in G/H$ and f represents 0 in $H^1(G/H, A^H)$.

Let $f \in C^1(G/H, A^H)$, then $f(h) = f(e) = f(e \cdot e) = f(e) + f(e) = 0$ for all $h \in H$. Hence $\mathrm{Res}(\mathrm{Inf}([f])) = 0$ already on the level of cochains.

Now suppose $f \in C^1(G,A)$ is a cocycle such that $f(h) = ha - a$ for some $a \in A$ and all $h \in H$. Let $f'(g) = f(g) - (ga - a)$, then f' represents the same class as f in $H^1(G,A)$ and $f'(h) = 0$ for all $h \in H$. Hence the cocycle condition $f'(gh) = gf'(h) + f'(g)$ implies that f' is constant on cosets and $f'(hg) = hf'(g) + f'(h)$ implies that f' takes values in A^H. Hence $f'(g) = f''(gH)$ for some $f'' \in C^1(G/H, A^H)$. Moreover f'' is a cocycle since $f''(g_1Hg_2H) = f'(g_1g_2) = g_1f'(g_2) + f'(g_1) = g_1Hf''(g_2H) + f''(g_1H)$. Hence the class of f lies in the image of Inf which shows exactness at $H^1(G,A)$. □

Corollary 2.4.14 (Inflation-Restriction Sequence)**.** *Let $H < G$ be a normal subgroup, $q \geq 1$ and A a $\mathbb{Z}[G]$-module such that $H^m(H, A) = 0$ for all $0 < m < q$, then the following sequence is exact.*

$$0 \to H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A).$$

Proof. By the lemma, the statement is true for $q = 1$. Now suppose it is true for some $q \geq 1$, then we prove it for $q + 1$. Embed A in an injective $\mathbb{Z}[G]$-module I. Then we first show that I^H is an injective $\mathbb{Z}[G/H]$-module. Suppose $A \subset B$ are $\mathbb{Z}[G/H]$ modules and $f : A \to I^H$ is a $\mathbb{Z}[G/H]$-homomorphism, then via the canonical map $\mathbb{Z}[G] \to \mathbb{Z}[G/H]$, f is also a $\mathbb{Z}[G]$-homomorphism $A \to I$ and so it extends to $\tilde{f} : B \to I$. But since H acts trivially on B we have $h\tilde{f}(b) = \tilde{f}(b)$ for all $b \in B$ and hence $\tilde{f} : B \to I^H$ extends f.

Moreover, $\mathrm{Hom}_H(-, I) = \mathrm{Hom}_G(-, \mathrm{Hom}_H(\mathbb{Z}[G], I))$ and $\mathrm{Hom}_H(\mathbb{Z}[G], I)$ is injective since $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module. Hence I is injective as a $\mathbb{Z}[H]$-module.

Consider the short exact sequence $0 \to A \to I \to B \to 0$ with $B = I/A$. This sequence is also exact as a sequence of $\mathbb{Z}[H]$-modules and since $0 < 1 < q + 1$, we have $H^1(H, A) = 0$ and so we find that $0 \to A^H \to I^H \to B^H \to 0$ is still exact. As Inf and Res are induced by functorial pairs and hence by chain maps, they commute with the connecting homomorphisms and we have a commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^{q+1}(G/H, A^H) \arrow[r, "\text{Inf}"] & H^{q+1}(G, A) \arrow[r, "\text{Res}"] & H^{q+1}(H, A) \\
0 \arrow[r] & H^q(G/H, B^H) \arrow[r, "\text{Inf}"] \arrow[u, "\delta"] & H^q(G, B) \arrow[r, "\text{Res}"] \arrow[u, "\delta"] & H^q(H, B) \arrow[u, "\delta"]
\end{tikzcd}$$

and because I (also as $\mathbb{Z}[H]$-module) and I^H are injective, all the vertical maps are isomorphisms. It remains to show that the lower row is exact which follows by induction since for all $0 < m < q$ we have the exact sequence $0 = H^m(H, I) \to H^m(H, B) \to H^{m+1}(H, A) = 0$. □

As hinted in the beginning of this section, 2.4.12 and 2.4.14 together can sometimes be used to reduce a problem to the case of groups of prime order p. For example to prove global class field theory one has to show that $H^1(G, C_L) = 0$ for all finite Galois extensions $K \subset L$ with Galois group G, where C_L is the idèle class group. It suffices to check this for degree p extensions. And as we saw before, cyclic groups have a particularly simple cohomology theory, thus greatly simplifying the problem. Here are two explicit examples of applying this method.

Example 2.4.15. *Consider the natural action of the dihedral group D_n on $\mathbb{C}$, then $H^q(D_n, \mathbb{C}) = 0$ for all $q \geq 1$.*

Proof. Let $H < D_n$ be the subgroup of rotations, then $\mathbb{C}^H = 0$ since rotations have no fixed points except 0 and so $H^q(H, \mathbb{C}) = 0$ for q even. Moreover if q is odd, then

$H^q(H, \mathbb{C}) = \ker N/(z-1)\mathbb{C} = 0$, where z is a primitive nth root of unity. Hence by inflation-restriction $H^q(D_n, \mathbb{C}) \cong H^q(D_n/H, \mathbb{C}^H)$ for all $q \geq 1$. But $\mathbb{C}^H = 0$ and as a result $H^q(D_n, \mathbb{C}) = 0$ for all $q \geq 1$. □

Example 2.4.16. *Let G be a finite group acting trivially on $\mathbb{Q}$, then $H^q(G, \mathbb{Q}) = 0$ for all $q \geq 1$.*

Proof. By 2.4.12 it suffices to show this for p-groups. For a cyclic group it follows immediately from 2.3.3, since in this case the norm map is just multiplication by $|G|$. Now assume the claim holds for all p-groups of cardinality p^s and let G be a p-group of cardinality p^{s+1}. There exists a normal subgroup $H < G$ such that $G/H \cong \mathbb{Z}/p\mathbb{Z}$. By inflation-restriction and the inductive hypothesis we find $H^q(G, \mathbb{Q}) = 0$. □

The Inflation-Restriction Sequence connects the groups $H^q(G/H, A^H)$, $H^q(H, A)$ and $H^q(G, A)$ in a particular case. The general case is treated by the Hochschild-Serre Spectral sequence [11] which we state here but whose proof shall be omitted.

Theorem 2.4.17 (Hochschild-Serre)**.** *Let H be a normal subgroup of G, then there exists a spectral sequence E_r^{ij} starting at the E_2 page which converges to $H^n(G, A)$ and satisfies $E_2^{ij} = H^i(G/H, H^j(H, A))$.*

To make sense of $H^i(G/H, H^j(H, A))$ we need an action of G/H on $H^j(H, A)$. It is defined by letting $g \in G$ act by the functorial pair $(h \mapsto ghg^{-1}, a \mapsto g^{-1}a)$. For a down-to-earth introduction to spectral sequences see [24, Chapter 1.7].

2.5 The Cup Product

In this section we introduce a multiplicative structure

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

called the cup product. For example it appears in class field theory as the Hilbert symbol. We mainly follow the construction of the cup product presented in [9, Chapter 3]. Given $\mathbb{Z}[G]$-modules A and B we equip $A \otimes_{\mathbb{Z}} B$ with a $\mathbb{Z}[G \times G]$-module structure in the natural way. For complexes $A_\bullet$ and $B_\bullet$ we define a complex $(A \otimes_{\mathbb{Z}} B)_n = \bigoplus_{i+j=n} A_i \otimes_{\mathbb{Z}} B_j$ with differentials

$$d : \sum_{i+j=n} a_i \otimes b_j \mapsto \sum_{i+j=n} (da_i) \otimes b_j + (-1)^i a_i \otimes (db_j).$$

It is straightforward to check $d^2 = 0$.

Lemma 2.5.1. *Let P, Q be projective $\mathbb{Z}[G]$-modules, then $P \otimes_{\mathbb{Z}} Q$ is a projective $\mathbb{Z}[G \times G]$-module.*

Proof. Projective modules are direct summands of free modules, so let F_1, F_2 be free $\mathbb{Z}[G]$-modules such that $P \oplus P' = F_1$ and $Q \oplus Q' = F_2$. Then $(P \otimes Q) \oplus (P' \otimes Q) \oplus (P \otimes Q') \oplus (P' \otimes Q') = F_1 \otimes F_2$ and so it remains to show that $F_1 \otimes_{\mathbb{Z}} F_2$ is a free $\mathbb{Z}[G \times G]$-module. To see this we just have to check that $\mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G]$ is free. But this follows easily from the isomorphism $\mathbb{Z}[G \times G] \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G] : (x, y) \mapsto x \otimes y$. □

Lemma 2.5.2. *A bounded double complex with exact rows has trivial total homology.*

Proof. The E_1 page of the associated spectral sequence vanishes and so the total cohomology is trivial [24, Chapter 1.7]. But of course one could also prove this by diagram chasing. □

Corollary 2.5.3. *If $M_\bullet$ is a flat bounded complex and $N_\bullet$ is an exact bounded complex, then $(M \otimes N)_\bullet$ is exact.*

Proof. Each of the rows $M_i \otimes N_\bullet$ is exact by flatness. □

Lemma 2.5.4. *Let $P_\bullet \to \mathbb{Z} \to 0$, $Q_\bullet \to \mathbb{Z} \to 0$ be projective $\mathbb{Z}[G]$-resolutions, then $P_\bullet \otimes_{\mathbb{Z}} Q_\bullet$ is a projective $\mathbb{Z}[G \times G]$ resolution of $\mathbb{Z}$.*

Proof. By 2.5.1 $\bigoplus_i (P_{n-i} \otimes_{\mathbb{Z}} Q_i)$ is a direct sum of projective modules and hence projective. Projective $\mathbb{Z}[G]$-modules are projective $\mathbb{Z}$-modules since they are direct summands of a free $\mathbb{Z}[G]$-module and $\mathbb{Z}[G]$ is a free $\mathbb{Z}$-module. Projective modules are flat (since Tor_1 vanishes) and so $(P \otimes Q)_\bullet$ is exact by 2.5.3.

It remains to show that $(Q_0 \otimes P_0)/d(P \otimes Q)_1 \cong \mathbb{Z}$. Note that as $\mathbb{Z}$-modules, we have $Q_0 = d(Q_1) \oplus \mathbb{Z}$ and $P_0 = d(P_1) \oplus \mathbb{Z}$. This shows that $P_0 \otimes Q_0 = \mathbb{Z} \oplus d(P_1) \oplus d(Q_1) \oplus d(P_1) \otimes d(Q_1)$. On the other hand $d(P \otimes Q)_1 = d(P_1) \otimes Q_0 + P_0 \otimes d(Q_1) = d(P_1) + d(Q_1) + d(P_1) \otimes d(Q_1)$ and the result follows. □

Definition 2.5.5. *Let $P_\bullet$, $Q_\bullet$ be projective resolutions of $\mathbb{Z}$ and A, B $\mathbb{Z}[G]$-modules. Given $a \in \mathrm{Hom}(P_i, A)$ and $b \in \mathrm{Hom}(Q_j, B)$ we define the cup product as $(a \cup b) : P_i \otimes_{\mathbb{Z}} Q_j \to A \otimes_{\mathbb{Z}} B : p \otimes q \mapsto a(p) \otimes b(q)$.*

Clearly the cup product is functorial in both arguments. More precisely if $f : A \to A'$ and $g : B \to B'$ are G-homomorphisms, then $f_*(a) \cup g_*(b) = (f \otimes g)_*(a \cup b)$.

Lemma 2.5.6. *For $a \in \mathrm{Hom}(P_i, A)$ and $b \in \mathrm{Hom}(Q_j, B)$ we have the formula*

$$d(a \cup b) = da \cup b + (-1)^i (a \cup db).$$

Proof. Unravelling the definitions we find

$$d(a \cup b) : p_{i+1} \otimes q_j + p_i \otimes q_{j+1} \mapsto a(dp_{i+1}) \otimes b(q_j) + (-1)^i a(p_i) \otimes b(dq_{j+1})$$

and hence the claim. □

Lemma 2.5.7. *The cup product induces a well-defined bilinear map* $H^i(G, A) \times H^j(G, B) \to H^{i+j}(G, A \otimes_{\mathbb{Z}} B)$.

Proof. If $da = 0$ and $db = 0$, then by 2.5.6 $d(a \cup b) = 0$. Moreover if $a = a' + da''$ and $b = b' + db''$, then $a \cup b = a' \cup b' + d(a'' \cup b') + (-1)^i d(a' \cup b'') + d(a'' \cup db'')$ and so the cup product is a well-defined on cohomology classes $H^i(G, A) \times H^j(G, B) \to H^{i+j}(G \times G, A \otimes_{\mathbb{Z}} B)$. Composing this with the restriction associated to the diagonal embedding $G \to G \times G$, we get the desired map.

Moreover, the construction is independent of the projective resolutions because if $P_\bullet, P'_\bullet, Q_\bullet$ and $Q'_\bullet$ are projective resolutions of $\mathbb{Z}$, then $P_\bullet$ is homotopy equivalent to $P'_\bullet$ and $Q_\bullet$ is homotopy equivalent to $Q'_\bullet$. These homotopy equivalences can naturally be tensored together to a homotopy equivalence between $(P \otimes Q)_\bullet$ and $(P' \otimes Q')_\bullet$. The isomorphisms on cohomology induced by these equivalences are compatible with the cup product construction. □

In degree 0 we recover the natural injective map $A^G \otimes B^G \to (A \otimes B)^G$. Moreover, one can check that the cup product is associative and we have

Lemma 2.5.8. *Using the canonical isomorphism* $A \otimes B \to B \otimes A$ *we may identify* $H^i(G, A \otimes B)$ *and* $H^i(G, B \otimes A)$. *Under this identification we have* $\alpha \cup \beta = (-1)^{ij} \beta \cup \alpha$, *where* $\alpha \in H^i(G, A)$ *and* $\beta \in H^j(G, B)$.

Proof. We show something stronger. Let $P_\bullet$ be a projective resolution of $\mathbb{Z}$, then there is an isomorphism of chain complexes $\phi : P_\bullet \otimes P_\bullet \to P_\bullet \otimes P_\bullet$ mapping $p \otimes q \in P_i \otimes P_j$ to $(-1)^{ij} q \otimes p \in P_j \otimes P_i$. This is verified by the computation

$$\begin{aligned} d(\phi(p \otimes q)) &= d((-1)^{ij} q \otimes p) = (-1)^{ij}(dq \otimes p + (-1)^j q \otimes dp) \\ &= (-1)^{(i+1)j} q \otimes dp + (-1)^{i(j+1)+i} dq \otimes p = \phi(d(p \otimes q)). \end{aligned}$$ □

Lemma 2.5.9. *Suppose* $0 \to A_1 \to A_2 \to A_3 \to 0$ *is exact and* $0 \to A_1 \otimes B \to A_2 \otimes B \to A_3 \otimes B \to 0$ *remains exact, then* $\delta(a \cup b) = \delta(a) \cup b$ *for all* $a \in H^i(G, A_3)$ *and* $b \in H^j(G, B)$, *where* δ *is the connecting homomorphism. Similarly* $\delta(a \cup b) = (-1)^i a \cup \delta(b)$ *for* $a \in H^i(G, A)$ *and* $b \in H^j(G, B_3)$, *when* $0 \to B_1 \to B_2 \to B_3 \to 0$ *is a short exact sequence such that* $0 \to A \otimes B_1 \to A \otimes B_2 \to A \otimes B_3 \to 0$ *remains exact.*

Proof Sketch. This essentially boils down to the fact that everything in the diagram

$$0 \to \mathrm{Hom}(P_\bullet \otimes Q_\bullet, A_1 \otimes B) \to \mathrm{Hom}(P_\bullet \otimes Q_\bullet, A_2 \otimes B) \to \mathrm{Hom}(P_\bullet \otimes Q_\bullet, A_3 \otimes B) \to 0$$

commutes. See [9, Proposition 3.4.8] for the details. □

Often we have a $\mathbb{Z}$-bilinear map $b : A \times B \to C$ such that $b(gx, gy) = gb(x, y)$ and after composing with the induced map $A \otimes B \to C$ we get a cup product with values in $H^{i+j}(G, C)$.

Lemma 2.5.10. *Let $0 \to A_1 \to A_2 \to A_3 \to 0$ and $0 \to B_1 \to B_2 \to B_3 \to 0$ be exact sequences of $\mathbb{Z}[G]$-modules equipped with a bilinear map $b : A_2 \times B_2 \to C$ for some $\mathbb{Z}[G]$-module C and assume further that b is trivial on $A_1 \times B_1$ and compatible with the diagonal action of G on $A_2 \otimes B_2$, then there are well-defined induced bilinear maps $A_1 \times B_3 \to C$ and $A_3 \times B_1 \to C$ and if we consider the corresponding cup products we have $\delta(\alpha) \cup \beta = (-1)^{i+1} \alpha \cup \delta(\beta)$ where $\alpha \in H^i(G, A_3)$ and $\beta \in H^j(G, B_3)$.*

Proof. Let $P_\bullet \to \mathbb{Z}$ be a projective resolution. Lift α to $\alpha' \in \operatorname{Hom}(P_i, A_2)$ and β to $\beta' \in \operatorname{Hom}(P_j, B_2)$, then $\delta(\alpha) \cup \beta$ is represented by $b(d\alpha', \beta')$ and $\alpha \cup \delta(\beta)$ is represented by $b(\alpha', d\beta')$. But by definition of the total differentials we find $d(b(\alpha', \beta')) = b(d\alpha', \beta') + (-1)^i b(\alpha', d\beta')$ from which the desired equality follows. □

Lemma 2.5.11. *Let $H < G$ be a subgroup and assume further that H is normal or finite index when necessary. Then the formulas*

$$\operatorname{Res}(\alpha \cup \beta) = \operatorname{Res}(\alpha) \cup \operatorname{Res}(\beta)$$
$$\operatorname{Inf}(\alpha \cup \beta) = \operatorname{Inf}(\alpha) \cup \operatorname{Inf}(\beta)$$
$$\operatorname{Cor}(\alpha \cup \operatorname{Res}(\beta)) = \operatorname{Cor}(\alpha) \cup \beta$$

hold for all cohomology classes α, β.

Proof. All of these hold in degree 0. Now one can use 2.5.9 and dimension shifting to deduce them in any degree. For example we will do this for $\operatorname{Cor}(\alpha \cup \operatorname{Res}(\beta)) = \operatorname{Cor}(\alpha) \cup \beta$. So let $H < G$ be a finite index subgroup $\alpha \in H^i(H, A)$ and $\beta \in H^j(G, B)$, where A and B are $\mathbb{Z}[G]$ modules and suppose the formula has been proven for $i' + j' < i + j$.

If $i > 0$, consider the short exact sequence $0 \to A \to \operatorname{Ind}_1^G(A) \to A' \to 0$ where $a \in A$ maps to the function $g \mapsto ga$ in $\operatorname{Ind}_1^G(A)$. We can write this as $0 \to A \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} A \to A' \to 0$ and so $0 \to A \otimes B \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} (A \otimes B) \to A' \otimes B \to 0$ remains exact. The $\mathbb{Z}[H]$-module $\mathbb{Z}[G] \otimes_{\mathbb{Z}} A \cong \operatorname{Ind}_1^G A$ has trivial cohomology since as an $\mathbb{Z}[H]$ module $\operatorname{Ind}_1^G = \bigoplus \operatorname{Ind}_1^H$ decomposes into a direct sum over cosets and then we can apply Shapiro's lemma 2.4.5. Hence there is α' such that $\alpha = \delta\alpha'$ and since both Cor and Res are functorial, 2.5.9 implies

$$\operatorname{Cor}(\alpha) \cup \beta = \delta(\operatorname{Cor}(\alpha') \cup \beta) = \delta(\operatorname{Cor}(\alpha' \cup \operatorname{Res}(\beta))) = \operatorname{Cor}(\alpha \cup \operatorname{Res}(\beta)).$$

If $j > 0$, consider the analogous exact sequence $0 \to B \to B \otimes \mathbb{Z}[G] \to B' \to 0$ which stays exact after tensoring with A and conclude similarly with $\beta = \delta\beta'$. The other formulas can be proven by the same method. Alternatively see [9, Prop 3.4.10]. □

Lemma 2.5.12. *Let G be a finite cyclic group, A a $\mathbb{Z}[G]$-module and $\chi : G \to \mathbb{Q}/\mathbb{Z}$ an injective homomorphism, then $H^q(G, A) \to H^{q+2}(G, A) : a \mapsto a \cup \delta\chi$ is an* *isomorphism for $q \geq 1$, where δ is the coboundary map in the long exact sequence coming from the short exact sequence of trivial G-modules* $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. *Similarly $A^G/N(A) \to H^2(G, A) : a \mapsto a \cup \delta\chi$ is an isomorphism.*

Proof. See [9, Prop 3.4.11]. □

2.6 Profinite Group Cohomology

Often it will be convenient to consider infinite Galois extensions. This does not really cause us much trouble, since the Galois group of any algebraic extension is profinite and we will show that most results about finite group cohomology extend to profinite group cohomology by "passing to the limit". References for the cohomology of profinite groups are [19, Chapter 1] and [21].

Definition 2.6.1 (Profinite group)**.** *A profinite group is a group G which is isomorphic to the projective limit of an inverse system of discrete finite groups G_i. We always equip profinite groups with the limit topology.*

More explicitly given an index set I and a set $J \subset I \times I$ such that for each $\alpha \in I$ we have a finite group G_α with the discrete topology and for each $(\alpha, \beta) \in J$ a homomorphism $f_{\alpha\beta} : G_\beta \to G_\alpha$ such that $f_{\alpha\beta} \circ f_{\beta\gamma} = f_{\alpha\gamma}$, we define

$$\lim_{\leftarrow} G_\alpha := \left\{ (g_\alpha) \in \prod_{\alpha \in I} G_\alpha : f_{\alpha\beta}(g_\beta) = g_\alpha \right\}$$

which is a closed subspace of the product $\prod_{\alpha \in I} G_\alpha$ since the $f_{\alpha\beta}$ are continuous. Any group of this form will be called profinite. In particular a profinite group is compact by Tychonoff's theorem [3, I. §9 Thm 3]. For an introduction to limits in categories, see [24, Chapter 1.4].

Example 2.6.2. *The additive group of p-adic integers $\mathbb{Z}_p$ is profinite.*

Proof. Indeed its closed subgroups are of the form $p^n\mathbb{Z}_p$ and it is straightforward to check that the map $\mathbb{Z}_p \to \lim_{\leftarrow} \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$ is an isomorphism, where the limit is with respect to the canonical maps $\mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$. Moreover this gives $\mathbb{Z}_p$ its standard topology. □

Given any group G we can construct a profinite group $\hat{G}$, called the profinite completion of G by setting $\hat{G} := \lim_{\leftarrow} G/N$, where $N < G$ runs through the normal finite index subgroups of G. For example $\hat{\mathbb{Z}}$ is the inverse limit of all cyclic groups and by the chinese remainder theorem $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$. The next lemma provides us with the most relevant examples of profinite groups for this thesis.

Lemma 2.6.3. *Let $K \subset L$ be a Galois extension (of any degree), then the Galois group $G = \mathrm{Gal}(L/K)$ is profinite.*

Proof. Let $K \subset F$ be a finite Galois extension contained in L. Then we have a canonical surjective map $G \to \mathrm{Gal}(F/K)$ with kernel $\mathrm{Gal}(L/F)$. Moreover whenever $F \subset F'$ are two such extensions we have a surjective map $res_{F,F'} : \mathrm{Gal}(F'/K) \to \mathrm{Gal}(F/K)$. Now consider the induced map

$$\phi : G \to \lim_{\leftarrow} \mathrm{Gal}(F/K),$$

where the limit ranges over all intermediate fields $K \subset F \subset L$, such that $K \subset F$ is a finite Galois extension. By definition

$$\lim_{\leftarrow} \mathrm{Gal}(F/K) = \left\{ (a_F) \in \prod_F \mathrm{Gal}(F/K) : \text{ for all } F \subset F' : res_{F',F}(a_{F'}) = a_F \right\}.$$

We wish to show that ϕ is an isomorphism. Let $\sigma \in G$ and suppose $\phi(\sigma) = e$. Let $x \in L$ and $K \subset F \subset L$ a finite Galois extension containing x. By assumption σ is the identity on F and so $\sigma(x) = x$. As x was arbitrary we conclude $\sigma = \mathrm{id}$. Hence ϕ is injective.

To see that ϕ is surjective let (τ_F) be an element of $\lim_{\leftarrow} \mathrm{Gal}(F/K)$ and define an automorphism τ of L by setting $\tau(x) = \tau_F(x)$, where F/K is some finite Galois extension containing x. This is well defined since any two finite Galois extensions $F, F'/K$ are contained in the finite Galois extension FF'/K and by the compatibility conditions in the definition of projective limit we find that $\tau_F(x) = \tau_{FF'}(x) = \tau_{F'}(x)$. Now if $x, y \in L$ we take a finite Galois extension F/K containing both x and y to show $\tau(x + y) = \tau(x) + \tau(y)$ and $\tau(xy) = \tau(x)\tau(y)$ so that τ is indeed an automorphism. □

Example 2.6.4. *Using the classification of finite fields one finds the isomorphism* $\hat{\mathbb{Z}} \to \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ *which maps* 1 *to the Frobenius automorphism* $x \mapsto x^q$.

Lemma 2.6.5. *Let* G *be a profinite group, then every open neighbourhood of the identity contains an open subgroup.*

Proof. Let $G = \left\{ (g_\alpha) \in \prod_{\alpha \in I} G_\alpha : f_{\alpha\beta}(g_\beta) = g_\alpha \right\}$ for some finite groups G_α and homomorphisms $f_{\alpha\beta} : G_\beta \to G_\alpha$ such that $f_{\alpha\beta} f_{\beta\gamma} = f_{\alpha\gamma}$. If $U \subset G$ is an open neighbourhood of the identity, then since the topology on G is induced by the product topology, U contains an open set of the form $V = \pi_1^{-1}(e) \cap \cdots \cap \pi_k^{-1}(e)$, where $\pi_i : G \to G_{\alpha_i}$ are the projections to some α_i. V is an open subgroup contained in U. □

Proposition 2.6.6. *A Hausdorff topological group is profinite if and only if it is compact and every open neighbourhood of the identity contains an open subgroup.*

Proof. We have seen that any profinite group has these properties, so let G be a compact Hausdorff topological group such that every open neighbourhood of the identity contains an open subgroup. Consider the canonical continuous map $\phi : G \to \lim_{\leftarrow} G/U$, where U ranges over the open normal subgroups of G with respect to the canonical maps $G/U \to G/V$ whenever $U \subset V$. Note that the G/U are finite since G is compact, so if we show that ϕ is an isomorphism of topological groups, then we will have shown that G is profinite.

Suppose $x \in \ker(\phi)$ such that $x \neq e$. Since G is Hausdorff and every open neighbourhood of the identity contains an open subgroup we can find an open subgroup $V < G$ such that $x \notin V$. Then $U = \bigcap_{g \in G} gVg^{-1}$ is a normal subgroup such that $x \notin U$. gVg^{-1} only depends on the class of g modulo V and so U is a finite intersection of open sets and hence open. Thus x is not in the kernel of the restriction $G \to G/U$. Absurd.

The image of ϕ is dense because if $W \subset \lim_{\leftarrow} G/U$ is open and non-empty, then W contains a non-empty set of the form $W' = \pi_{U_1}^{-1}(a_1) \cap \cdots \cap \pi_{U_n}^{-1}(a_n)$ where π_{U_i} is the projection map to G/U_i and $a_i \in G/U_i$. Let $b \in W'$ and $x \in G$ a representative of b modulo $U_1 \cap \cdots \cap U_n$, then $\pi_{U_i}(\phi(x)) = a_i$ for all i and so $\phi(x) \in W'$. Moreover, G is compact and $\lim_{\leftarrow} G/U$ is Hausdorff since it is a subspace of a product of Hausdorff spaces, so ϕ is a closed map. Hence $\phi(G)$ is closed and dense and so ϕ is surjective. Consequently ϕ is an isomorphism of topological groups. □

Corollary 2.6.7. *A closed subgroup of a profinite group is profinite.*

Definition 2.6.8. *Let G be a profinite group and A a $\mathbb{Z}[G]$-module, then we define $A^\delta := \bigcup_{U<G} A^U$, where the union is over all open subgroups of G. A is called a discrete G-module if $A^\delta = A$.*

A $\mathbb{Z}[G]$-module A is discrete if and only if $G \times A \to A : (g, a) \to ga$ is continuous, where A has the discrete topology.

Lemma 2.6.9. *The assignment $A \mapsto A^\delta$ is a functor from the category of $\mathbb{Z}[G]$-modules to the category of discrete G-modules. It is adjoint to the forgetful functor.*

Proof. Note that for any G-module A, A^δ is a submodule since the stabiliser of $x+y$ contains $\mathrm{Stab}(x) \cap \mathrm{Stab}(y)$. Let $f : A \to B$ be a morphism of $\mathbb{Z}[G]$-modules. Let $\overline{f}$ be the restriction of f to A^δ. If $b = f(a)$, wih $a \in A^\delta$, then there is an open subgroup $H < G$ such that H fixes a. Since f is a homomorphism H fixes b, too. Consequently the image of $\overline{f}$ is contained in B^δ.

For the second statement we have to show that for all $\mathbb{Z}[G]$-modules B and discrete G-modules A, there is a natural isomorphism $\mathrm{Hom}(A, B) \cong \mathrm{Hom}(A, B^\delta)$. But by the same argument as before, the image of any homomorphism $A \to B$ lies in B^δ, since A is discrete. □

Corollary 2.6.10. *The category of discrete G-modules has enough injectives.*

Proof. The category of $\mathbb{Z}[G]$-modules has enough injectives. Let A be a discrete G-module, then there is an injective $\mathbb{Z}[G]$-module I and a monomorphism $\iota : A \to I$.

Since A is discrete the image of ι is contained in I^δ. It remains to show that I^δ is injective. This is true because for all discrete G-modules A, we have $\operatorname{Hom}(A, I^\delta) = \operatorname{Hom}(A, I)$, hence the functor $A \mapsto \operatorname{Hom}(A, I)$ is exact. □

As a result we may construct the cohomology of a discrete G-module A using an injective resolution $I^\bullet$ of A and taking the cohomology of the complex

$$A^G \to (I^0)^G \to (I^1)^G \to \dots$$

i.e. we define $H^q(G, A)$ as the qth right derived functor of $A \mapsto A^G$ in the category of discrete G-modules. To actually compute these cohomology groups it is very useful to introduce the complex of continuous cochains. Let A be a discrete G-module, then we let $C^q(G, A)$ denote the abelian group of continuous functions $G^q \to A$. The groups $C^q(G, A)$ form a complex with differentials

$$\begin{aligned}(df)(g_1, \dots, g_q) &= g_1 f(g_2, \dots, g_q) \\ &\quad + \sum_{i=1}^{q-1} (-1)^i f(g_1, \dots, g_i g_{i+1}, \dots, g_q) + (-1)^q f(g_1, \dots, g_{q-1}).\end{aligned}$$

We have $d^2 = 0$ since even on non continuous cochains $d^2 = 0$ by the same reasoning as in 2.1.5. Denote by $\tilde{H}^k(G, A)$ the kth cohomology of the complex $C^\bullet(G, A)$.

Lemma 2.6.11. *Given a short exact sequence* $0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$ *of discrete G-modules, the induced sequence* $0 \to C^k(G, A) \to C^k(G, B) \to C^k(G, C) \to 0$ *is exact. Moreover, these exact sequences form a short exact sequence of chain complexes.*

Proof. $C^k(G, A) \to C^k(G, B)$ is injective since ι is injective. If $f \in C^k(G, B)$ maps to 0 in $C^k(G, C)$, then the image of f is contained in $\iota(A)$ which is homeomorphic to A since A and B have the discrete topology. Hence $f = \iota \circ f'$ for some $f' \in C^k(G, A)$. If $f \in C^k(G, C)$ fix a set $B' \subset B$ such that $\pi|_{B'}$ is bijective, then $\pi|_{B'}$ is a homeomorphism because B and C have the discrete topology and $f' = \pi|_{B'}^{-1} \circ f \in C^k(G, B)$ satisfies $\pi \circ f' = f$.

That these maps are maps of chain complexes, i.e. commute with the differentials can be checked without difficulty by applying π and ι to the definition of the differentials. □

Similarly to the abstract case we define induced modules for discrete modules.

Definition 2.6.12. *Let G be a profinite group, $H < G$ a closed subgroup and A a discrete H-module. Then we define $\operatorname{Ind}_H^G(A)$ as the set of continuous functions $f : G \to A$ such that $f(hg) = hf(g)$. We view $\operatorname{Ind}_H^G(A)$ as a $\mathbb{Z}[G]$-module by letting G act by right translation.*

Lemma 2.6.13. *If A is discrete, then* $\operatorname{Ind}_H^G(A)$ *is discrete.*

Proof. Let $f \in \operatorname{Ind}_H^G(A)$, then f is locally constant since A is discrete. By compactness of G, f takes finitely many values on disjoint closed and open sets $U_1, \ldots, U_n$. By 2.6.5, a basis of open sets is given by all left cosets of open subgroups of G. Since G is compact, each U_i is compact and hence a finite union of cosets of open subgroups of G. By intersecting these groups we find that U_i is a union of some cosets of a single open subgroup $V_i \subset G$. In particular $U_iV_i \subset U_i$ and so $V = \bigcap_{i=1}^n V_i$ is an open subgroup of G such that $U_iV \subset U_i$ for all i, i.e. f is fixed by V. □

Lemma 2.6.14. *Let $H < G$ be a closed subgroup of a profinite group G, A a discrete G-module and B a discrete H-module, then* $\operatorname{Hom}_H(A, B) = \operatorname{Hom}_G(A, \operatorname{Ind}_H^G(B))$.

Proof. Like in the abstract case, the isomorphism is induced by the map $\operatorname{Ind}_H^G(B) \to B : f \mapsto f(1)$. But since A is discrete it is straightforward to check that if an open $U < G$ fixes a, then then $\psi(a)(gU) = \psi(gUa)(1) = \psi(ga)(1) = \psi(a)(g)$ for any $\psi : A \to \operatorname{Ind}_H^G(B)$ and so $\psi(a)$ is constant on cosets of U and in particular continuous. So $\operatorname{Hom}_G(A, \operatorname{Hom}_H(\mathbb{Z}[G], B)) = \operatorname{Hom}_G(A, \operatorname{Ind}_H^G(B))$ and the claim follows from standard tensor-hom adjunction. □

Proposition 2.6.15. *Let G be a profinite group and A a discrete G-module, then*

$$\tilde{H}^q(G, A) = \lim_{\rightarrow} H^q(G/U, A^U),$$

where U ranges over the open normal subgroups of G.

Proof. Consider the canonical map $\psi : \lim_{\rightarrow} H^q(G/U, A^U) \to \tilde{H}^q(G, A)$ induced by the maps $H^q(G/U, A^U) \to \tilde{H}^q(G, A) : [f] \mapsto [f \circ \pi]$, where $\pi : G \to G/U$ is the quotient map. By an argument similar to the proof of 2.6.13 every cocycle $f \in C^q(G, A)$ factors through G/U for some open subgroup U and so ψ is surjective.

It remains to show that ψ is injective. Suppose that $f_U \in \ker \psi$, then there exists $f'_U \in C^{q-1}(G, A)$ such that $f_U = df'_U$. By shrinking U we can assume that $f'_U \in C^{q-1}(G/U, A^U)$ so that f_U represents 0 in $H^q(G/U, A^H)$. Consequently $\ker \psi = 0$, as desired. □

Proposition 2.6.16. *For all discrete G-modules M we have isomorphisms $\phi_k(M) : \tilde{H}^k(G, M) \to H^k(G, M)$ for all $k \geq 0$ such that for all short exact sequences $0 \to A \to B \to C \to 0$ of discrete G-modules, the diagram*

$$\begin{tikzcd}
\tilde{H}^k(G,A) \arrow[r] \arrow[d, "\phi_k(A)"] & \tilde{H}^k(G,B) \arrow[r] \arrow[d, "\phi_k(B)"] & \tilde{H}^k(G,C) \arrow[r] \arrow[d, "\phi_k(C)"] & \tilde{H}^{k+1}(G,A) \arrow[d, "\phi_{k+1}(A)"] \\
H^k(G,A) \arrow[r] & H^k(G,B) \arrow[r] & H^k(G,C) \arrow[r] & H^{k+1}(G,A)
\end{tikzcd}$$

commutes. Here the bottom row is the long exact sequence associated to the right derived functor which can be obtained by choosing suitable injective resolutions using the horseshoe lemma. The top row is the long exact sequence associated to the short exact sequence of chain complexes from 2.6.11.

Proof. We will show that the functors $H^i(G, -)$ and $\tilde{H}^i(G, -)$ are effaceable for $i > 0$ and conclude that they are universal ∂-functors and hence isomorphic (see [10, Proposition 2.2.1]). However, we will not use this terminology here and write out everything.

We have $\tilde{H}^0(G, A) = H^0(G, A) = A^G$ and so we may set $\phi_0(A) = \mathrm{id}$. Suppose the ϕ_k are defined for some $k \geq 0$, then we will define ϕ_{k+1}. Let A be a discrete G-module and let $B = I(A) = \mathrm{Ind}_1^G(A)$. We show that $\tilde{H}^i(G, B) = 0$ for $i \geq 1$. By 2.6.15 it suffices to show $H^i(G/U, B^U) = 0$ for all normal open subgroups $U < G$. But $B^U = \mathrm{Ind}_1^{G/U}(A)$ and so this follows directly from 2.4.5.

A embeds into B via $\iota : A \to B : a \mapsto (g \mapsto ga)$. Clearly quotients of discrete G-modules are again discrete G-modules and so we have a short exact sequence of discrete G-modules $0 \to A \xrightarrow{\iota} B \to B/\iota(A) \to 0$ which induces the following commutative diagram

$$\begin{tikzcd}
\tilde{H}^k(G, B) \arrow[r] \arrow[d, "\phi_k(B)"] & \tilde{H}^k(G, B/\iota(A)) \arrow[r] \arrow[d, "\phi_k(B/\iota(A))"] & \tilde{H}^{k+1}(G, A) \arrow[r] & 0 \\
H^k(G, B) \arrow[r] & H^k(G, B/\iota(A)) \arrow[r] & H^{k+1}(G, A) \arrow[r] & H^{k+1}(G, B)
\end{tikzcd}$$

with exact rows. Hence this diagram already defines $\phi_{k+1}(A)$ as the injective map induced by $\phi_k(B/\iota(A))$. Moreover, if $0 \to A' \to A \to A'' \to 0$ is a short exact sequence of discrete G-modules, then we also obtain a short exact sequence $0 \to I(A') \to I(A) \to I(A'') \to 0$ by 2.6.11 since $I(A) = C^1(G, A)$. This induces the commutative diagram

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & A' \arrow[r] \arrow[d] & A \arrow[r] \arrow[d] & A'' \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I(A') \arrow[r] \arrow[d] & I(A) \arrow[r] \arrow[d] & I(A'') \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C' \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & C'' \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

with exact columns and rows by the 9-lemma which gives rise to a commutative diagram of chain complexes $C^\bullet(G,-)$. Since the connecting homomorphisms are functorial, this shows that the ϕ_{k+1} commute with the connecting homomorphisms as required.

It remains to show that ϕ_{k+1} is surjective. For this let $0 \to A \to I \to A' \to 0$ be a short exact sequence of discrete G-modules, where I is injective. Then the diagram

$$\begin{tikzcd}
\tilde{H}^k(G,A') \arrow[r] \arrow[d, "\phi_k(A')"] & \tilde{H}^{k+1}(G,A) \arrow[r] \arrow[d, "\phi_{k+1}(A)"] & \tilde{H}^{k+1}(G,I) \arrow[d] \\
H^k(G,A') \arrow[r] & H^{k+1}(G,A) \arrow[r] & 0
\end{tikzcd}$$

shows that $\phi_{k+1}(A)$ is surjective, as required. □

Now that we can compute profinite group cohomology using continuous cochains many things follow.

Corollary 2.6.17. *There are natural inflation, restriction and corestriction maps just as in the abstract case and 2.4.14 and 2.4.11 continue to hold.*

Corollary 2.6.18. *If $G = \lim_{\leftarrow} G_i$ and $A = \lim_{\rightarrow} A_j$, then there is a natural isomorphism $H^q(G,A) \to \lim_{\rightarrow} H^q(G_i, A_j)$.*

Proof. This is true on the level of continuous cochains and similar to 2.6.15. □

Corollary 2.6.19. *Using this limit we can define the cup product for profinite cohomology via the cup products on $H^i(G/U, A^U) \times H^j(G/U, B^U)$ where $U < G$ is an open normal subgroup.*

2.7 Galois Cohomology

Let L/K be a Galois extension, then $G = \text{Gal}(L/K)$ is a profinite group. If A is a discrete G-module, we write $H^i(L/K, A)$ for $H^i(G,A)$. If L is a separable closure of K, then we write $H^i(K,A)$ for $H^i(L/K,A)$. To see that this is well-defined, let L_1, L_2 be two separable closures of K. Let $\alpha : L_1 \to L_2$ be a K-isomorphism, then $\Phi : \text{Gal}(L_1/K) \to \text{Gal}(L_2/K) : \sigma \mapsto \alpha \circ \sigma \circ \alpha^{-1}$ is an isomorphism of profinite groups and we can see a discrete $\text{Gal}(L_2/K)$-module as a discrete $\text{Gal}(L_1/K)$ module via this isomorphism. If A is a discrete $\text{Gal}(L_2/K)$-module then we would hope that $H^i(L_1/K, A)$ and $H^i(L_2/K, A)$ are related in a simple way and indeed we have

Lemma 2.7.1. *The functorial pair (Φ, id) induces an isomorphism $H^i(L_1/k, A) \to H^i(L_2/k, A)$ which is independent of α.*

Proof. It is clear that (Φ^{-1}, id) induces an inverse of (Φ, id), so we get an isomorphism $H^i(L_1/k, A) \to H^i(L_2/k, A)$. Now suppose $\alpha' : L_1 \to L_2$ is another k-isomorphism. Then $\alpha' = \tau \circ \alpha$ for some $\tau \in \text{Gal}(L_2/K, A)$ and so to show independence of α it suffices to show that conjugation by an element $\tau \in \text{Gal}(L_2/K) =: G$

induces the identity map on cohomology. This is obvious in $H^0(G, A) = A^G$ and the general case follows from a straightforward dimension shifting argument. □

Moreover, if $L \subset L'$, then $\mathrm{Gal}(L'/L) \subset \mathrm{Gal}(L'/K)$ is a closed subgroup and $\mathrm{Gal}(L/K) = \mathrm{Gal}(L'/K)/\mathrm{Gal}(L'/L)$ so we have natural maps $\mathrm{Res}_K^L : H^i(L'/K, A) \to H^i(L'/L, A)$ and $\mathrm{Inf}_L^{L'} : H^i(L/K, A) \to H^i(L'/K, A)$.

Now fix a field k and a separable closure k^s, then we set $G_k := \mathrm{Gal}(k^s/k)$. The first examples of Galois modules are the additive and multiplicative groups of k^s. Note that they are discrete G_k-modules since any element of k^s is contained in a finite Galois extension of k. Using 2.6.15 we find that $H^1(k, (k^s)^\times) = 0$ by Hilbert's Theorem 90 and $H^q(k, k^s) = 0$ for $q \geq 1$ by 2.4.6.

Proposition 2.7.2 (Kummer Theory). *Let k be a field, where ℓ is invertible in k, then $H^1(k, \mu_\ell) \cong k^\times/(k^\times)^\ell$.*

Proof. Since ℓ is invertible in k, every element of k^s is an ℓth power and from $H^1(k, (k^s)^\times) = 0$ and the short exact sequence $1 \to \mu_\ell \to (k^s)^\times \xrightarrow{\ell} (k^s)^\times \to 1$ we obtain the exact sequence $k^\times \xrightarrow{\ell} k^\times \to H^1(k, \mu_\ell) \to 0$, hence the desired isomorphism. □

Corollary 2.7.3. *Let k be a field containing the ℓth roots of unity μ_ℓ, where ℓ is invertible in k and L/k a cyclic Galois extension of degree ℓ, then there exists a generator $\alpha \in L$ such that $\alpha^\ell \in k$.*

Proof. Let $\chi : G_k \to \mu_\ell$ be surjective with kernel G_L, then $\chi \in H^1(k, \mu_\ell)$ since G_k acts trivially on μ_ℓ. By the definition of the coboundary map there exists $a \in k^\times$ such that $\chi(\sigma) = \sigma(\alpha)/\alpha$ for any $\alpha \in k^s$ such that $\alpha^\ell = a$. As $\ker \chi = G_L$ we conclude $\alpha \in L$, moreover α is not fixed by any non-trivial element of $\mathrm{Gal}(L/k)$ since χ is surjective, so α must be a generator. □

Proposition 2.7.4 (Artin-Schreier Theory). *Let k be a field of characteristic p, then $H^1(k, \mathbb{F}_p) \cong k/\wp(k)$, where $\wp(x) = x^p - x$.*

Proof. Since $x^p - x - a$ is separable for all $a \in k^s$ we have a short exact sequence $0 \to \mathbb{F}_p \to k^s \xrightarrow{\wp} k^s \to 0$ and hence an exact sequence $k \xrightarrow{\wp} k \to H^1(k, \mathbb{F}_p) \to 0$ since $H^1(k, k^s) = 0$. □

Corollary 2.7.5. *Let k be a field of characteristic p and L/k a Galois extension of degree p, then there is a generator $\alpha \in L$ such that $\alpha^p - \alpha \in k$.*

Proof. Similar to 2.7.3. □

Next, let's we see how these ideas can be applied to recover a classical result on elliptic curves.

Theorem 2.7.6 (Weak Mordell-Weil)**.** *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over a number field K, then $E(K)/2E(K)$ is finite.*

Proof. The standard reference for this proof is of course [22].

Without loss of generality we may assume $A, B \in \mathcal{O}_K$. We will also, for the moment, assume that all 2-torsion points of E are defined over K. Note that multiplication times 2 is surjective on $E(\overline{\mathbb{Q}})$. Hence we have an exact sequence

$$0 \to E(\overline{\mathbb{Q}})[2] \to E(\overline{\mathbb{Q}}) \xrightarrow{\cdot 2} E(\overline{\mathbb{Q}}) \to 0.$$

Passing to cohomology we obtain the exact sequence

$$E(K) \xrightarrow{\cdot 2} E(K) \to H^1(K, E(\overline{\mathbb{Q}})[2]) \to H^1(K, E(\overline{\mathbb{Q}})) \tag{1}$$

and hence an injective map

$$E(K)/2E(K) \xrightarrow{\delta} H^1(K, E(\overline{\mathbb{Q}})[2]).$$

It remains to show that the image of δ is finite. Note that we assumed $E(K)[2] = E(\overline{\mathbb{Q}})[2]$. Let $\chi : G_K \to E(K)[2] = E(\overline{\mathbb{Q}})[2]$ be in the image of δ. Since G_K acts trivially on $E(K)[2]$, χ is a continuous homomorphism. As the sequence is exact, $\chi : G_K \to E(K)[2]$ is in the image of δ if and only if it is a coboundary in $H^1(K, E(\overline{\mathbb{Q}}))$ i.e. if and only if there is $P \in E(\overline{\mathbb{Q}})$ such that $2P \in E(K)$ and $\chi(\sigma) = \sigma(P) - P$.

Let L/K be the field extension generated by the coordinates of all the points $P \in E(\overline{\mathbb{Q}})$ such that $2P \in K$. Then $\bigcap_{\chi \in \operatorname{im} \delta} \ker \chi = \operatorname{Gal}(\overline{\mathbb{Q}}/L)$ and in particular $\operatorname{Gal}(\overline{\mathbb{Q}}/L)$ is a closed normal subgroup, so L/K is Galois. We will show that L/K is a finite extension since then the image of δ is contained in $H^1(\operatorname{Gal}(L/K), E(K)[2])$ which is a finite group.

For any $\sigma \in \operatorname{Gal}(L/K)$ we have $\sigma^2 = \operatorname{id}$. To see this extend σ to $\sigma' : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}$ and note that $\chi((\sigma')^2) = 2\chi(\sigma') = 0$ for all $\chi \in \operatorname{im} \delta$ so $(\sigma')^2$ and in particular σ^2 fixes L. This implies that $\operatorname{Gal}(L/K) \cong \prod_{s \in S} \langle \sigma_s \rangle$ for some set S, where each σ_s has order 2. By Kummer theory L is of the form $L = K(\sqrt{a_s} : s \in S)$ for some $a_s \in K$ and σ_s acts as $\sqrt{a_s} \mapsto -\sqrt{a_s}$.

Suppose $p \subset \mathcal{O}_K$ is a prime where E has good reduction and $p \nmid 2$. Then the reduction $E(K)[2] \to E(\mathcal{O}_K/p)$ is injective by [22, VII.3.1]. Let $K \subset L' \subset L$ be a finite Galois subextension, $\mathfrak{p}$ a prime of L' lying over p and σ in the inertia group at $\mathfrak{p}$, then $\sigma(P) - P = 0$ in $E(\mathcal{O}_{L'}/\mathfrak{p})$ for all P with coefficients in L' since σ induces the identity on $\mathcal{O}_{L'}/\mathfrak{p}$. But as the reduction was injective this shows that $\sigma(P) - P = 0$ in $E(K)$ and so $\sigma = \operatorname{id}$. This shows that the inertia group at primes of good reduction is trivial, i.e. L' is unramified at all such primes. Since L is generated by the L', we conclude that L is unramified at all such p.

Going back to our description of L we conclude that the only prime divisors of the a_s are in the finite set of primes where E has bad reduction. Hence to show that the extensions L/K is finite we only need to show that $\{x \in K^\times/(K^\times)^2 : q|x \implies \text{ E has bad reduction at } q\}$ is finite which follows directly from the S-unit version of the Dirichlet unit theorem [17, Theorem 5.11].

Earlier we assumed that the 2 torsion of E is contained in $E(K)$. We now show that this assumption is harmless. Let $K \subset L$ be a finite Galois extension such that $E(L)$ contains the 2 torsion, then $E(L)/2E(L)$ is finite and we have the commutative diagram

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & H^1(L/K, E(L)[2]) \arrow[d] \\
E(K) \arrow[r, "\cdot 2"] \arrow[d] & E(K) \arrow[r] \arrow[d] & H^1(K, E(L)[2]) \arrow[d] \\
E(L) \arrow[r, "\cdot 2"] & E(L) \arrow[r] & H^1(L, E(L)[2])
\end{tikzcd}$$

Since $H^1(L/K, E(L)[2])$ is finite this shows that $E(K)/2E(K)$ is finite. □

2.8 Cohomological Dimension

A major difference between the cohomology of finite groups and the cohomology of profinite groups is that many interesting profinite groups have finite 'cohomological dimension'. That is for large indices i, $H^i(G, A) = 0$ for all discrete G-modules A. Note that already cyclic groups do not have this property. The main reference for this topic is [21]. Throughout let G be a profinite group.

Definition 2.8.1. *The p-cohomological dimension of G, denoted* $\mathrm{cd}_p(G)$*, is the least* n *such that for all p-primary discrete G-modules A we have* $H^k(G, A) = 0$ *for all* $k > n$*. If no such* n *exists, it is defined to be* ∞*.*

Definition 2.8.2. *We set* $\mathrm{cd}(G) = \sup \mathrm{cd}_p(G)$ *and if k is a field, then we set* $\mathrm{cd}(k) = \mathrm{cd}(G_k)$ *and* $\mathrm{cd}_p(k) = \mathrm{cd}_p(G_k)$*, where* $G_k := \mathrm{Gal}(k^s/k)$*.*

Lemma 2.8.3. *If* $H < G$ *is a closed subgroup, then* $\mathrm{cd}_p(H) \leq \mathrm{cd}_p(G)$*.*

Proof. We have $H^n(G, \mathrm{Ind}_H^G(A)) = H^n(H, A)$ for all discrete H-modules A and if A is p-primary, then so is $\mathrm{Ind}_H^G(A)$. □

Lemma 2.8.4. *Let* $H < G$ *be a pro-p Sylow subgroup, then* $cd_p(G) = cd_p(H)$*.*

Proof. For every open normal subgroup $U < G$, $H/(U \cap H)$ is a p Sylow subgroup of G/U and so by 2.4.11, $\mathrm{Res} : H^n(G/U, A^U) \to H^n(H/(U \cap H), A^U)$ is injective for all n. Hence $H^n(G, A) \to H^n(H, A)$ is injective by 2.6.15. This shows $\mathrm{cd}_p(G) \leq \mathrm{cd}_p(H)$ and the other inequality is satisfied by 2.8.3. □

Lemma 2.8.5. *For a pro-p group G, the following are equivalent*

(i) $\mathrm{cd}_p(G) \leq n$

(ii) $H^{n+1}(G, A) = 0$ *for all discrete p-primary G-modules A.*

(iii) $H^{n+1}(G, A) = 0$ *for all finite discrete p-primary G-modules A.*

(iv) $H^{n+1}(G, A) = 0$ *for all finite simple p-primary discrete G-modules A.*

(v) $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$

Proof. Clearly $(i) \implies (v)$. Now assume (v) and let A be a finite simple p-primary discrete G-module A and let $U \subset \bigcap_{a \in A} \mathrm{Stab}(a)$ be an open normal subgroup of G. Then A is a $\mathbb{Z}[G/U]$-module. Since A is simple, either $pA = A$ or $pA = 0$. If $pA = A$, then A would be divisible and so either 0 or infinite. Consequently A is an irreducible representation of the p-group G/U over $\mathbb{F}_p$, i.e. an irreducible modular representation. The only such representation is the trivial one [26, Proposition 6.2.1], so $A = \mathbb{Z}/p\mathbb{Z}$.

Suppose (iv), and let A be a finite discrete p-primary G-module A. Let $A = A = A_0 \supset A_1 \supset A_2 \supset \cdots \supset A_m = 0$ be a composition series of A. Then $H^{n+1}(G, A_i/A_{i+1}) = 0$ for all i by assumption. From the long exact sequence in cohomology we find that $H^{n+1}(G, A_{i+1}) \to H^{n+1}(G, A_i)$ is surjective for all i and so $H^{n+1}(G, A) = 0$.

If (iii) holds, let A be a discrete p-primary G-module. Then $H^{n+1}(G, A') = 0$ for all finite submodules $A' \subset A$. Since A is torsion we find $A = \lim_{\to} A_f$, where A_f runs through the finite submodules of A. Now 2.6.18 implies $H^{n+1}(G, A) = 0$.

Assume (ii) and let $k \geq 1$ such that $H^{n+k}(G, A) = 0$ for all discrete p-primary G-modules A. Then we can embed $A \subset C = \mathrm{Ind}_1^G(A)$ which is p-primary as well. By Shapiro's lemma $H^q(G, C) = 0$ for all $q \geq 1$. Hence the coboundary $\delta : H^{n+k}(G, C/A) \to H^{n+k+1}(G, A)$ is an isomorphism and $H^{n+k+1}(G, A) = 0$. By induction we conclude (i). □

Definition 2.8.6. *A free pro-p group on a set S is a free object in the category of pro-p groups, i.e. a group $F(S)$ with $S \subset F(S)$ such that for every function $f : S \to G$ for some pro-p group G there exists a unique homomorphism $\tilde{f} : F(S) \to G$ such that $\tilde{f}(s) = f(s)$ for $s \in S$. The cardinality of S is the rank of the free pro-p group $F(S)$.*

If a free pro-p group on S exists it is automatically unique up to unique isomorphism since it was defined by a universal property. We can show existence of a free pro-p group by taking the ordinary free group K on the set S and setting

$$F(S) = \lim_{\leftarrow} K/U,$$

where U runs through the finite index normal subgroups of K such that K/U is a p-group.

Lemma 2.8.7. *Let G be a free pro-p group of rank ≥ 1, then* $\mathrm{cd}_p(G) = \mathrm{cd}(G) = 1$

Proof. Since G is a pro-p group we have $\mathrm{cd}(G) = \mathrm{cd}_p(G)$ by 2.8.4. Since the rank is ≥ 1 there exists a non-trivial continuous homomorphism $G \to \mathbb{Z}/p\mathbb{Z}$, i.e. $H^1(G, \mathbb{Z}/p\mathbb{Z}) \neq 0$ and $\mathrm{cd}_p(G) \geq 1$.

For $\mathrm{cd}_p(G) \leq 1$ we show that $H^2(G, \mathbb{Z}/p\mathbb{Z}) = 0$. It turns out that in abstract cohomology there is a bijection between $H^2(G, A)$ and classes of group extensions $1 \to A \to E \to G \to 1$ such that the G-action on A induced by conjugation in E agrees with the action on A as a $\mathbb{Z}[G]$-module [20, VII. §3]. Here two extensions are equivalent if there exists a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & A \arrow[r] \arrow[d, "1"] & E \arrow[r] \arrow[d] & G \arrow[r] \arrow[d, "1"] & 1 \\
1 \arrow[r] & A \arrow[r] & E' \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

The correspondence comes from the following construction. Given the extension $1 \to A \to E \to G \to 1$ we choose a for each $g \in G$ a representative $s(g) \in E$, i.e. $s : G \to E$ is a set-theoretic section. Then $s(g)s(g')A = s(gg')A$ and so there exists a function $f : G^2 \to A$ such that $s(g)s(g') = f(g, g')s(gg')$ and conversely given f one can construct a multiplication on E in this way. The associativity of multiplication in E then shows that f satisfies the cocycle condition and so defines an element in $H^2(G, A)$. We don't need the whole correspondence but the proof idea is based on this concept. When G is a free group, then any surjective map $E \to G$ admits a section $G \to E$ which will then show that the corresponding cocycle is a coboundary.

So let $f \in C^2(G, \mathbb{Z}/p\mathbb{Z})$ be a continuous cocycle and let $E = \mathbb{Z}/p\mathbb{Z} \times G$ as a topological space, where $\mathbb{Z}/p\mathbb{Z}$ has the discrete topology and G the profinite topology. We define a group structure on E using f. If $(a, g), (a', g') \in E$, then we set $(a, g)(a', g') = (a + ga' + f(g, g'), gg')$. Since f satisfies

$$gf(g', g'') + f(g, g'g'') = f(gg', g'') + f(g, g')$$

this operation is associative. Setting $g' = g'' = 1$ we find $gf(1, 1) = f(g, 1)$ for all $g \in G$ and so $(a, g)(-f(1, 1), 1) = (a, g)$ for all $(a, g) \in E$ and $(-f(1, 1), 1)$ is a right identity element. Finally, one can verify that a right inverse of (a, g) is given by $(-g^{-1}f(1, 1) - g^{-1}a - g^{-1}f(g, g^{-1}), g^{-1})$ and consequently E is a group. Since f is continuous E even has the structure of a compact topological group and the projection $E \to G$ is a surjective continuous group homomorphism. Using 2.6.6 we verify that E is a profinite group. Let $V \subset E$ be an open neighbourhood of the identity, then V contains a set of the form $\{-f(1, 1)\} \times U$, where $U \subset G$ is an open neighbourhood of the identity. G is profinite and so there is an open subgroup $H < G$ such that $\{-f(1,1)\} \times H \subset E$. However, this might not be a subgroup of E. But if we can construct an open subgroup $M < G$ such that $\{-f(1,1)\} \times M$ is a subgroup of E, then we can intersect M with H to find the desired subgroup of E. To find M, consider the open set $S = \{(g,g') : f(g,g') = gf(1,1) \wedge f(1,1) = g^{-1}f(g,g^{-1})\} \subset G \times G$. Since G is profinite and $(1,1) \in S$, there exists an open subgroup $M < G$ such that $M \times M \subset S$. Now if $g, g' \in M$, then

$$(-f(1,1),g)(-f(1,1),g') = (-f(1,1) - gf(1,1) + f(g,g'), gg') = (-f(1,1), gg')$$

and

$$(-f(1,1),g)^{-1} = (-g^{-1}f(1,1) + g^{-1}f(1,1) - g^{-1}f(g,g^{-1}), g^{-1}) = (-f(1,1), g^{-1}),$$

thus $\{-f(1,1)\} \times M \subset E$ is a subgroup. Hence E is profinite and in particular a pro-p group. Now since G is free, there exists a continuous section $\sigma : G \to E$ which is also a homomorphism. If we write $\sigma(g) = (-h(g), g)$, then this implies

$$(-h(gg'), gg') = (-h(g), g)(-h(g'), g') = (-h(g) + -gh(g') + f(g,g'), gg')$$

and so $f(g,g') = gh(g') - h(gg') + h(g)$ is a coboundary as desired. □

Corollary 2.8.8. $\mathrm{cd}(\hat{\mathbb{Z}}) = 1$.

Proof. Since $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, the pro-$p$ sylow subgroup of $\hat{\mathbb{Z}}$ is $\mathbb{Z}_p$. This is a free pro-p group of rank 1: Let $G = \lim G_i$ be a pro-p group and $x \in G$, then for each i we have a map $\mathbb{Z}_p \to G_i$ such that $1 \mapsto x$ since the G_i are p-groups and so the order of x is a power of p in G_i. These maps are easily seen to be compatible and hence there is a continuous map $\mathbb{Z}_p \to G$ such that $1 \mapsto x$. This map is unique since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. We conclude that $\mathrm{cd}(\hat{\mathbb{Z}}) = 1$ by 2.8.4 and 2.8.7. □

Corollary 2.8.9. *For any perfect field k such that $G_k \cong \hat{\mathbb{Z}}$ we have $H^2(k, \overline{k}^{\times}) = 0$.*

Proof. Since $\mathrm{cd}(k) = 1$ we immediately find that $H^2(k, \mu_\ell) = H^3(k, \mu_\ell) = 0$, where μ_ℓ is the group of ℓth roots of unity contained in k^s. But from the long exact sequence associated to $1 \to \mu_\ell \to \overline{k}^{\times} \xrightarrow{\ell} \overline{k}^{\times} \to 1$ we conclude that multiplication by ℓ is an isomorphism on $H^2(k, \overline{k}^{\times})$. But since $H^2(k, \overline{k}^{\times}) = \lim_{\to} H^2(L/k, L^s)$ is a torsion module we must have $H^2(k, \overline{k}^{\times}) = 0$. □

The point of this corollary is that $H^2(k, \overline{k}^{\times})$ has another interpretation which classifies division algebras over k whose center is k as we see later. Now this means that over any field such that $\mathrm{cd}(k) = 1$ there are no non-trivial such division algebras. For example finite fields have absolute Galois group $\hat{\mathbb{Z}}$ and so we can directly show that every finite division algebra is commutative. This can of course also be proven elementarily. But there are also stranger fields with absolute Galois group $\hat{\mathbb{Z}}$. For example let k be algebraically closed of characteristic 0, then one can show that all finite extensions of $k((t))$ are ramified and using ramification theory one can show that these are all cyclic. Hence the algebraic closure of $k((t))$ is the union $\bigcup_{n\geq 1} k((t^{1/n}))$ [20, IV. Prop 8]. From this it follows that the absolute Galois group of $k((t))$ is $\hat{\mathbb{Z}}$ and so there are no division algebras over $k((t))$ with center $k((t))$. Indeed every division algebra D over $k((t))$ is commutative since its center is a finite extension $L/k((t))$ whose Galois group is a closed subgroup of $\hat{\mathbb{Z}}$. Hence $\mathrm{cd}(L) \leq 1$ by 2.8.3 and $D = L$.

The ideas in lemma 2.8.7 can in fact be taken quite a bit further to show that there is an equivalence between $\mathrm{cd}(G) \leq 1$ and G being a free pro-p group. More precisely, this can be used to show

Theorem 2.8.10. *Let G be a pro-p group, then $n(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z})$ is the minimal number of generators needed to generate G as a pro-p group and $r(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z})$ is the minimal number of relations between those generators needed to describe G.*

Proof. See [21, I. 4.2-4.3]. □

3 Nonabelian Cohomology

One of the strengths of Galois Cohomology is that there are many different interpretations of the group $H^1(G, A)$. In this section we will see more such interpretations which don't even require A to be abelian. Our exposition is based on [21, I. §5], [9, Chapter 2] and [7]. When trying to define $H^q(G, A)$ for nonabelian groups A on which G acts by automorphisms, one runs into the difficulty that in general the coboundaries don't form a normal subgroup or not even a group! However, we can still define $H^0(G, A)$ as A^G which agrees with the abelian case and is a group. For $H^1(G, A)$ we define

Definition 3.0.1. *Let A be a group on which G acts by automorphisms. Then we define the pointed set (not group!)*

$$H^1(G, A) = \{f : G \to A : f(gh) = f(g)g(f(h))\}/\sim,$$

where $f \sim f'$ if and only if there is $a \in A$ such that $f(g) = a^{-1}f'(g)g(a)$ for all $g \in G$. The distinguished element is the class of elements of the form $a^{-1}g(a)$, $a \in A$.

If A is abelian this reduces to our old definition using inhomogeneous cochains. We will not attempt to define higher nonabelian cohomology groups. In the previous definition one has to check that $f_a(g) = a^{-1}g(a)$ satisfies the cocycle condition and that f_a and f_b are equivalent for all $a, b \in A$. This follows from

$$f_a(gh) = a^{-1}gh(a) = a^{-1}g(a)g(a^{-1})gh(a) = f_a(g)g(f_a(h))$$

and

$$f_a(g) = a^{-1}g(a) = (b^{-1}a)^{-1}b^{-1}g(b)g(b^{-1}a) = (b^{-1}a)^{-1}f_b(g)g(b^{-1}a).$$

With these definitions we still have

Lemma 3.0.2. *Let $1 \to A \to B \to C \to 1$ be a short exact sequence of groups with compatible G-actions. Then we have an exact sequence in cohomology*

$$1 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C).$$

Proof. The interesting part is the map $\delta : C^G \to H^1(G, A)$. It is defined as follows. Denote the maps in the original sequence by $\pi : B \to C$ and $\iota : A \to B$. Let $c \in C^G$, then there is $b \in B$ such that $\pi(b) = c$ and $f_b(g) = b^{-1}g(b)$ is a priori an element of $H^1(G, B)$. But in fact we have that $\pi(f_b(g)) = \pi(b)^{-1}\pi(g(b))^{-1} = c^{-1}g(c) = 1$ since $c \in C^G$. By the exactness of the original sequence we have $f_b(g) \in A$, i.e. $f_b \in H^1(G, A)$. f_b does not depend on the choice of b. Let $b, b' \in B$ such that $\pi(b) = \pi(b')$, then $f_{b'}(g) = (b^{-1}b')^{-1}f_b(g)g(b^{-1}b')$ and $b^{-1}b' \in \ker(\pi) = A$, hence $f_{b'} \sim f_b$. Thus it makes sense to define $\delta c := f_b$ for any lift b of c.

An element c is in the kernel of δ if and only if there exists $b \in B$ and $a \in A$ such that $\pi(b) = c$ and $b^{-1}g(b) = a^{-1}g(a)$ for all $g \in G$, i.e. $ba^{-1} \in B^G$. Since $\pi(ba^{-1}) = c$ this is true if and only if there is a lift $b \in B^G$ of c, i.e. if $c \in \pi(B^G)$.

If $f \in H^1(G, A)$ is in the image of δ, then by definition it is trivial in $H^1(G, B)$. On the other hand if $f \in H^1(G, A)$ becomes trivial in $H^1(G, B)$ then there exists $b \in B$ such that $f(g) = b^{-1}g(b)$ and hence $1 = \pi(f(g)) = c^{-1}g(c)$ where $c = \pi(b)$. Hence $c \in C^G$ and $f = \delta c$. Exactness at the other points in the sequence is easily verified. □

Of course if G is profinite and acts continuously on A with the discrete topology, then we can define $H^1(G, A)$ with continuous cocycles or equivalently as the limit $\lim_{\to} H^1(G/U, A^U)$. Moreover, the previous lemma still holds when G is profinite and if $G = \mathrm{Gal}(L/K)$ is a Galois group we write $H^1(L/K, A)$ for $H^1(G, A)$.

3.1 Galois Descent

Let us now introduce the main example of nonabelian cohomology. Throughout we fix a finite Galois extension L/K. The question is whether two objects which are isomorphic over L are also isomorphic over K, i.e. if we can descend from an isomorphism over L to an isomorphism over K. This is a very imprecise formulation so here an example. Consider the extension $\mathbb{C}/\mathbb{R}$, then any two quadratic forms on a real vector space V become isomorphic on $V \otimes_{\mathbb{R}} \mathbb{C}$ and so the answer is clearly no since $x^2 - y^2$ and $x^2 + y^2$ are not isomorphic over $\mathbb{R}$. But using cohomology we can precisely determine when the answer is no and even classify all objects Y over K which become isomorphic to a fixed object X over L. This is a key idea in the study of central simple algebras and in particular in proving the cohomological interpretation of the Brauer group.

To formalise this we need to make a few conventions. Our approach is slightly more general than the one in [9, Chapter 2] but the ideas are basically the same. Let $\mathscr{C}_L$ be a category whose objects are L-vector spaces with additional structure and such that every morphism is also a linear map. Moreover, we assume that $\mathscr{C}_L$ is a subcategory of another category $\mathscr{C}_K$ which consists of K-vector spaces with additional structure and there is a 'base-change' functor $F : \mathscr{C}_K \to \mathscr{C}_L$. We make the following assumptions:

(A) A morphism in $\mathscr{C}_L$ is an isomorphism if and only if it is bijective on the underlying vector space.

(B) For every object A in $\mathscr{C}_L$ and finite group of automorphisms H, there exists a fixed object A^H, i.e. an object B with a morphism $\iota : B \to A$ such that for all morphisms $f : C \to A$ such that $h \circ f = f$ for all $h \in H$ there exists a unique $\tilde{f} : C \to B$ such that $\iota \circ \tilde{f} = f$.

(C) On the level of vector spaces, $F(V) = V \otimes_K L$.

(D) For every object Y of $\mathscr{C}_K$ there exists an action of $G = \mathrm{Gal}(L/K)$ on $F(Y)$ such that $F(Y)^G \cong Y$ in $\mathscr{C}_K$.

(E) For any objects A in $\mathscr{C}_K$ and B in $\mathscr{C}_L$ and $\mathscr{C}_K$-morphism $f : A \to B$ there exists a unique $\mathscr{C}_L$-morphism $\overline{f} : F(A) \to B$ which extends f.

Now we can formulate Galois Descent in the category $\mathscr{C}_L$.

Theorem 3.1.1 (Galois Descent). *Fix an object $X \in \mathscr{C}_K$, then the set* [1] *of isomorphism classes of objects $Y \in \mathscr{C}_K$ such that $F(Y) \cong F(X)$ is in bijective correspondence with $H^1(L/K, \mathrm{Aut}(F(X)))$, where G acts on $\mathrm{Aut}(F(X))$ by conjugation and the class of X maps to the trivial class in $H^1(G, \mathrm{Aut}(F(X)))$.*

Example 3.1.2. *Let $\mathscr{C}_L$ be the category of L-vector spaces sitting inside the category $\mathscr{C}_K$ of K-vector spaces. Let $F(V) = V \otimes_K L$, where G acts on the right factor, then the conditions $(A)-(E)$ are satisfied. If $V = K^d$, then $\mathrm{Aut}(F(V)) = GL_d(L)$ and any vector space W such that $W \otimes L \cong V \otimes L$ has the same dimension as V and so $H^1(G, GL_d(L)) = 1$. For $d = 1$, this gives another proof of Hilbert's Theorem 90.*

[1] We assume the category to be sufficiently nice such that this is a set.

Example 3.1.3. *Suppose* $\operatorname{char} K \neq 2$ *and let* $\mathscr{C}_K$ *be the category of* K*-vector spaces with a quadratic form and* $\mathscr{C}_L$ *the category of* L*-vector spaces with a quadratic form. Then the orthogonal group* $O_d(L)$ *is the group of automorphisms of* $(L^d, x_1^2+\cdots+x_d^2)$ *and so* $H^1(G, O_d(L))$ *classifies quadratic forms over* K *which are isomorphic to* $x_1^2+\cdots+x_d^2$ *over* L*.*

Example 3.1.4. *Let* $\mathscr{C}_L$ *be the category of smooth projective geometrically irreducible curves over L and* $\mathscr{C}_K$ *the category of smooth projective geometrically irreducible curves over* K*. By switching to the isomorphic categories of function fields we can apply Galois Descent and so for example* $H^1(G, PGL_2(L))$ *classifies the curves which become isomorphic to* $\mathbb{P}^1$ *over* L*.*

Before we go into the proof we need some preliminaries.

Definition 3.1.5. *Let* A *be a group. A torsor for* A *is a nonempty set* X *such that* A *acts freely and transitively on the right on* X*.*

One can think of a torsor as a shadow of the group which forgot the identity element. In particular A itself is a torsor for A. It turns out to be useful to study these to get a better understanding of H^1 and in particular to prove Galois Descent.

Definition 3.1.6. *Let* G *be a group and* A *a group equipped with an action of* G *by automorphisms. Then a* G*-torsor for* A *is a torsor* X *for* A *such that the actions are compatible, i.e. for all* $a \in A, g \in G, x \in X$ *we have*

$$g(x \cdot a) = g(x) \cdot g(a).$$

Two G*-torsors* X, Y *for* A *are isomorphic if there exists a bijection* $\phi : X \to Y$ *such that* $\phi(g(x)) = g(\phi(x))$ *and* $\phi(x \cdot a) = \phi(x) \cdot a$ *for all* $g \in G$ *and* $a \in A$*.*

Lemma 3.1.7. *Let* G *be a group and* A *be a group equipped with an action of* G *by automorphisms. Then* $H^1(G, A)$ *is in bijection with the set of isomorphism classes of* G*-torsors for* A *and the base point is sent to* A*.*

A torsor X *with base point* x *is mapped to the class of the cocycle* $f : G \to A$*, satisfying* $g(x) = x \cdot f(g)$ *and a cocycle* f *is mapped to the torsor with set* $X = A$ *and group action* $g * x = f(g)g(x)$*.*

Proof. Let X be a G-torsor for A. By definition X is nonempty so we may pick $x \in X$. Since A acts freely and transitively, there is a function $f_x : G \to A$ such that $g(x) = x \cdot f_x(g)$ for all $g \in G$. This is a cocycle since

$$x \cdot f(gh) = g(h(x)) = g(x \cdot f(h)) = g(x) \cdot g(f(h)) = x \cdot f(g)g(f(h)).$$

Further the class of $f_x \in H^1(G, A)$ does not depend on the choice of x. To see this consider $x, y \in X$, then there exists $a \in A$ such that $y = x \cdot a$ because A, by definition, acts transitively on X. But now for any $g \in G$

$$y \cdot f_y(g) = g(y) = g(x \cdot a) = g(x) \cdot g(a) = x \cdot f_x(g)g(a) = y \cdot a^{-1} f_x(g)g(a),$$

so $f_x \sim f_y$. We denote the class of this cocycle by $\phi(X)$.

Conversely if $f \in H^1(G, A)$, then we can define a G-torsor by taking the set $X = A$ with the action of A being right multiplication. We define the action of G by $g * x = f(g)g(x)$ for all $g \in G$ and $x \in X$. This is a group action since for $g, h \in G$ and $x \in X$

$$gh * x = f(gh)gh(x) = f(g)g(f(h)h(x)) = f(g)g(h * x) = g * (h * x)$$

and $f(e) = f(ee) = f(e)f(e)$ implies that $f(e) = e$, hence $e * x = x$. This action is compatible with the action of A since for $g \in G, x \in X, a \in A$ we have

$$g * (x \cdot a) = g * (xa) = f(g)g(xa) = (g * x)g(a).$$

We denote this torsor by $\psi(f)$. It is clear that ψ sends the trivial class, i.e. the class of the constant cocycle $g \mapsto e$ to the torsor A.

It remains to show that ϕ and ψ are inverse to each other. So let $f \in H^1(G, A)$ and $f' = \phi(\psi(f))$, then by definition we have $f'(g) = ef'(g) = g * e = f(g)e = f(g)$. Let X be a G-torsor for A and fix $x \in X$, then we have a bijection $\alpha : X \to \psi(\phi(X))$ given by $\alpha(x \cdot a) = a$. α is an isomorphism since if $y = x \cdot b \in X$ and $a \in A$, then $\alpha(y \cdot a) = \alpha(x)ba = \alpha(y)a$. Moreover for all $g \in G$ and $a \in A$ one has

$$\alpha(g(x \cdot a)) = \alpha(x \cdot af(g)) = af(g) = g(\alpha(x \cdot a)). \qquad \square$$

Proof of Galois Descent. Suppose Y is an object of $\mathscr{C}_K$ such that $F(Y) \cong F(X)$ in $\mathscr{C}_L$. Then $A = \operatorname{Aut}(F(X))$ acts transitively and freely on the set of isomorphisms $F(X) \to F(Y)$ by composition on the right. Further we have a compatible G-action on the set of isomorphisms $F(X) \to F(Y)$ by conjugation. More precisely, if $\alpha : F(Y) \to F(X)$ is an isomorphism, $\phi \in A$ and $\sigma \in G$, we have $\sigma \circ \alpha \circ \phi \circ \sigma^{-1} = \sigma \circ \alpha \circ \sigma^{-1} \circ \sigma \circ \phi \circ \sigma^{-1}$. Hence every object in $\mathscr{C}_K$ that becomes isomorphic to $F(X)$ in $\mathscr{C}_L$ gives rise to a G-torsor for A.

On the other hand given a G-torsor for A we can take a corresponding cocycle $f \in H^1(G, A)$ and attach to it an object Y of $\mathscr{C}_K$ as follows. Define a new G-action on $F(X)$ by letting g act by $f(g) \circ g$. This is a group action thanks to the cocycle condition as in the proof of 3.1.7. Now let Y be the fixed object under this group action whose existence is guaranteed by (B). Moreover if $f'(g) = a^{-1}f(g)a^g$ is another cocycle representing the same class as $f(g) \in H^1(G, A)$, then $a^{-1}f(g)ga = f'(g)g$ and so a defines an isomorphism between Y' and Y, where Y' is the object associated to f'. Hence the construction doesn't depend on the choice of cocycle.

We wish to show that $F(Y) \cong F(X)$. We already have a canonical map $Y \to F(X)$ since Y is the fixed object of some group action. By (E) this extends to a unique L-linear map $\alpha : F(Y) \to F(X)$.

The rest of the proof uses the method from [7]. Consider the vector space $U = F(X)/F(Y)$. It has a G-action induced by the modified G-action on $F(X)$. Let $v \in F(X)$ and denote by $\overline{v}$ its class in the quotient U. Define the trace $Tr(v) = \sum g * v \in Y$. So Tr maps U to 0. Let $\overline{v} \in U$, then for $a \in L^\times$ we have

$$Tr(a\overline{v}) = \sum_{g \in G} g(a)(g * \overline{v}) = 0.$$

But the functions $a \mapsto g(a)$ are L-linearly independent by Lemma 2.2.1. Hence $g * \overline{v} = 0$ for all $g \in G$ and in particular $\overline{v} = 0$. Thus α is surjective.

Next we show that it is injective. Let $v_1, \ldots, v_d$ be a K-basis of Y, then $\alpha(v_1), \ldots, \alpha(v_d)$ is K-linearly independent in $F(X)$ and by (C) it suffices to show that it is L-linearly independent as well. Suppose it isn't, then we may take a minimal relation $\sum_{i=1}^k \lambda_i \alpha(v_i) = 0$ and without loss of generality we assume $\lambda_1 = 1$. Since the v_i are G-invariant (under the modified action) we get another relation $\sum_{i=1}^k \sigma(\lambda_i)\alpha(v_i)$ for every $\sigma \in G$ But since the v_i are K-linearly independent there exists σ such that $\sigma(\lambda_j) \neq \lambda_j$ for some j. Subtracting the new relation with such a σ gives a strictly shorter non-trivial relation since $1 - \sigma(1) = 0$. Contradiction. Finally α is bijective and (A) implies $F(X) \cong F(Y)$.

It remains to prove that these constructions are inverse to each other. If we start with an object Y such that there is an isomorphism $\alpha : F(X) \to F(Y)$, then the associated cocycle is $f(\sigma) = \alpha^{-1} \circ \alpha^\sigma$ since this is the unique automorphism such that $\alpha^\sigma = \alpha \circ f(\sigma)$. Then $f(\sigma) \circ \sigma = \alpha^{-1} \circ \sigma \circ \alpha$ and so α defines an isomorphism between the fixed points of $f(\sigma) \circ \sigma$ and the fixed points of σ, i.e. between Y' and Y, where Y' is the object associated to f and using (D) we find that the object associated to f is isomorphic to $F(Y)^G = Y$.

If we start with a cocycle f, we get an object Y and an isomorphism $\alpha^{-1} : F(Y) \to F(X)$ induced by the inclusion $Y \to F(X)$. The cocycle we get back is $g(\sigma) = \alpha^{-1} \circ \sigma \circ \alpha \circ \sigma^{-1}$. Suppose $x \in F(X)$ such that $x = \lambda y$ with $\lambda \in L$ and $y \in Y$, then $\alpha(\lambda y) = \lambda \otimes y$ and so $(\alpha^{-1} \circ \sigma \circ \alpha)(\lambda y) = \sigma(\lambda) y = \sigma(\lambda) f(\sigma)\sigma(y) = f(\sigma)(\sigma(\lambda y))$. Since $F(X)$ is spanned by Y over L we find that $\alpha^{-1} \circ \sigma \circ \alpha = f(\sigma) \circ \sigma$ and $f = g$ as required. □

3.2 Principal Homogeneous Spaces

This section treats a special class of Torsors called principal homogeneous spaces.

Definition 3.2.1. *Let A be an algebraic group defined over k. A variety V defined over k together with a free and transitive (right) action of A on V by morphisms is* *called a principal homogeneous space for A over k if the map $V \times V \to A$ sending (v, w) to the element $a \in A$ such that $va = w$ is a k-morphism, which we will denote by $v^{-1}w$. Two principal homogeneous spaces V, V' for A over k are isomorphic if there is a k-isomorphism $\phi : V \to V'$ such that $\phi(v)a = \phi(va)$ for all $v \in V$ and $a \in A$.*

In particular we treat the special case when A is an elliptic curve E over k, i.e. a smooth projective irreducible curve of genus 1 which has a k-point and which has defining equations with coefficients in k. Any principal homogeneous space V for E is isomorphic to E over $\overline{k}$ since the map $a \mapsto av_0$ for some $v_0 \in V$ is an isomorphism with inverse $v \mapsto v_0^{-1}v$.

Proposition 3.2.2. *Let K/k be a finite Galois extension. The set of isomorphism classes of principal homogeneous spaces for E over k which have a K-point is in bijective correspondence with $H^1(K/k, E_K)$, where the trivial class corresponds to those spaces which have a k-point.*

Proof. If V is a principal homogeneous space for E which has a K-point v_0, then $V \to E : v \mapsto v_0^{-1}v$ is an isomorphism defined over K. So V has a K-point if and only if it becomes isomorphic to E over K. Moreover the automorphisms of E as an principal homogeneous space are just translation by some point and so the group of automorphisms defined over K is just E_K. It remains to check that the conditions for Galois Descent are satisfied. But the category of smooth irreducible projective curves is isomorphic to the category of the corresponding function fields and so this is easily verified. The proof in [22, X.2. Theorem 2.2] uses the same idea but basically reproves Galois Descent for curves. □

Example 3.2.3. *Let E be the elliptic curve over $\mathbb{Q}$ defined by $x^3 + y^3 + 60z^3 = 0$ with origin $[1, -1, 0]$ and let V be the projective cubic defined by $3x^3 + 4y^3 + 5z^3 = 0$, then V is a principal homogeneous space for E over $\mathbb{Q}$.*

Proof. Let $K = \mathbb{Q}(e^{2\pi i/3}, 3^{1/3}, 4^{1/3})$ and consider the K-isomorphism

$$\alpha : V \to E : [x, y, z] \mapsto [3^{1/3}x, 4^{1/3}y, 12^{-1/3}z],$$

then E acts on V by $(v, a) \mapsto \alpha^{-1}(\alpha(v) + a)$. Thus V is already a principal homogeneous space for E over K. We just have to show that it is also a principal homogeneous space over $\mathbb{Q}$, i.e. that the map $V \times V \to E : (v, w) \mapsto \alpha(v) - \alpha(w)$ is defined over $\mathbb{Q}$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Since addition on E is defined over $\mathbb{Q}$ we only need that $\alpha^\sigma(v) - \alpha^\sigma(w) = \alpha(v) - \alpha(w)$ for all $v, w \in V$ or equivalently that $\alpha^\sigma(\alpha^{-1}(P)) - P$ is constant for $P \in E$. If $P = [x, y, z]$, then $\alpha^\sigma(\alpha^{-1}(P)) = [\omega_1 x, \omega_2 y, (\omega_1\omega_2)^{-1}z]$, where $\sigma(3^{1/3}) = \omega_1 3^{1/3}$ and $\sigma(4^{1/3}) = \omega_2 4^{1/3}$. For $P = [1, -1, 0]$ we get $\alpha^\sigma(\alpha^{-1}(P)) - P = [\omega_1, -\omega_2, 0]$, so we need to check that

$\alpha^\sigma(\alpha^{-1}(P)) - P = [\omega_1, -\omega_2, 0]$ for all $P \in E$. Since $[-1, 1, 0]$ is a point of inflexion suffices to show that $P, [\omega_1, -\omega_2, 0]$ and $-\alpha^\sigma(\alpha^{-1}(P))$ are collinear and using that $-[x, y, z] = [y, x, z]$ on E we are left with showing that $[x, y, z], [\omega_1, -\omega_2, 0]$ and $[\omega_2 y, \omega_1 x, (\omega_1\omega_2)^{-1}z]$ are collinear but this follows from the easily verifiable fact that

$$\det \begin{pmatrix} x & y & z \\ \omega_2 y & \omega_1 x & (\omega_1\omega_2)^{-1}z \\ \omega_1 & -\omega_2 & 0 \end{pmatrix} = 0. \qquad \square$$

Corollary 3.2.4. *Keeping the notation from 3.2.3, V has no rational points.*

Proof. By 3.2.2, V has no rational points if and only if V does not correspond to the trivial class in $H^1(K/\mathbb{Q}, E_K)$. Let $v = [4^{1/3}, -3^{1/3}, 0] \in V$, then we need to show that there is no $P \in E_K$ such that $\alpha(\sigma(v)) - \alpha(v) = \sigma(P) - P$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. We do this by contradiction. Suppose there was such a $P \in E_K$. Let $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ and $\omega_1 = \sigma(3^{1/3})3^{-1/3}, \omega_2 = \sigma(4^{1/3})4^{-1/3}$. Then $\alpha(\sigma(v)) - \alpha(v) = [\omega_2, -\omega_1, 0] - [1, -1, 0] = [\omega_2, -\omega_1, 0]$. Recall that if the origin of an elliptic curve is a point of inflexion then 3 points add to 0 if and only if they are collinear. The line $\omega_1 X + \omega_2 Y = 0$ intersects E in $[\omega_2, -\omega_1, 0]$ only and so $3[\omega_2, -\omega_1, 0] = 0$, hence $\sigma(3P) = 3P$ for all $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Using sage one can check that $E_\mathbb{Q} = 0$ and so $3P = 0$. Moreover, E is isomorphic to the elliptic curve given by $y^2 + 2xy + 20y = x^3 - x^2 - 20x - 400/3$ and its third division polynomial is $3x^4 - 400x$. Note that if $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ fixes $(3/4)^{1/3}$, then $[\omega_2, -\omega_1, 0] = [1, -1, 0]$ and so $\sigma(P) = P$. As a result $P \in E_F$, where $F = \mathbb{Q}((3/4)^{1/3})$. If $P = (x, y)$, then $3P$ implies $3x^4 - 400x = 0$ and since $400/3 = 4/3 \cdot 100$ is not a cube in F we must have $x = 0$ and $y^2 + 20y + 400/3 = 0$, but then $y \notin \mathbb{R}$ and $F \subset \mathbb{R}$ which is a contradiction. $\square$

In general one can similarly show that $ax^3 + by^3 + cz^3 = 0$ is a principal homogeneous space for the elliptic curve $x^3 + y^3 + abcz^3 = 0$ and one can check whether $ax^3 + by^3 + cz^3 = 0$ has a rational point by computing with the elliptic curve $x^3 + y^3 + abcz^3 = 0$. By first treating the cases $p = 3, 4, 5$ and then using that at least one of $3, 5, 15, 45$ must be a cube mod another prime p one can show that $3x^3 + 4y^3 + 5z^3 = 0$ has a point in all completions of $\mathbb{Q}$. This method was given as an exercise in the Elliptic Curves Course taught at Imperial College London by Toby Gee this year.

Hence the curve $3x^3 + 4y^3 + 5z^3 = 0$ gives a non-trivial element of the Tate-Shafarevic group $Ш(E/\mathbb{Q})[3]$, where E is the elliptic curve $x^3 + y^3 + 60z^3 = 0$. For an infinite family of elliptic curves with $Ш(E/\mathbb{Q})[2] \neq 0$, see [22, X.6.5] which says that for a prime $p \equiv 1 \pmod 8$ such that 2 is not a 4th power mod p, the equations $w^2 = 1 + 4pz^4$, $w^2 + 2 = 2pz^4$, $w^2 + 2pz^4 = 2$ have solutions in all completions of $\mathbb{Q}$ but not in $\mathbb{Q}$ and $Ш(E/\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$, where E is the elliptic curve $y^2 = x^3 + px$.

The definition of principal homogeneous space worked for a general algebraic group and indeed we still have

Proposition 3.2.5. *Let K/k be a finite Galois extension and A an algebraic group over k. The set of isomorphism classes of principal homogeneous spaces for A over k which have a K-point is in bijective correspondence with $H^1(K/k, A_K)$.*

However, the proof is more complicated since we cannot just move to the category of function fields anymore. It relies on Weil's descent criterion [27, Theorem 3] and can be found in [14, Proposition 4].

4 Central Simple Algebras

Throughout this section fix a perfect[2] field k and an algebraic closure $\overline{k}$. Quite surprisingly central simple algebras are intimately connected to Galois Cohomology and Class Field Theory. The book [9] studies this connection in great detail and we put together some of them in this section.

Definition 4.0.1. *A central simple algebra (c.s.a.) over k is a ring with unity A containing k such that the center of A is k, A is a finite dimensional vector space over k and A contains no proper two-sided ideals.*

Example 4.0.2. *Any division algebra is a central simple algebra over its center.*

Example 4.0.3. *For $a, b \in k$ we may define the quaternion algebra $Q(a,b)_k$ by adjoining elements i, j to k satisfying the relations*

$$i^2 = a, j^2 = b, ij = -ji.$$

More explicitly we can take $i = \begin{pmatrix} 0 & a \\ 1 & 0 \end{pmatrix}$ and $j = \begin{pmatrix} \sqrt{b} & 0 \\ 0 & -\sqrt{b} \end{pmatrix}$ and see $Q(a,b)_k$ as a subalgebra of $M_2(k(\sqrt{b}))$.

Lemma 4.0.4. *For each $n \geq 1$, the matrix algebra $M_n(k) \cong \mathrm{End}_k(k^n)$ is a central simple algebra over k and we have $M_n(k) \otimes_k M_m(k) \cong M_{nm}(k)$.*

Proof. The center of $M_n(k)$ is k and any if I is a non-zero two-sided ideal, then it contains some non-zero $A \in I$ with coefficients a_{ij}. Then there exist indices (i,j) such that $a_{ij} \neq 0$. Let E_{ij} be the matrix whose coefficients are all 0 except for the (i,j) entry which is 1, then $a_{ij}E_{ij} = E_{ji}AE_{ij} \in I$ and so $E_{ij} \in I$. By multiplying with permutation matrices we get that $E_{ij} \in I$ for all i, j and so $I = M_n(k)$.

The second statement basically boils down to block matrix multiplication. □

[2] This assumption is only for simplicity and in [9, Chapter 4] the results are proven in the general case as well.

Theorem 4.0.5 (Wedderburn). *For any central simple algebra A over k, there exists a unique division algebra $D \supset k$ and an integer n such that*

$$A \cong M_n(D).$$

Proof. Not given, see [9, Chapter 2] for a proof. □

Corollary 4.0.6. *Let A be a central simple algebra over k, then there exists a finite field extension $k \subset L$ such that $A \otimes_k L \cong M_n(L)$. One says that L splits A. Moreover the dimension of A over k is a square.*

Proof. Note that $A \otimes \overline{k}$ is a central simple algebra over $\overline{k}$. By Wedderburn's theorem there is a finite dimensional division algebra $D \supset \overline{k}$ such that $A \otimes \overline{k} \cong M_n(D)$. Every element $x \in D$ defines a finite extension $\overline{k} \subset \overline{k}(x)$ and hence $x \in \overline{k}$ and $D = \overline{k}$. Let $\phi : A \otimes \overline{k} \to M_n(\overline{k})$ be an isomorphism. Let $e_1, \ldots, e_m$ be a k-basis of A. Note that this is a $\overline{k}$-basis of $A \otimes \overline{k} \cong M_n(\overline{k})$ and hence $m = n^2$.

Let $L \supset k$ be the field extension obtained by adjoining all the coefficients of the matrices $\phi(e_1 \otimes 1), \ldots, \phi(e_m \otimes 1)$ to k. This is a finite field extension of k and viewing $A \otimes L$ as a subring of $A \otimes \overline{k}$ we have $\phi(A \otimes L) \subset M_n(L)$. Since ϕ is injective and $\dim_L(A \otimes L) = m = n^2 = \dim_L M_n(L)$ we conclude that ϕ defines an isomorphism $A \otimes L \to M_n(L)$. □

Lemma 4.0.7. *A k-algebra A is a central simple algebra if and only if there exists a finite field extension $k \subset L$ such that L splits A.*

Proof. By the previous corollary it remains to show that if $k \subset L$ is finite field extension such that L splits A, then A is central simple over k. Suppose $I \subset A$ is a two-sided ideal, then $I \otimes L$ is a two-sided ideal of $A \otimes L$ and hence either $I \otimes L = 0$ or $I \otimes L = A \otimes L$. For dimension reasons we have $I = 0$ or $I = A$. Now suppose $z \in A$ is in the center of A, then $z \otimes 1$ central in $A \otimes L$. Hence $z \otimes 1 = 1 \otimes y$ for some $y \in L$, but this implies $z = y \in k$. □

Corollary 4.0.8. *If A, B are central simple algebras over k, then $A \otimes_k B$ is central simple over k and if L splits A and B, then it also splits $A \otimes_k B$.*

Proof. Let $k \subset L$ be a finite extension which splits both A and B, then L splits $A \otimes_k B$ because

$$A \otimes_k B \otimes_k L \cong A \otimes_k M_m(L) \cong A \otimes L \otimes M_m(k) \cong M_n(L) \otimes M_m(k) \cong M_{nm}(L),$$

for some integers $n, m \geq 1$, where we used the isomorphism from 4.0.4. Consequently $A \otimes_k B$ is a central simple algebra by 4.0.7. □

When we study the Brauer group we will apply Galois Descent to classify which algebras are split by L. To do so we need to know the automorphisms of $M_n(L)$ and from those we can also immediately find the automorphisms of any central simple algebra.

Lemma 4.0.9. *Let L be a field, then $PGL_n(L) \to \mathrm{Aut}_K(M_n(L)) : a \mapsto (x \mapsto axa^{-1})$ is an isomorphism.*

Proof. This is done in [9, Corollary 2.4.2]. □

Theorem 4.0.10 (Skolem-Noether)**.** *Let A be a central simple algebra over k, then all k-automorphisms of A are inner.*

Proof. This is [9, thm 2.7.2]. By 4.0.7 there is a finite extension $k \subset L$, which we may assume to be Galois since k is perfect, such that $A \otimes_k L \cong M_n(L)$ for some $n \geq 1$. By the lemma all L-automorphisms of $A \otimes_k L$ are inner and we have a short exact sequence

$$1 \to L^\times \to (A \otimes L)^\times \to \mathrm{Aut}_L(A \otimes_k L) \to 1.$$

Passing to (nonabelian) cohomology we obtain the exact sequence

$$k^\times \to A^\times \to \mathrm{Aut}_k(A) \to H^1(L/k, L^\times)$$

and by Hilbert's Theorem 90 we conclude that the map $A^\times \to \mathrm{Aut}_k(A)$ is surjective, i.e. every k-automorphism of A is inner. □

4.1 The Brauer Group

Now we can construct the Brauer group attached to the field k. It gives a group structure on equivalence classes of central simple algebras under a certain equivalence relation. Later we will see that it also appears as a Galois Cohomology group. It is an important invariant of the field k and satisfies a local-global principle which generalises the classical Hasse principle.

Definition 4.1.1 (Brauer Equivalence)**.** *Two central simple algebras A, B over k are called Brauer equivalent (over k) if there exist integers $n, m \geq 1$ such that*

$$A \otimes_k M_n(k) \cong B \otimes_k M_m(k).$$

Let $\mathrm{Br}(k)$ denote the set[3] *of Brauer equivalence classes of all central simple algebras.*

Using Lemma 4.0.4 it is straightforward to check that Brauer equivalence is indeed an equivalence relation on isomorphism classes of central simple algebras.

[3] This is indeed a set as every central simple algebra over k is in particular a finite dimensional vector space over k and so isomorphism classes of algebras of dimension n can be identified with functions $m : k^n \times k^n \to k^n$, satisfying the k-algebra axioms for multiplication.

Definition 4.1.2 (Opposite Ring). *Let A be a ring, then the opposite ring A^{op} consists of the same set and the same addition just multiplication is given by $x \cdot_{op} y = y \cdot x$, where $\cdot$ is the product on A.*

Theorem 4.1.3. *The set $Br(k)$ with the operation $\otimes_k$ is an abelian group, with inverse of the class of a central simple algebra A being the class of the opposite algebra A^{op}.*

Proof. The operation $\otimes_k$ is commutative and associative and by definition of Brauer equivalence the class of $M_1(k)$ is a neutral element for $\otimes_k$. Thus we need to check that $\otimes_k$ respects Brauer equivalence and that A^{op} is indeed the inverse of A. So let A, A', B, B' be central simple algebras over k and $n, m, r, s \geq 1$ such that

$$A \otimes_k M_n(k) \cong A' \otimes_k M_m(k), \quad B \otimes_k M_r(k) \cong B' \otimes_k M_s(k),$$

then by Lemma 4.0.4

$$(A \otimes_k B) \otimes_k M_{nr}(k) \cong (A' \otimes_k B') \otimes_k M_{ms}(k).$$

This shows that Brauer equivalence is compatible with the tensor product.

Now let A be a central simple algebra and consider the k-linear map given by

$$\phi : A \otimes A^{op} \to \mathrm{End}_k(A) : (a \otimes b) \mapsto (x \mapsto axb).$$

This is an algebra homomorphism since $(a \otimes b)(a' \otimes b') = (aa' \otimes b'b)$. Clearly ϕ is non-zero, as for example the image of $(1 \otimes 1)$ is the identity. Since $A \otimes A^{op}$ is simple, we conclude that $\ker(\phi) = 0$ and so ϕ is injective. For dimension reasons it is surjective. Hence $A \otimes_k A^{op} \cong \mathrm{End}_k(A) \cong M_n(k)$, where $n = \dim_k(A)$. □

Proposition 4.1.4. *Every element of* $\mathrm{Br}(k)$ *has a unique representative which is a division algebra.*

Proof. This is a consequence of Wedderburn's theorem 4.0.5. Let A be a central simple algebra and D the unique division algebra such that $A \cong M_n(D) \cong D \otimes M_n(k)$. This shows that the class of A is represented by D. Moreover if D' is another division algebra which is Brauer equivalent to A, then there are $l, m \geq 1$ such that

$$M_l(D') \cong D' \otimes M_l(k) \cong A \otimes M_m(k) \cong D \otimes M_{nm}(k) \cong M_{nm}(D)$$

and the uniqueness part of Wedderburns theorem shows that $D \cong D'$. □

The previous proposition shows that the Brauer group of k is trivial if and only if there are no non-trivial division algebras over k with center k. So this is a "closedness" condition.

Example 4.1.5. *The Brauer group of an algebraically closed field is trivial, since the only division algebra over an algebraically closed field is the field itself. In particular,* $\mathrm{Br}(\mathbb{C}) = 0$ *and* $\mathrm{Br}(\overline{\mathbb{Q}}) = 0$.

Theorem 4.1.6. *The Brauer group of a finite field is trivial.*

Proof. We will show that every central division algebra over a finite field F is trivial. This follows from the fact that every finite division algebra is commutative, so it equals its center.

The first theorem in [28] is precisely this statement. We replicate its beautiful proof presented there. Let D be a finite division algebra and let F be its center. Let $|F| = q$ and n the dimension of D over F. We wish to show that $n = 1$. For $x \in D^\times$ let $Z(x)$ denote the subfield of D consisting of the elements which commute with x and let $\delta(x)$ be its dimension over F. Then D is a vector space over $Z(x)$ and so $\delta(x)$ divides n. By the orbit-stabiliser theorem the cardinality of the conjugacy class of x in $D^\times$ is $[D^\times : Z(x)^\times]$. Let S be a set of representatives of the conjugacy classes of non-central elements, then

$$q^n - 1 = q - 1 + \sum_{x \in S} \frac{q^n - 1}{q^{\delta(x)} - 1}. \tag{2}$$

Suppose $n > 1$ and let P be the nth cyclotomic polynomial, i.e. the product $P(q) = \prod(q - \zeta)$ over all primitive nth roots of unity ζ. P is the minimal polynomial of a primitive root of unity and hence has integral coefficients. Since $\delta(x) < n$ for all $x \in S$ we conclude that the integer $P(q)$ divides all terms in the sum in (2). As $P(q)$ also divides the left side it must divide $q - 1$. This is the desired contradiction since for all nth primitive roots ζ, one has $|q - \zeta| \geq \Re(q - \zeta) > q - 1$. □

Example 4.1.7. *Later we will see that* $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$.

Next we will show that the Brauer group is isomorphic to a certain cohomology group using Galois Descent. Let L/k be a finite Galois extension, $CSA_L(n)$ the isomorphism classes of central simple algebras A such that $A \otimes L \cong M_n(L)$ and $\mathrm{Br}(L/k)$ the subgroup of $\mathrm{Br}(k)$ of classes split by L. Note that this is a subgroup thanks to 4.0.8.

Lemma 4.1.8. $CSA_L(n)$ *is in bijection with* $H^1(L/k, PGL_n(L))$.

Proof. We apply Galois descent 3.1.1 to the category of L-algebras inside the category of k-algebras. By 4.0.7 any k-algebra which becomes isomorphic to $M_n(L)$ over L is automatically a central simple algebra over k. Together with the determination of the automorphism group of $M_n(L)$ from lemma 4.0.9 this proves the result. □

Theorem 4.1.9. *Let L/k be a finite Galois extension, then there is an isomorphism*

$$\mathrm{Br}(L/k) \to H^2(L/k, L^\times)$$

and glueing these together gives an isomorphism $\mathrm{Br}(k) \cong H^2(k, \overline{k}^\times)$.

Proof Sketch. A full proof can be found in [9, Chapter 4.4]. Let $A \in CSA_L(n)$ and f the corresponding cocycle in $H^1(L/k, PGL_n(L))$. Consider the short exact sequence $1 \to L^\times \to GL_n(L) \to PGL_n(L) \to 1$. Because $L^\times$ is commutative and contained in the center of $GL_n(L)$ it turns out that there is a coboundary $\delta : H^1(L/k, PGL_n(L)) \to H^2(L/k, L^\times)$ as shown in [9, 4.4.1]. By the general form of Hilbert's Theorem 90 we have $H^1(L/k, GL_n(L)) = 0$, so δ is injective.

Now let $n = [L : k]$, then $L \otimes_L L \cong L^n$ and so there is a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & L^\times \arrow[r] \arrow[d, "\mathrm{id}"] & (L \otimes_L L)^\times \arrow[r] \arrow[d] & (L \otimes_L L)^\times / L^\times \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & L^\times \arrow[r] & GL_n(L) \arrow[r] & PGL_n(L) \arrow[r] & 1
\end{tikzcd}$$

which induces the diagram

$$\begin{tikzcd}
H^1(L/k, (L \otimes_L L)^\times / L^\times) \arrow[r, "\delta"] \arrow[d] & H^2(L/k, L^\times) \arrow[r] \arrow[d, "\mathrm{id}"] & H^2(L/k, (L \otimes_L L)^\times) \\
H^1(L/k, PGL_n(L)) \arrow[r, "\delta"] & H^2(L/k, L^\times) &
\end{tikzcd}$$

Now one can check that $(L \otimes_L L)^\times \cong \mathrm{Ind}_1^{\mathrm{Gal}(L/k)}(L^\times)$ and so by Shapiro's Lemma $H^2(L/k, (L \otimes_L L)^\times) = 0$ and δ is surjective. Thus $H^2(L/k, L^\times)$ is already in bijection with $H^1(L/k, PGL_n(L))$.[4] To conclude one can further check that the map δ is well-defined on Brauer equivalence classes and is a group homomorphism.

The second statement follows since every element in $\mathrm{Br}(k)$ is split by some finite extension L/k and $H^2(k, \overline{k}^\times)$ is the directed union of the $H^2(L/k, L^\times)$ because the inflation maps $H^2(L/k, L^\times) \to H^2(k, \overline{k}^\times)$ are injective by inflation-restriction 2.4.14. □

Corollary 4.1.10. *The only division algebras containing $\mathbb{R}$ and which are finite dimensional over $\mathbb{R}$ are $\mathbb{R}, \mathbb{C}$ and the classical quaternions.*

Proof. The only division algebra over $\mathbb{C}$ is $\mathbb{C}$ itself since $\mathbb{C}$ is algebraically closed. By 2.3.2, $H^2(\mathbb{C}/\mathbb{R}, \mathbb{C}^\times) = \mu_2$. Thus $\mathbb{R}$ and the quaternions are the division algebras with center $\mathbb{R}$. Conversely the center of any division algebra containing $\mathbb{R}$ is a field extension of $\mathbb{R}$. In order for the division algebra to be finite dimensional over $\mathbb{R}$ this needs to be a finite extension and so the center is either $\mathbb{R}$ or $\mathbb{C}$. □

[4] This shows that any central simple algebra split by L has dimension at most n^2 over k.

Corollary 4.1.11. *For any field k, the Brauer group* $\mathrm{Br}(k)$ *is a torsion group, more concretely for any central simple algebra A over k, there exists m and l such that $A^{\otimes m} \cong M_l(k)$.*

Proof. Every central simple algebra is split by some finite Galois extension and so $\mathrm{Br}(k)$ is the directed union of the $\mathrm{Br}(K/k)$ which are all torsion groups since restriction-corestriction shows that $H^2(K/k, K^\times)$ is killed by $[K : k]$. Thus $\mathrm{Br}(k)$ is a torsion group and the second statement follows from Wedderburn's Theorem since k is the unique division algebra which represents the trivial class in $\mathrm{Br}(k)$. □

Corollary 4.1.12. *The m-torsion part is given by* $\mathrm{Br}(k)[m] \cong H^2(k, \mu_m)$.

Proof. Apply Hilbert's Theorem 90 and the long exact sequence associated to

$$1 \to \mu_m \to \overline{k}^\times \xrightarrow{m} \overline{k}^\times \to 1.$$ □

Corollary 4.1.13. *Let $K \subset L$ be a cyclic Galois extension, then the norm $N : L^\times \to K^\times$ is surjective if and only if* $\mathrm{Br}(L/K) = 0$.

Proof. By 2.3.2 we have $H^2(L/K, L^\times) = K^\times/N(L^\times)$, so the result follows from the theorem. □

Definition 4.1.14. *A field k is said to satisfy property C_r if every homogeneous polynomial in n variables over k of degree d such that $n > d^r$ has a root in $\mathbb{P}^{n-1}(k)$.*

Lemma 4.1.15. *If k is C_1, then any algebraic extension K/k is C_1.*

Proof. Assume that K/k is finite. If $f(y_1, \ldots, y_n) = 0$ is a homogeneous equation over K in n variables, then $N_{K/k}(f(\sum_i x_{1i}e_i, \ldots, \sum_i x_{ni}e_i)) = 0$ is a homogeneous equation over k in $[K : k]n$ variables, where the e_i are a k-basis of K. If the degree of the first equation is $d < n$, then the degree of the second equation is $[K : k]d < [K : k]n$ and hence has a nontrivial solution. Since every homogeneous equation only involves finitely many coefficients we can in fact conclude that K is C_1 for any algebraic extension K/k. □

Corollary 4.1.16. *The Brauer group of a C_1 field is trivial.*

Proof. If k is C_1 and L/k is cyclic with k-basis $e_1, \ldots, e_n$ then $N(\sum x_i e_i) - x_0^n a$ is a homogeneous equation of degree n in $n + 1 > n$ variables and so the norm $N_{L/k}$ is surjective. Every algebraic extension of a C_1 field is also C_1, thus $\mathrm{Br}(L/K) = 0$ for every cyclic L/K cyclic with K/k algebraic. Now suppose L/k is a Galois extension of degree p^s, then using that p-groups are solvable we employ 2.4.14 and the cyclic case to show that $\mathrm{Br}(L/k) = 0$. For a general finite Galois extension L/k we can use 2.4.12 to reduce to the case of p-extensions. □

Corollary 4.1.17. *If k (not necessarily perfect) is C_1, then $cd(k) \leq 1$.*

Proof. Let p be a prime and $H < G_k$ be a pro-p sylow subgroup and k_p the fixed field of H. By 2.8.4 it will suffice to show $\mathrm{cd}_p(k_p) \leq 1$. If $p = \mathrm{char}(k)$, then from 2.4.6 and the Artin-Schreier sequence $0 \to \mathbb{F}_p \to k^s \to k^s \to 0$ we find $H^2(k_p, \mathbb{Z}/p\mathbb{Z}) = 0$ and so $cd_p(k) \leq 1$ by 2.8.5.

If $p \neq \mathrm{char}(k)$, then $k_p(\mu_p)/k_p$ is a Galois extension such that $\mathrm{Gal}(k_p(\mu_p)/k_p)$ is both a quotient of H and of order coprime to p hence $\mu_p \subset k_p$ and $H^2(k_p, \mathbb{Z}/p\mathbb{Z}) = H^2(k_p, \mu_p) = \mathrm{Br}(k_p)[p] = 0$ since k_p is C_1. Thus $\mathrm{cd}_p(k) \leq 1$ by 2.8.5. □

Example 4.1.18. *The converse of this statement is false. In fact there are fields which are not C_r for any r but have trivial Brauer group. Let p_n be an enumeration of the prime numbers. Then let $k_0 = \mathbb{C}$ and $k_n = k_{n-1}((t^{1/m}, p_n \nmid m))$. We set $k = \bigcup k_i$. One can show that $G_k = \hat{\mathbb{Z}}$ and so $cd(k) = 1$. But in [2] it is shown that this field is not C_r for any r.*

However in general it is a conjecture [21, II. 4.5] that k having property C_r implies $\mathrm{cd}(k) \leq r$. The case $r = 2$ is established and for $r > 2$ we know [12, Theorem 1.15] at least that $\mathrm{cd}_p(k) \leq \lceil (r-2)\log_2(p) + 1 \rceil$.

5 Local Class Field Theory

One of the main motivations for the development of group cohomology was to find a good formulation of the theorems of class field theory. In this section we develop the class field theory of local fields with finite residue field as in [5], [16] and [20].

Throughout K will be a field, complete with respect to a discrete valuation and finite residue field k and $\overline{K}$ will denote its separable closure. Interesting examples are finite extensions of $\mathbb{Q}_p$ and Laurent series $k((t))$ for a finite field k. From a modern point of view local class field theory is the study of the cohomology of the $\mathrm{Gal}(L/K)$-module $L^\times$ for all finite Galois extensions L/K. For example we can compute the Brauer group of a field and by Tate's theorem this will give rise to isomorphisms $K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(L/K)^{ab}$ for every Galois extension L/K. In particular this helps us understand the abelian extensions of a local field. A famous consequence is the local Kronecker-Weber theorem, i.e. that every finite abelian extension of $\mathbb{Q}_p$ is contained in a cyclotomic extension $\mathbb{Q}_p(\zeta_m)$ for some m.

5.1 The Cohomology of a Local Field

Recall the correspondence between separable extensions of the residue field k and separable, unramified extensions of K [5, Chapter I. 7.]. It will be used frequently in the following section.

Lemma 5.1.1. *Let G be a finite group and let M be a compact topological $\mathbb{Z}[G]$-module with a decreasing filtration of closed submodules $M = M^0 \supset M^1 \supset \dots$ such that $\bigcap M^i = \{0\}$ and $H^q(G, M^i/M^{i+1}) = 0$ for all $i \geq 0$, then $H^q(G, M) = 0$.*

Proof. From the short exact sequences

$$1 \to M^{n-1}/M^n \to M^0/M^n \to M^0/M^{n-1} \to 1,$$

we deduce that $H^q(G, M^0/M^n) \cong H^q(G, M^0/M^{n-1}) \cong \dots \cong H^q(G, M^0/M^1) = 0$. The conditions on the filtration show that the canonical map

$$M \to \lim_{\leftarrow} M/M^n$$

is injective and has compact and dense image. Hence it is an isomorphism of $\mathbb{Z}[G]$-modules. Moreover for any finite d, the sets of the form $(M^n)^d$ form a base of the topology of M. Since G is finite we can apply this to get canonical isomorphisms

$$C^q(G, M) \cong M^{|G|^q} \cong \left(\lim_{\leftarrow} M/M^n\right)^{|G|^q} \cong \lim_{\leftarrow}(M/M^n)^{|G|^q} \cong \lim_{\leftarrow} C^q(G, M/M^n)$$

which induce an isomorphism $H^q(G, M) \cong \lim_{\leftarrow} H^q(G, M/M^n) = 0$. □

Lemma 5.1.2. *For every finite unramified Galois extension $K \subset L$ with group G we have*

$$H^q(G, U_L) = 0$$

for all $q \geq 1$, where $U_L = \{x \in L^\times : v_L(x) = 0\}$ is the group of units of L.

Proof. G is isomorphic to the Galois group of an extension of finite fields and hence cyclic. It suffices to show $H^1(G, U_L) = 0$ and $H^2(G, U_L) = 0$. The first of these follows from Hilbert's Theorem 90 since there is a G-isomorphism $L^\times \cong \mathbb{Z} \oplus U_L$ because L/K is unramified, so $0 = H^1(G, L^\times) \cong H^1(G, \mathbb{Z}) \oplus H^1(G, U_L)$.

Let π be a uniformiser of K, then π is also a uniformiser of L since the extension is unramified. Let $U^n = 1 + \pi^n \mathcal{O}_L$ for $n \geq 1$ and $U^0 = U_L$. G naturally acts on U^n for all $n \geq 0$. We have G-module isomorphisms $U^n/U^{n+1} \cong k_L^+$ for $n \geq 1$ and $U^0/U^1 \cong k_L^\times$, where k_L is the residue field of L. Now theorem 2.4.6 implies that $H^q(G, U^n/U^{n+1}) = 0$ for all $q \geq 1$, since G is isomorphic to $\mathrm{Gal}(k_L/k)$. By Hilbert's Theorem 90 we have $H^1(G, U^0/U^1) = 0$. Since the Brauer group of a finite field is trivial we also have $H^2(G, U^0/U^1) = 0$. (Alternatively since the Herbrand quotient of a finite module is trivial by 2.3.8.) Now Lemma 5.1.1 shows $H^2(G, U_L) = 0$, as required. □

Corollary 5.1.3. *For a finite unramified Galois extension $K \subset L$, there is an isomorphism $H^2(L/K, L^\times) \cong H^2(L/K, \mathbb{Z})$.*

Lemma 5.1.4. *For a finite unramified extension $K \subset L$, we have $H^2(G, L^\times) \cong \operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong \mathbb{Z}/[L : K]\mathbb{Z}$.*

Proof. Consider the short exact sequence of trivial G-modules

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

As L/K corresponds to a separable extension of k, G is cyclic and by looking at the resolution 2.3.2 we immediately find that the cohomology of $\mathbb{Q}$ is trivial and so

$$\operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong H^2(G, \mathbb{Z}) \cong H^2(G, L^\times).$$

Since G is cyclic we get an isomorphism $\operatorname{Hom}(G, \mathbb{Q}/\mathbb{Z}) = \mathbb{Z}/[L : K]\mathbb{Z}$. □

In the sequel we write $H^q(L/K)$ for $H^q(L/K, L^\times)$ and we denote the above isomorphism by $\alpha_{L/K} : H^2(L/K) \to G^\vee$, where $G^\vee := \operatorname{Hom}_{cts}(G, \mathbb{Q}/\mathbb{Z})$.

Lemma 5.1.5. *Let $K \subset L \subset E$ be finite unramified Galois extensions, then the diagram*

$$\begin{tikzcd}
H^2(L/K) \arrow[r, "\operatorname{Inf}_{E/L}"] \arrow[d, "\alpha_{L/K}"] & H^2(E/K) \arrow[d, "\alpha_{E/K}"] \\
\operatorname{Gal}(L/K)^\vee \arrow[r] & \operatorname{Gal}(E/K)^\vee
\end{tikzcd}$$

commutes, where the bottom map is induced by the restriction of automorphisms to the subfield L.

Proof. Let us describe the map $\alpha_{L/K}^{-1}$ more explicitly. Given $\chi \in \operatorname{Gal}(L/K)^\vee$, choose $f : \operatorname{Gal}(L/K) \to \mathbb{Q}$ such that $\chi \equiv f \pmod{\mathbb{Z}}$. Then

$$\left(\alpha_{L/K}^{-1}\chi\right)(\sigma, \tau) = \pi^{f(\sigma)+f(\tau)-f(\sigma\tau)}.$$

Using this for the extensions L/K and E/K and remembering the definition of the map $\operatorname{Inf}_{E/L}$ we find

$$\left(\operatorname{Inf}_{E/L} \circ \alpha_{L/K}^{-1}\chi\right)(\sigma, \tau) = \left(\alpha_{L/K}^{-1}\chi\right)(\sigma|_L, \tau|_L).$$

Now the key observation is that if f lifts $\chi : \operatorname{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ to $\mathbb{Q}$, then $\sigma \mapsto f(\sigma|_L)$ lifts $\chi_E : \operatorname{Gal}(E/K) \to \mathbb{Q}/\mathbb{Z} : \sigma \mapsto \chi(\sigma|_L)$. This shows that

$$\left(\alpha_{E/K}^{-1}\chi_L\right)(\sigma, \tau) = \left(\alpha_{L/K}^{-1}\chi\right)(\sigma|_L, \tau|_L)$$

as required. □

Given unramified extensions L_α/K, the field extension generated by all the L_α is again unramified. Thus the union of all separable, unramified extensions is the maximal separable, unramified extension denoted by K^{un}. The previous lemmas combined together with 2.6.15 show that we have a unique isomorphism

$$H^2(K^{un}/K) \xrightarrow{\alpha_K} \mathrm{Gal}(K^{un}/K)^\vee$$

such that for all finite unramified Galois extensions $K \subset L$, the diagram

$$\begin{tikzcd}
H^2(L/K) \arrow[r, "\mathrm{Inf}_{K^{un}/L}"] \arrow[d, "\alpha_{L/K}"] & H^2(K^{un}/K) \arrow[d, "\alpha_K"] \\
\mathrm{Gal}(L/K)^\vee \arrow[r] & \mathrm{Gal}(K^{un}/K)^\vee
\end{tikzcd}$$

commutes. Further there is an isomorphism $\mathrm{Gal}(K^{un}/K) \cong \mathrm{Gal}(\overline{k}/k) \cong \hat{\mathbb{Z}}$. One can make this explicit by letting $q = |k|$, choosing the automorphism $\mathrm{Frob}_q : K^{un} \to K^{un}$ such that $\mathrm{Frob}_q(a) \equiv a^q \pmod{\pi}$ and sending this to $1 \in \hat{\mathbb{Z}}$. Then we see that $\mathrm{Gal}(K^{un}/K)^\vee \to \mathbb{Q}/\mathbb{Z} : \chi \mapsto \chi(\mathrm{Frob}_q)$ is an isomorphism. The composite of α_K with this isomorphism is called the invariant map and denoted by inv_K. For an unramified Galois extension $K \subset L$ one defines $\mathrm{inv}_{L/K}$ as $\mathrm{inv}_K \circ \mathrm{Inf}_L^{K^{un}}$.

We now turn to ramified extensions. The goal is to show that in fact already $H^2(K^{un}/K) = H^2(\overline{K}/K)$ which implies $H^2(\overline{K}/K) \cong \mathbb{Q}/\mathbb{Z}$.

Lemma 5.1.6. *Let $K \subset L$ be a finite Galois extension. Then $H^2(L/K)$ contains a cyclic subgroup of order $n = [L : K]$.*

Proof. Let e be the ramification index and f the degree of the residue field extension. Then we have commutative diagrams

$$\begin{tikzcd}
L^\times \arrow[r, "v_L"] & \mathbb{Z} \\
K^\times \arrow[r, "v_K"] \arrow[u] & \mathbb{Z} \arrow[u, "e"']
\end{tikzcd}
\qquad
\begin{tikzcd}
G_L^\vee \arrow[r, "\chi \mapsto \chi(\mathrm{Frob}_L)"] & \mathbb{Q}/\mathbb{Z} \\
G_K^\vee \arrow[r, "\chi \mapsto \chi(\mathrm{Frob}_K)"] \arrow[u] & \mathbb{Q}/\mathbb{Z} \arrow[u, "f"']
\end{tikzcd}$$

We will use that $L^{un} = LK^{un}$ which follows from the fact that the residue fields of L and K have the same algebraic closure. This implies that the map $\mathrm{Gal}(L^{un}/L) \to \mathrm{Gal}(K^{un}/K) : \sigma \mapsto \sigma|_{K^{un}}$ is injective and as a result induces a restriction map $\mathrm{Res} : H^q(K^{un}/K) \to H^q(L^{un}/L)$. Consider the diagram

$$\begin{tikzcd}
H^2(L^{un}/L) \arrow[r, "v_L"] & H^2(\mathrm{Gal}(L^{un}/L), \mathbb{Z}) \arrow[r, "\sim"] & \mathrm{Gal}(L^{un}/L)^\vee \arrow[r, "\chi \mapsto \chi(\mathrm{Frob}_L)"] & \mathbb{Q}/\mathbb{Z} \\
H^2(K^{un}/K) \arrow[r, "v_K"] \arrow[u, "\mathrm{Res}"] & H^2(\mathrm{Gal}(K^{un}/K), \mathbb{Z}) \arrow[r, "\sim"] \arrow[u, "e \cdot \mathrm{Res}"] & \mathrm{Gal}(K^{un}/K)^\vee \arrow[r, "\chi \mapsto \chi(\mathrm{Frob}_K)"] \arrow[u, "e \cdot \mathrm{Res}"] & \mathbb{Q}/\mathbb{Z} \arrow[u, "ef"]
\end{tikzcd}$$

The rows compose to inv_L and inv_K and $n = ef$. Finally we obtain the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & H^2(L/K) \arrow[r] & H^2(\overline{K}/K) \arrow[r, "\mathrm{Res}"] & H^2(\overline{L}/L) \\
0 \arrow[r] & \ker(\mathrm{Res}) \arrow[r] \arrow[u, "\iota"] & H^2(K^{un}/K) \arrow[r, "\mathrm{Res}"] \arrow[u, "\mathrm{Inf}"] & H^2(L^{un}/L) \arrow[u, "\mathrm{Inf}"] \\
0 \arrow[r] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[r] \arrow[u] & \mathbb{Q}/\mathbb{Z} \arrow[r, "n"] \arrow[u, "\mathrm{inv}_K^{-1}"] & \mathbb{Q}/\mathbb{Z} \arrow[u, "\mathrm{inv}_L^{-1}"]
\end{tikzcd}$$

with exact rows. Since inv_K and inv_L are isomorphisms, we see that $\ker(\mathrm{Res}) \cong \mathbb{Z}/n\mathbb{Z}$. Further ι is injective since Inf is injective by 2.4.14 and Hilbert 90. □

Lemma 5.1.7. *If $K \subset L$ is a finite Galois extension with group G, then there exists an open subgroup $V \subset U_L$ such that $H^q(G, V) = 0$ for all $q \geq 1$.*

Proof. We follow the approach taken in [5, Chapter 6, 1.4]. The idea is to use the additive group of L which already known to be free over $\mathbb{Z}[G]$ by the normal basis theorem. Let $\alpha \in L$ such that $\{\sigma(\alpha)\}_{\sigma\in G}$ is a basis of L over K. By multiplying α with a high power of a uniformiser π_K of K we may assume that $\sigma(\alpha) \in \mathcal{O}_L$ for all $\sigma \in G$. Now let $M = \sum_{\sigma\in G} \sigma(\alpha)\mathcal{O}_L$. M is an open subgroup of $\mathcal{O}_L$ so there is $N \geq 1$ such that $\pi_K^N \mathcal{O}_L \subset M$. Let $V = 1 + \pi_K^N M$, then V is a subgroup of U_L since for $x, y \in M$ one has

$$(1+\pi_K^N x)(1+\pi_K^N y) = 1+(x+y)\pi_K^N + xy\pi_K^{2N} \in 1+\pi_K^N M + \pi_K^{2N}\mathcal{O}_L \subset 1+\pi_K^N M + \pi_K^N M$$

further V is open since it contains $1 + \pi_K^{2N}\mathcal{O}_L$. Note that V is a closed subset of the compact group U_L and $V^i = 1 + \pi_K^{N+i} M$ is a decreasing filtration of V by closed $\mathbb{Z}[G]$-submodules. By Lemma 5.1.1 it suffices to show that $H^q(G, V^i/V^{i+1}) = 0$ for all i. There is an isomorphism of $\mathbb{Z}[G]$-modules $V^i/V^{i+1} \to M/\pi_K M : 1 + \pi_K x \mapsto \overline{x}$ and $M/\pi_K M \cong \mathrm{Ind}_1^G(\mathcal{O}_L/\pi_K\mathcal{O}_L)$. Thus by Shapiro's lemma $H^q(G, V^i/V^{i+1}) = 0$, as required. □

Lemma 5.1.8. *Let $K \subset L$ be a cyclic Galois extension of degree n, then $H^2(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ and $H^2(L/K)$ is contained in the image of* $\mathrm{Inf} : H^2(K^{un}/K) \to H^2(\overline{K}/K)$.

Proof. Let $V \subset U_L$ be a subgroup as in Lemma 5.1.7, then $h(U_L) = h(V)h(U_L/V) = 1$, since V has trivial cohomology and U_L/V is finite. Now even though the extension might be ramified we still have $L^\times/U_L \cong \mathbb{Z}$ and so $h(L^\times) = h(U_L)h(\mathbb{Z}) = h(\mathbb{Z})$. But $H^2(G, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$ and $H^1(G, \mathbb{Z}) = 0$ by 2.3.3, hence $h(L^\times) = n$. Hilbert's Theorem 90 implies that $n = h(L^\times) = |H^2(L/K)|$ and Lemma 5.1.6 completes the proof. □

Lemma 5.1.9. *Let $K \subset L$ be a finite Galois extension of degree n, then $H^2(L/K) \cong \mathbb{Z}/n\mathbb{Z}$ and $H^2(L/K)$ is contained in the image of* $\mathrm{Inf} : H^2(K^{un}/K) \to H^2(\overline{K}/K)$.

Proof. We already know that $H^2(L/K)$ contains a cyclic subgroup of order n. Thus it suffices to show $|H^2(L/K)| \leq [L : K]$. Let p be a prime dividing n and G_p a p-sylow subgroup of $G = \mathrm{Gal}(L/K)$, then $H^2(G, L^\times) \to H^2(G_p, L^\times)$ is injective on p-primary components. Hence it suffices to show the lemma in the case that G is a p-group.

So assume that G is a p-group. For $|G| = p$ the claim has already been proven. Now assume the claim holds for p-groups of order p^d and let $|G| = p^{d+1}$. Let $H < G$ be a normal subgroup such that G/H is cyclic of order p. Then we have the inflation restriction sequence

$$0 \to H^2(L^H/K) \to H^2(L/K) \to H^2(L/L^H)$$

and so $|H^2(L/K)| \leq |H^2(L^H/K)||H^2(L/L^H)| \leq p \cdot p^d = p^{d+1}$ by the inductive hypothesis and the cyclic case. □

Theorem 5.1.10. $H^2(\overline{K}/K) \cong H^2(K^{un}/K) \cong \mathbb{Q}/\mathbb{Z}$.

Proof. $H^2(\overline{K}/K)$ is the directed union of the $H^2(L/K)$, for L a finite Galois extension. As we have seen, these are all contained in the image of $\mathrm{Inf} : H^2(K^{un}/K) \to H^2(\overline{K}/K)$, hence Inf is an isomorphism. □

This shows for example that every central simple algebra over K is split by an unramified extension of K. Furthermore, the isomorphism $H^2(\overline{K}/K) \cong \mathbb{Q}/\mathbb{Z}$ allows us to apply Tate's theorem in the next section.

5.2 Abelian Extensions

We begin this section with a general theorem due to Tate about finite group cohomology whose proof we shall omit. This is also one of the few places where we need the Tate cohomology groups.

Definition 5.2.1. *Let G be a finite group and A a $\mathbb{Z}[G]$-module. For $q \in \mathbb{Z}$ define the Tate cohomology groups as*

$$\hat{H}^q(G, A) = \begin{cases} H^q(G, A) & q \geq 1 \\ A^G/NA & q = 0 \\ \ker N/\langle a - ga : a \in A, g \in G\rangle & q = -1 \\ H_{-q-1}(G, A) & q \leq -2 \end{cases}$$

The Tate cohomology groups form a 'cohomological functor' in the sense that given a short exact sequence of $\mathbb{Z}[G]$-modules $0 \to A \to B \to C \to 0$ we get a (very) long exact sequence

$$\cdots \to \hat{H}^{i-1}(G, C) \to \hat{H}^i(G, A) \to \hat{H}^i(G, B) \to \hat{H}^i(G, C) \to \hat{H}^{i+1}(G, A) \to \dots$$

This sequence comes from glueing together homology and cohomology by applying the snake lemma to the diagram

$$\begin{tikzcd}
\dots \arrow[r] & H_1(G,C) \arrow[r] & A_G \arrow[r] \arrow[d, "N"] & B_G \arrow[r] \arrow[d, "N"] & C_G \arrow[r] \arrow[d, "N"] & 0 & \\
 & 0 \arrow[r] & A^G \arrow[r] & B^G \arrow[r] & C^G \arrow[r] & H^1(G,A) \arrow[r] & \dots
\end{tikzcd}$$

In addition, the cup product on group cohomology extends to a cup product on Tate Cohomology $\hat{H}^p(G,A) \times \hat{H}^q(G,B) \overset{\cup}{\to} \hat{H}^{p+q}(G, A \otimes B)$ and now we can state Tate's theorem [16, II.3.11].

Theorem 5.2.2 (Tate)**.** *Let G be a finite group and C a $\mathbb{Z}[G]$-module such that for all subgroups $H < G$ we have $H^1(H,C) = 0$ and $H^2(H,C)$ is cyclic of order $|H|$, then for all r the map $\hat{H}^r(G,\mathbb{Z}) \to \hat{H}^{r+2}(G,C)$ given by the cup product with a generator of $H^2(G,C)$ is an isomorphism.*

This applies to class field theory in the following situation: If L/K is a finite Galois extension of local fields, then we proved that $G = \mathrm{Gal}(L/K)$ and $C = L^\times$ satisfy the conditions of the theorem. For $r = 1$, we get an isomorphism $H^1(G,\mathbb{Z}) \to H^3(G,L^\times)$ and so we deduce $H^3(G,L^\times) = 0$ since $H^1(G,\mathbb{Z}) = 0$ for any finite group G and passing to the limit, $H^3(K,\overline{K}^\times) = 0$.

More importantly, the isomorphism $\hat{H}^{-2}(G,\mathbb{Z}) \to \hat{H}^0(G,L^\times) = K^\times/N(L^\times)$ will play a significant role. By definition, $\hat{H}^{-2}(G,\mathbb{Z}) = H_1(G,\mathbb{Z})$. This homology group has another interpretation as shown in the following lemma.

Lemma 5.2.3. *Let G be a finite group, then $H_1(G,\mathbb{Z}) \cong G^{ab}$.*

Proof. Consider the exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, where the right hand maps $g \mapsto 1$ for all $g \in G$ and I_G is its kernel. Since $\mathbb{Z}[G]$ is free, it has trivial homology and so we have an exact sequence $0 \to H_1(G,\mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G \to \mathbb{Z} \to 0$. The map $\mathbb{Z}[G]/I_G \to \mathbb{Z}$ is an isomorphism and so $H_1(G,\mathbb{Z}) \to I_G/I_G^2$ is an isomorphism, too. Let $f : G^{ab} \to I_G/I_G^2 : g \mapsto g-1$, then $f(gh) = gh - 1 = (g-1)(h-1) + (g-1) + (h-1) = f(g) + f(h)$ so this is a homomorphism. It is surjective since I_G/I_G^2 is generated by elements of the form $gh - h$ with $g, h \in G$. But $gh - h - g + 1 = (g-1)(h-1) = 0 \pmod{I_G^2}$ and so $gh - h = g - 1 = f(g)$ is in the image of f. To show injectivity, let C be a cyclic group of order m, then $I_C/I_C^2 \cong (x-1)\mathbb{Z}[x]/(x^m - 1, (x-1)^2) \cong \mathbb{Z}[x]/(x^{m+1} + x^{m-2} + \dots + 1, x-1) \cong \mathbb{Z}/m\mathbb{Z}$ and so $f : C \to I_C/I_C^2$ is also injective in this case. If C is a cyclic quotient of G, then we have a commutative diagram

$$\begin{tikzcd}
G \arrow[r] \arrow[d, "f"] & C \arrow[d] \\
I_G/I_G^2 \arrow[r] & I_C/I_C^2
\end{tikzcd}$$

where the right downward arrow is an isomorphism. Hence if $g \in \ker(f)$, then $g \in \ker \chi$ for all characters $\chi : G \to \mathbb{Q}/\mathbb{Z}$. Consequently $\ker(f) < G^{ab}$ is trivial. □

By Tate's theorem there is an isomorphism $\phi_{L/K} : K^\times/N(L^\times) \to G^{ab}$ which is called the local Artin map. But since we didn't define the cup product on Tate cohomology we state another result which allows us to reason about the local Artin map in terms of usual group cohomology.

Lemma 5.2.4. *Let G be the Galois group of a finite Galois extension of local fields L/K. Let $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ be a character, then $\chi(\phi_{L/K}(a)) = \mathrm{inv}_K(a \cup \delta\chi)$ for all $a \in K^\times$, where $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ is the coboundary associated to $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.*

Proof. This is done in [19, Theorem 3.1.6]. □

This allows us to avoid Tate Cohomology in most places. However, it should be noted that many results on group cohomology extend to Tate Cohomology. The main tool for establishing these is dimension shifting because it turns out that $\hat{H}^q(G, \mathrm{Ind}_1^G(A))$ vanishes for all q. When G is finite, then $\mathrm{Ind}_1^G A \cong \mathbb{Z}[G] \otimes_{\mathbb{Z}} A$ and there is a canonical surjection $\mathbb{Z}[G] \otimes A \to A : g \otimes a \mapsto ga$. Let A' be the kernel of this map, then the long exact sequence furnishes isomorphisms $\hat{H}^{q-1}(G, A) \cong \hat{H}^q(G, A')$ which allow us to lower indices. For example the corestriction-restriction lemma 2.4.11 still holds in Tate Cohomology. For the properties of Tate Cohomology see [20, Chapter VIII] or [19]. Returning to class field theory, here is a first important application of the lemma.

Lemma 5.2.5. *If $K \subset E \subset L$ are finite field extensions of a local field K with L/K and E/K Galois, then*

$$\begin{tikzcd}
K^\times \arrow[r, "\phi_{L/K}"] \arrow[d, "\mathrm{id}"] & \mathrm{Gal}(L/K)^{ab} \arrow[d] \\
K^\times \arrow[r, "\phi_{E/K}"] & \mathrm{Gal}(E/K)^{ab}
\end{tikzcd}$$

commutes, where the right arrow is restriction of an automorphism to E.

Proof. Let χ be any character of $\mathrm{Gal}(E/K)$ and χ' its pull-back to $\mathrm{Gal}(L/K)$, then by 5.2.4 it suffices to show that $\mathrm{inv}_K(a \cup \delta\chi) = \mathrm{inv}_K(a \cup \delta\chi')$ for any $a \in K^\times$. By definition $a = \mathrm{Inf}_E^L(a)$ and $\chi' = \mathrm{Inf}_E^L(\chi)$ and since inflation is induced by chain maps everything is compatible and $\mathrm{inv}_K(a \cup \delta\chi') = \mathrm{inv}_K(\mathrm{Inf}(a \cup \delta\chi)) = \mathrm{inv}_K(a \cup \delta\chi)$ as required. □

Consequently the $\phi_{L/K}$ glue together to a unique map $\phi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$. Moreover if L/K is unramified, then $\phi_{L/K}(a) = \mathrm{Frob}^{v(a)}$. To see this recall that $\mathrm{inv}_{L/K}$ is given by

$$H^2(L/K, L^\times) \overset{v}{\to} H^2(L/K, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(L/K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\chi \mapsto \chi(\mathrm{Frob})} \mathbb{Q}/\mathbb{Z}.$$

Thus for any $a \in K^\times$ and character χ of $\mathrm{Gal}(L/K)$ we have

$$\chi(\phi_{L/K}(a)) = (\delta^{-1}(v(a)\delta\chi))(\mathrm{Frob}) = v(a)\chi(\mathrm{Frob}) = \chi(\mathrm{Frob}^{v(a)}).$$

Example 5.2.6. *Let p be an odd prime and $a \in \mathbb{Z}$ square-free, coprime to p. By Hensel's lemma a is a square in $\mathbb{Q}_p$ if and only if a is a square mod p and if we identify* $\mathrm{Gal}(\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p)$ *with a subgroup of* $\{\pm 1\}$*, then*

$$\phi_{\mathbb{Q}_p(\sqrt{a})/\mathbb{Q}_p}(x) = \left(\frac{a}{p}\right)^{v_p(x)}.$$

Moreover, if L/K is abelian, then $\phi_{L/K} : K^\times/N_{L/K}(L^\times) \to \mathrm{Gal}(L/K)$ is an isomorphism, so ϕ_K extends to an isomorphism $\phi_K : \widehat{K^\times} \to \mathrm{Gal}(K^{ab}/K)$, where $\widehat{K^\times} = \lim_{\leftarrow} K^\times/N_{L/K}(L^\times)$. This is the completion of $K^\times$ with respect to the 'norm topology' which has as a basis of open sets the cosets of the subgroups of $K^\times$ of the form $N_{L/K}(L^\times)$ for some finite abelian extension L/K. Such subgroups are called norm subgroups of $K^\times$.

One can show that the canonical isomorphism $K^\times \to U_K \times \mathbb{Z}$ induces an isomorphism $\widehat{K^\times} \cong U_K \times \hat{\mathbb{Z}}$ and so in a sense we have determined all abelian extensions of K. This can be made way more explicit by Lubin-Tate theory [16], but in the global case no such thing is known.

We will prove the isomorphism $\widehat{K^\times} \cong U_K \times \hat{\mathbb{Z}}$ at the end of this section but first we shall derive a famous consequence in the case $K = \mathbb{Q}_p$. We have an isomorphism $\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times \times \hat{\mathbb{Z}}$ such that the projection $\mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{Q}_p^{un}/\mathbb{Q}_p)$ corresponds to the projection to the $\hat{\mathbb{Z}}$ factor as $\phi_{K^{un}/K}(a) = \mathrm{Frob}^{v(a)}$. From this we can get

Theorem 5.2.7 (Local Kronecker-Weber Theorem)**.** *The maximal abelian extension of $\mathbb{Q}_p$ is the extension obtained by adjoining all the roots of unity, i.e. $\mathbb{Q}_p^{ab} = \bigcup_{m \geq 1} \mathbb{Q}_p(\zeta_m)$.*

Proof. We have already seen that the $\hat{\mathbb{Z}}$ factor comes from the unramified extensions of $\mathbb{Q}_p$. By Galois Theory there is an abelian extension $L/\mathbb{Q}_p$ such that $L \cap \mathbb{Q}_p^{un} = \mathbb{Q}_p$ and $L\mathbb{Q}_p^{un} = \mathbb{Q}_p^{ab}$ and $\mathrm{Gal}(L/\mathbb{Q}_p) \cong \mathbb{Z}_p^\times$.

Since $\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_p(\zeta_{p^n-1}) = \bigcup_{m \nmid p} \mathbb{F}_p(\zeta_m)$ we have $\mathbb{Q}_p^{un} = \bigcup_{m \nmid p} \mathbb{Q}_p(\zeta_m)$. It remains to show that L can be obtained from $\mathbb{Q}_p$ by adjoining some roots of unity. The extensions $\mathbb{Q}_p(\zeta_{p^n})$ are abelian and totally ramified, so $\mathbb{Q}_p(\zeta_{p^n}) \cap \mathbb{Q}_p^{un} = \mathbb{Q}_p$ and $\mathbb{Q}_p(\zeta_{p^n}) \subset L$. On the other hand the Galois group of $L' = \bigcup_{n \geq 1} \mathbb{Q}_p(\zeta_{p^n})$ over $\mathbb{Q}_p$ is $\mathbb{Z}_p^\times$. So $\mathrm{Gal}(L/\mathbb{Q}_p) \to \mathrm{Gal}(L'/\mathbb{Q}_p)$ is a continuous surjective map $\mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$. Thus it suffices to show that any such map is also injective. We complete this in the next lemma. □

Lemma 5.2.8. *Any continuous surjective group homomorphism $f : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times$ is injective.*

Proof. For any odd prime p we have $\mathbb{F}_p^\times \times \mathbb{Z}_p \cong \mathbb{Z}_p^\times$ via the exponential map. For $p = 2$, we have $\{\pm 1\} \times \mathbb{Z}_2 \cong \mathbb{Z}_2^\times$. Since any non-zero, closed subgroup of $\mathbb{Z}_p$ has finite index (by taking limits one shows that a closed subgroup of $\mathbb{Z}_p$ is a $\mathbb{Z}_p$-module) and the image of f is infinite, we conclude that $\ker f$ is contained in the finite factor. But then f defines an isomorphism $G \times \mathbb{Z}_p \to H \times \mathbb{Z}_p$ for some finite groups G, H such that $|H| < |G|$. This is a contradiction since f would have to map the torsion subgroup G onto H isomorphically. □

Now we can even deduce the classical Kronecker-Weber theorem from the local version as shown in [23].

Theorem 5.2.9 (Kronecker-Weber Theorem)**.** *Any finite abelian extension $K/\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_m)$ for some integer m.*

Proof. Let $p \in \mathbb{Z}$ be a prime which ramifies in K and $\mathfrak{p}$ a prime of K above p. Then $K_\mathfrak{p}/\mathbb{Q}_p$ is an abelian extension and so there exists an m_p such that $K_\mathfrak{p} \subset \mathbb{Q}_p(\zeta_{m_p})$. Set $m = \prod_{p|\Delta_K} p^{v_p(m_p)}$ then we will show $L := K(\zeta_m) = \mathbb{Q}(\zeta_m)$. $L = K\mathbb{Q}(\zeta_m)$ is an abelian extension of $\mathbb{Q}$. Let $\mathfrak{q}$ be a prime of L lying over a prime $p \mid m$ then $L_\mathfrak{q}/\mathbb{Q}_p$ is an abelian extension and we let $F/\mathbb{Q}_p$ be its maximal unramified subextension. Whenever $p \nmid k$, then $\mathbb{Q}_p(\zeta_k)/\mathbb{Q}_p$ is unramified so $L_\mathfrak{q} = F(\zeta_{p^e})$, where $e = v_p(m)$. Moreover $\mathbb{Q}_p(\zeta_{p^e}) \cap F = \mathbb{Q}_p$ since $F/\mathbb{Q}_p$ is unramified. As a result $\mathrm{Gal}(L_\mathfrak{q}/F) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^e})/\mathbb{Q}_p) \cong (\mathbb{Z}/p^e\mathbb{Z})^\times$. But $\mathrm{Gal}(L_\mathfrak{q}/F)$ is isomorphic to the inertia group $I_p \subset \mathrm{Gal}(L/\mathbb{Q})$. Now consider the group I generated by all the inertia groups I_p for $p \mid m$, then the extension $L^I/\mathbb{Q}$ is unramified and so $L^I = \mathbb{Q}$ by Minkowski's theorem. Finally $|I| \leq \prod_{p|m} |I_p| \leq \phi(m)$, hence $[L : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$ which implies $L = \mathbb{Q}(\zeta_m)$ as required. □

Definition 5.2.10. *Suppose $\mu_m \subset K$ and let $a, b \in K^\times/(K^\times)^m \cong H^1(K, \mu_m)$, then we define the (mth power) Hilbert symbol $(a, b)_{K,m}$ as the pairing*

$$H^1(K, \mu_m) \times H^1(K, \mu_m) \xrightarrow{\cup} H^2(K, \mu_m \otimes \mu_m) \cong \mathrm{Br}(K)[m] \cong \mu_m.$$

When K and m are clear from the context we will omit them from the notation.

Remark 5.2.11. *There is a canonical isomorphism $H^2(K, \mu_m \otimes \mu_m) \cong H^2(K, \mu_m) \otimes \mu_m$ given by the cup product. Together with the invariant map we get a canonical isomorphism $H^2(K, \mu_m \otimes \mu_m) \cong \mu_m$.*

Proposition 5.2.12. *The Hilbert symbol is a non-degenerate pairing and $(a, b)_{K,m} = 1$ if and only if a is a norm from $K(b^{1/m})$.*

Proof. Let $b \in K^\times$ and suppose that $(a, b)_{K,m} = 1$ for all $a \in K^\times$, then $\delta a \cup \delta b = 0$ for all $a \in K^\times$, where δ is the coboundary associated to the Kummer sequence. We apply lemma 2.5.10 to the sequences $0 \to \mathbb{Z} \xrightarrow{m} \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \to 0$ and $0 \to \mu_m \to \overline{K}^\times \xrightarrow{m} \overline{K}^\times \to 0$ with the pairing $\mathbb{Z} \times \overline{K}^\times \to \overline{K}^\times : (m, x) \mapsto x^m$.

Now we have $0 = \delta a \cup \delta b = a \cup \delta^2 b$ and so $\chi_b(\phi_K(a)) = 0$ by 5.2.4, where $\chi_b = \delta b$ is the Kummer character of b. ϕ_K hits every continuous finite quotient and so it hits every coset of every open subgroup. Thus the image of ϕ_K is dense in $\mathrm{Gal}(K^{ab}/K)$ and consequently $\chi_b = 0$ and b is an nth power.

On the other hand if $L = K(b^{1/m})$ has degree m over K, then χ_b induces an isomorphism $\mathrm{Gal}(L/K) \to \mathbb{Z}/m\mathbb{Z}$, thus $\chi_b(\phi_{L/K}(a)) = 0$ if and only if $a \in N_{L/K}(L)$. If the degree of L/K is less than m, then we can use a Hilbert symbol with small enough m to deduce the claim in the same way. □

Theorem 5.2.13 (Existence Theorem)**.** *All open finite index subgroups of $K^\times$ are norm subgroups and $\widehat{K^\times} \cong U_K \times \hat{\mathbb{Z}}$.*

Proof. This is basically the method of proof from [16] but we avoid the use of the norm limitation theorem. First let $N = N_{L/K}(L^\times) < K^\times$ be a norm subgroup, then the local Artin map is an isomorphism $K^\times/N \to \mathrm{Gal}(L/K)$. Thus N has finite index in $K^\times$. Since U_L is compact, $N(U_L)$ is closed in U_K and it has finite index since $U_K/N(U_L)$ embeds into $K^\times/N$. Hence $N(U_L)$ is open in U_K which is open in $K^\times$ and so $N(U_L)$ is an open finite index subgroup of $K^\times$.

Now let $M < K^\times$ be a finite index open subgroup. For a finite extension K'/K, set $D_{K'} = \bigcap N_{L/K'}(L^\times)$ where L runs over the finite extensions of K'. Then $N_{K'/K}D_{K'} = D_K$. Clearly $D_K \subset N_{K'/K}D_{K'}$. For the other inclusion, let $a \in D_K$ and look at the sets $S_L = N^{-1}_{K'/K}(a) \cap N_{L/K'}(L^\times)$, where L is a finite extension of K'. Each S_L is non-empty since a is a norm from L/K by definition of D_K. Further $S_{LE} \subset S_L \cap S_E$ for any finite extensions $L, E/K'$. Each S_L is non-empty since a is a norm from L/K by definition of D_K. Similarly to above one checks that the S_L are compact and so their intersection is non-empty as required.

Now we show that D_K is divisible. Let $a \in D_K$, n a positive integer and $L = K(\mu_n)$. Since $D_K = N_{L/K}(D_L)$ there is $b \in D_L$ such that $a = N_{L/K}(b)$. Moreover the Hilbert symbol satisfies $(b,c)_{L,n} = 1$ for all $c \in L^\times$ by definition of D_L. Hence b is an nth power and so is a. As a result D_K is divisible.

Since $M < K^\times$ has finite index and D_K is divisible, $D_K \subset M$. Each $N_{L/K}(L^\times) \cap U_K$ is compact and M is open so there are finite extensions $L_1, \ldots, L_s$ of K such that $N(L_1^\times) \cap \cdots \cap N(L_s^\times) \cap U_K \subset M$, taking $L = L_1 L_2 \ldots L_s$ we find $N_{L/K}(L^\times) \cap U_K \subset M$.

Let $N = N_{L/K}(L^\times)$, then $N \cap (U_K \cdot (N \cap M)) \subset M$ since if $a \in U_K$, $b \in N \cap M$ such that $ab \in N$, then $a \in N \cap U_K \subset M$ and also $ab \in M$. $N \cap M$ has finite index in $K^\times$ and as a result $U_K(N \cap M)$ is a finite index subgroup of $K^\times$ containing U_K. But U_K is the kernel of the valuation $v : K^\times \to \mathbb{Z}$, hence $U_K(N \cap M) = v^{-1}(m\mathbb{Z})$ for some non-zero integer m. This is the norm group of the unramified extension of degree m by the computation of the cohomology of unramified extensions 5.1.3.

Finally M contains the intersection of two norm groups N and $U_K(N \cap M)$ and so M contains a norm group $N_{F/K}(F^\times)$ for some finite field extension F/K. By possibly extending F we may assume that F/K is Galois. Moreover, if F' is the maximal abelian subextension of F then $\mathrm{Gal}(F'/K) = \mathrm{Gal}(F/K)^{ab}$ and $N(F') = N(F)$ since the local Artin map is an isomorphism. So we may assume that F/K is a finite abelian extension. Let E be the fixed field of $\phi_{F/K}(M)$. Since F/K is abelian, E/K is Galois and we have $N_{E/K}(E^\times) = \ker \phi_{E/K} = \ker(\phi_{F/K}|_E) = M$ since $\phi_{F/K}(M) = \mathrm{Gal}(F/E)$. In conclusion M is the norm group of the finite abelian extension E/K.

For the second part of the theorem note that the groups of the form $V \times n\mathbb{Z}$ where $V < U_K$ is an open subgroup are norm groups and they form a basis of open neighbourhoods of the identity in the norm topology. U_K is profinite as can be checked with 2.6.6. Thus the canonical map $U_K \to \lim_{\leftarrow} U_K/V$ where V runs through the open subgroups is an isomorphism. Hence there is a canonical isomorphism $\widehat{K^\times} \to U_K \times \hat{\mathbb{Z}}$. □

Corollary 5.2.14. *The assignment $L \mapsto N(L) := N_{L/K}(L^\times)$ is a bijection from the finite abelian extensions of K to the finite index open subgroups of $K^\times$.*

Proof. By the existence theorem $L \mapsto N(L)$ is surjective. Suppose L, L' are two abelian extensions of K such that $N(L) = N(L')$, then $E = LL'$ is another abelian extension and $N(E) \subset N(L) \cap N(L')$. Moreover, by 5.2.5 $\phi_{E/K}(x)|_L = \mathrm{id}$ if and only if $x \in N(L) = N(L')$ if and only if $\phi_{E/K}(x)|_{L'} = \mathrm{id}$. As $\phi_{E/K}$ is surjective we find $\mathrm{Gal}(E/L') = \mathrm{Gal}(E/L)$ and by Galois Theory $L = L'$. □

Given a finite abelian extension L/K we define its conductor as the least non-zero integer c such that $(1+\pi_K^c \mathcal{O}_K) \subset N(L)$. The conductor exists since $N(L) \cap \mathcal{O}_K^\times$ is an open subgroup of $\mathcal{O}_K^\times$. We have already seen that if L/K is unramified, then $H^2(L/K, U_L) = 0$ and since L/K is cyclic this implies $N(U_L) = U_K$ and $c = 0$. Moreover, we have

Proposition 5.2.15. *Let L/K be a finite abelian extension with ramification index e and inertia degree f whose residue field has characteristic p and let c be its conductor, then*

- *$c = 0$ if and only if L/K is unramified;*
- *$c = 1$ if and only if L/K is tamely ramified;*
- *$c \geq 2$ if and only if L/K is wildly ramified.*

In the last case the inequality $v_p(e) \leq (c-1)f$ holds.

Proof. Let $n = ef = [L : K]$ and E/K the maximal unramified subextension. Let π_L be a uniformiser of L, then $N_{L/E}(\pi_L)$ is a uniformiser of E and so $v_K(N_{L/K}(\pi_L)) = f$. Hence we always have $\pi_K^f \in N(L)$ for some uniformiser π_K. Moreover if $\pi_K^s \in N(L)$ for some $0 < s < f$, then we have an element in L with valuation $0 < es/n < 1$.

Absurd. This shows that $f = \min\{v_K(N(x)) : x \in \pi_L\mathcal{O}_L\}$ and thus $n = [K^\times : N(L)] = f[U_K : N(U_L)]$.

If $c = 0$, then $U_K \subset N(U_L)$ and so $e = 1$, i.e. L/K is unramified.

If $c \geq 1$, then $U_K \not\subset N(L)$, i.e. $e > 1$ and L/K is ramified.

If $c = 1$, then $(1 + \pi_K\mathcal{O}_K) \subset N(L)$ and $e \mid [U_K : (1 + \pi_K\mathcal{O}_K)]$, hence $p \nmid e$ and L/K is tamely ramified.

If $c \geq 2$, then $(N(L) \cap (1 + \pi_K\mathcal{O}_K))/(1 + \pi_K^c\mathcal{O}_K)$ is a non-zero p-group of cardinality at most $p^{f(c-1)}$ and so $v_p(e) \leq (c-1)f$. □

5.3 ℓ-Extensions

In this section we assume that the characteristic of K is 0, i.e. that K is a finite extension of $\mathbb{Q}_p$ and we indicate how one can think about the possible ℓ-extensions of K, i.e. not necessarily abelian Galois extensions whose degree is a power of ℓ for some prime ℓ. On the way we encounter the Tate Duality Theorem and Euler-Poincaré characteristics.

Theorem 5.3.1. *The cohomological dimension of K satisfies $cd(K) \leq 2$.*

Proof. Lang proved in his thesis [13] that the maximal unramified extension K^{un} of K is a C_1 field. As a result $\mathrm{cd}(K^{un}) \leq 1$ by 4.1.17. Let $H = \mathrm{Gal}(\overline{K}/K^{un})$ then we have an exact sequence

$$1 \to H \to G_K \to G_k \to 1.$$

Since $G_k = \hat{\mathbb{Z}}$ we have $cd(k) \leq 1$ as well. Now the Hochschild-Serre spectral sequence 2.4.17

$$H^i(K^{un}/K, H^j(K^{un}, A)) \implies H^{i+j}(K, A)$$

shows that $H^n(K, A) = 0$ for $n \geq 3$, where A is a torsion G_K-module. Thus $\mathrm{cd}(K) \leq 2$. □

Lemma 5.3.2. *Let K be a field complete with respect to a discrete valuation v and finite residue field, then $K^\times/(K^\times)^n$ is finite.*

Proof. Let $R = \{x \in K : v(x) \geq 0\}$ and $\pi \in R$ a uniformiser. When $v(x)$ is sufficiently large, then both $\exp(x) = \sum_{n \geq 0} \frac{x^n}{n!}$ and $-\log(1-x) = \sum \frac{x^n}{n}$ converge. Hence there is an isomorphism $\exp : \pi^s R \to 1 + \pi^s R$ for s large enough. $\pi^s R/n\pi^s R = R/nR$ is finite since $R/\pi R$ is finite by assumption and so $1 + \pi^s R/(1 + \pi^s R)^n$ is finite as well. Using that the residue field is finite it is straightforward to check that $R^\times/(1 + \pi^s R)$ is finite as well.

Considering the following diagram it is easy to see that $R^\times/(R^\times)^n$ is finite

$$\begin{tikzcd}
0 \arrow[r] & (1+\pi^s R) \arrow[r] \arrow[d, "n"] & R^\times \arrow[r] \arrow[d, "n"] & R^\times/(1+\pi^s R) \arrow[r] \arrow[d, "n"] & 0 \\
0 \arrow[r] & (1+\pi^s R) \arrow[r] & R^\times \arrow[r] & R^\times/(1+\pi^s R) \arrow[r] & 0
\end{tikzcd}$$

hence also $K^\times/(K^\times)^n$ is finite since $K^\times \cong \mathbb{Z} \times R^\times$. □

Proposition 5.3.3. *Let A be a finite G_K-module. Then $H^i(K, A)$ is finite for all i.*

Proof. For $i = 0$ this is trivial. For $i > 2$ this follows from 5.3.1. Since A is finite, there exists a finite extension L/K such that G_L acts trivially on A and so A is isomorphic to a direct sum of copies of $\mathbb{Z}/n\mathbb{Z}$. After adjoining sufficiently many roots of unity we find a Galois extension L/K such that over L, A is isomorphic to a direct sum of some μ_n. Then $H^1(L, \mu_n) \cong L^\times/(L^\times)^n$ is finite by 5.3.2. Moreover by the cohomology long exact sequence and 5.1.10 $H^2(L, \mu_n) = \mathrm{Br}(L)[n] = \mathbb{Z}/n\mathbb{Z}$ is finite, too. From the spectral sequence $H^i(L/K, H^j(L, A)) \implies H^{i+j}(K, A)$ we conclude that $H^i(K, A)$ is finite for $i = 1, 2$. □

This allows us to define the Euler-Poincaré characteristic by

$$\chi(A) = \frac{h^0(A)h^2(A)}{h^1(A)},$$

where A is a discrete G_K-module and $h^i(A) = |H^i(K, A)|$. This is an additive function on the category of finite discrete G_K-modules since $cd(K) \leq 2$ by 5.3.1, i.e. for every short exact sequence $0 \to A \to B \to C \to 0$ we have $\chi(B) = \chi(A)\chi(C)$.

Let A be a finite G_K module and set $A' = \mathrm{Hom}_{\mathbb{Z}}(A, \overline{K}^\times)$ with G_K acting by $(g, f) \mapsto (x \mapsto gf(g^{-1}x))$, then we have

Theorem 5.3.4 (Tate Duality)**.** *Let A be a finite discrete G_K module, then the cup product*

$$H^i(K, A) \times H^{2-i}(K, A') \to H^2(K, \overline{K}^\times) \cong \mathbb{Q}/\mathbb{Z}$$

is a non-degenerate bilinear pairing for $0 \leq i \leq 2$.

Proof Sketch. The idea is to show that the functor $A \mapsto H^2(K, A)$ for A finite is representable as $A \mapsto \mathrm{Hom}_G(A, I)$ for some torsion module I. One then uses the computation of the Brauer group of a local field to show that $I = \mu$ is the module of all roots of unity. Now $A' = \mathrm{Hom}(A, I)$ since A is finite and so the theorem follows for $i = 2$. For $i = 0$ one switches the roles of A and A' and uses $A'' = A$. For $i = 1$ one can use dimension shifting to reduce to $i = 2$. See [21, II.5. Theorem 2] for the proof. □

Note that for $A = \mathbb{Z}/n\mathbb{Z}$ we recover the properties of the Hilbert symbol. Let ℓ be a prime and $G_K(\ell)$ the maximal pro-ℓ quotient of G_K, i.e. the Galois group of the maximal ℓ-extension of K.

Lemma 5.3.5. *If $G_K(\ell) = G_K/N$, then $H^1(N, \mathbb{Z}/\ell\mathbb{Z}) = H^2(N, \mathbb{Z}/\ell\mathbb{Z}) = 0$.*

Proof. If $H^1(N, \mathbb{Z}/\ell\mathbb{Z}) \neq 0$, then there is a non-trivial continuous map $N \to \mathbb{Z}/\ell\mathbb{Z}$ and N has a non-trivial pro-ℓ quotient. This is impossible because if N/M is the maximal pro-ℓ quotient, then M is also normal in G since N/gMg^{-1} is another pro-ℓ quotient of N. But by maximality of M this implies $N = M$.

Let $K(\ell)$ be the maximal ℓ-extension of K and let $K(\ell) \subset L$ be any algebraic extension, write $L = \lim_{\rightarrow} L_\alpha$ as a union over finite subextensions $K \subset L_\alpha \subset L$. Let A be a central simple algebra over L and $\{e_i\}$ be a L-basis of A. Then by writing e_ie_j and e_i^{-1} as linear combinations of the e_i there exists a finite subextension $K \subset K' \subset L$ such that all the coefficients are in K'. So there is a central simple algebra A' over K' such that $A = A' \otimes_{K'} L$. This shows that $\mathrm{Br}(L) = \lim_{\rightarrow} \mathrm{Br}(L_\alpha)$. If $L_\alpha \subset L_\beta$ is Galois of degree p^s, then we have the commutative square

$$\begin{tikzcd}
\mathrm{Br}(L_\alpha) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}"] & \mathrm{Br}(L_\beta) \arrow[d, "\mathrm{inv}"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "p^s"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

Since $K(\ell)$ contains the maximal unramified ℓ-extension of K which have arbitrarily high degree over K we find that the ℓ-primary component of $\mathrm{Br}(L)$ vanishes. Let $M < N$ be a pro-ℓ sylow subgroup and L the fixed field of M, then $L(\mu_\ell)/L$ is a Galois extension of order prime to ℓ. Thus $\mu_\ell \subset L$ and $\mathrm{Br}(L)(\ell) = H^2(M, \mu_\ell) = H^2(M, \mathbb{Z}/\ell\mathbb{Z}) = 0$ and so $\mathrm{cd}_\ell(N) \leq 1$ by 2.8.5 and 2.8.4. In particular $H^2(N, \mathbb{Z}/\ell\mathbb{Z}) = 0$. □

Corollary 5.3.6. *Suppose K is a finite extension of $\mathbb{Q}_p$, then the maximal pro-ℓ quotient $G_K(\ell)$ can be generated by $\dim_{\mathbb{F}_\ell} K^\times/(K^\times)^\ell$ elements. If K does not contain the ℓth roots of unity μ_ℓ, then $G_K(\ell)$ is free and if $\mu_\ell \subset K$, then there is one relation between those generators.*

Proof. From the lemma and inflation-restriction 2.4.14 we find that the inflation maps

$$H^i(K(\ell)/K, \mathbb{Z}/\ell\mathbb{Z}) \to H^i(K, \mathbb{Z}/\ell\mathbb{Z})$$

are isomorphisms for $i = 1, 2$. Thus 2.8.10 shows that the minimal number of generators of $G_K(\ell)$ is $\dim H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ and the minimal number of relations between those generators is $\dim H^2(K, \mathbb{Z}/\ell\mathbb{Z})$. The dual of $\mathbb{Z}/\ell\mathbb{Z}$ is μ_ℓ and so by Tate Duality the dimension of $H^2(K, \mathbb{Z}/\ell\mathbb{Z})$ is equal to the dimension of $H^0(K, \mu_\ell)$ which is zero or one depending on whether μ_ℓ is contained in K or not. Moreover, $H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ is dual to $H^1(K, \mu_\ell) = K^\times/(K^\times)^\ell$ and the claim follows. □

To compute the dimension of $K^\times/(K^\times)^\ell$ one could analyse the exponential map. Alternatively, there is a strong result on Euler-Poincare characteristics [21, II. 5.7]:

Theorem 5.3.7. *For any finite discrete G_K-module A we have $\chi(A) = \|a\|_K$, where $\|\cdot\|_K$ is the absolute value of K normalised to $|p| = p^{-[K:\mathbb{Q}_p]}$ and a is the cardinality of A.*

Corollary 5.3.8. *Let d be the dimension of $K^\times/(K^\times)^\ell$. If $\mu_\ell \subset K$, then $d = 2$ if $\ell \neq p$ and $d = [K : \mathbb{Q}_p] + 2$ if $\ell = p$. If $\mu_\ell \not\subset K$, then $d = 1$ if $\ell \neq p$ and $d = [K : \mathbb{Q}_p] + 1$ if $\ell = p$.*

Proof. We have $H^0(K, \mathbb{Z}/\ell\mathbb{Z}) = \mathbb{Z}/\ell\mathbb{Z}$ and $H^2(K, \mathbb{Z}/\ell\mathbb{Z})$ is dual to $H^0(K, \mu_\ell)$ which has dimension 1 if $\mu_\ell \subset K$ and 0 if $\mu_\ell \not\subset K$. Putting this together with the fact that $\chi(\mathbb{Z}/\ell\mathbb{Z}) = 1$ if $\ell \neq p$ and $\chi(\mathbb{Z}/\ell\mathbb{Z}) = \ell^{-[K:\mathbb{Q}_p]}$ if $\ell = p$ we find the dimension of $H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ which is dual to $K^\times/(K^\times)^\ell$. □

We investigate the previous results a bit more closely in the case $K = \mathbb{Q}_p$. If $\ell \nmid p(p-1)$, then $\mu_\ell \not\subset \mathbb{Q}_p$ and $G_K(\ell)$ is free of rank 1, i.e. isomorphic to $\mathbb{Z}_\ell$. For such ℓ, every Galois ℓ-extension is cyclic since its group is a quotient of $\mathbb{Z}_\ell$ and moreover there is a unique such extension for every power of ℓ. Since there are cyclic unramified extensions of every degree these extensions must all be unramified. So for example this shows that every Galois extension of $\mathbb{Q}_5$ whose degree is a power of 3 is a cyclic unramified extension. This is not surprising since ramification theory [20, IV] shows that any prime divisor of the ramification index of any finite Galois extension of $\mathbb{Q}_p$ must divide $p(p-1)$.

For $p = \ell$ we have that $G_K(p)$ is free of rank 2 for $p > 2$ and $G_K(p)$ is generated by 3 elements with one relation if $p = 2$. So for example for $p > 2$, a p-group can be generated by 2 elements if and only if it appears as a Galois group of a finite extension of $\mathbb{Q}_p$.

6 Global Class Field Theory

In this section we outline some of the theorems of global class field theory in terms of the local ones. For simplicity we formulate the theory in terms of number fields but one can generalise to other global fields, like function fields of algebraic curves over a finite field. We refer to [16] for most substantial proofs. The main tools for which are

1. Classical results in algebraic number theory from [17] like the finiteness of the class group, Dirichlet unit theorem and Frobenius elements

2. Cohomological methods which connect to the local theory

3. Density of certain classes of primes which can be derived from the study of the Dedekind zeta function.

In local class field theory we showed that for any finite Galois extension of local fields L/K one has $H^1(L/K, L^\times) = 0$ and $H^2(L/K, L^\times) \cong \mathbb{Z}/[L : K]\mathbb{Z}$ and this isomorphism is compatible with inflation and restriction, i.e. the conditions of Tate's theorem are satisfied and we get the local Artin map $\phi_K : K^\times \to \mathrm{Gal}(K^{ab}/K)$. Now the goal is to take a number field K and somehow glue all the local Artin maps ϕ_{K_v} of the completions K_v together to a global Artin map $\phi_K : C_K \to \mathrm{Gal}(K^{ab}/K)$, where C_K is the idele class group. As in the local theory this is a powerful tool for studying the abelian extensions of a global field. In addition the theory gives rise to local-global principles, which determine some object over K from all the corresponding objects over all the completions K_v. For example $\mathrm{Br}(\mathbb{Q})$ is determined by the Brauer groups $\mathrm{Br}(\mathbb{Q}_p)$ and $\mathrm{Br}(\mathbb{R})$ which gives rise to the Hasse Principle. Another main feature of the theory are reciprocity laws, which generalise the famous law of quadratic reciprocity in several ways.

6.1 The Fundamental Exact Sequence

Definition 6.1.1 (Ideles). *Let K be a number field, then we the define the ideles of K as*

$$\mathbb{I}_K := \left\{ (x_v) \in \prod_v K_v^\times : x_v \in \mathcal{O}_v^\times \text{ for all but finitely many } v \right\}.$$

For a finite set of places S of K we set $\mathbb{I}_{K,S} = \prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_v^\times$ equipped with the product topology. Now $\mathbb{I}_K = \bigcup_S \mathbb{I}_{K,S}$ and we give it the limit topology. A basis of this topology is given by the sets of the form $\prod_{v\in S} U_v$ such that $U_v \subset K_v^\times$ is open and $U_v = \mathcal{O}_v$ for all but finitely many v.

Let L/K be a finite Galois extension, then the global Artin map is defined as the unique map $\phi_{L/K} : \mathbb{I}_K \to \mathrm{Gal}(L/K)^{ab}$ such that for each place v of K, the diagram

$$\begin{tikzcd}
K_v^\times \arrow[r, "\phi_v"] \arrow[d] & \mathrm{Gal}(L_w/K_v)^{ab} \arrow[d] \\
\mathbb{I}_K \arrow[r, "\phi_{L/K}"] & \mathrm{Gal}(L/K)^{ab}
\end{tikzcd}$$

commutes, where ϕ_v is the local Artin map of K_v. $\phi_{L/K}$ is well-defined since the ϕ_v vanish on $\mathcal{O}_v^\times$, when v is unramified in L and only finitely many places are ramified.

Definition 6.1.2. *The idele class group of a number field K is $C_K := \mathbb{I}_K/K^\times$.*

The classical ideal class group is a quotient of the idele class group and we will later see the very powerful result that $\phi_{L/K}$ factors through C_K. This is the basis of the higher reciprocity laws which generalise the classical law of quadratic reciprocity.

Let L/K be a finite Galois extension with group G, then G acts on $\mathbb{I}_L$ by $\sigma(x_w) = (\sigma(x_{\sigma w}))$ and one can show that the inclusion $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ induces an isomorphism $\mathbb{I}_L^G \cong \mathbb{I}_K$. Since $H^1(G, L^\times) = 0$ by Hilbert's Theorem 90 this also gives an isomorphism $C_L^G \cong C_K$. Now the analogue to the local theory is

Theorem 6.1.3. *Let L/K be a cyclic Galois extension of number fields, then $H^1(L/K, C_L) = 0$ and $H^2(L/K, C_L)$ is of order $[L : K]$.*

Proof. See [16]. □

Corollary 6.1.4. *Let $K \subset L$ be a finite Galois extension of number fields with Galois group G, then $H^1(G, C_L) = 0$.*

Proof. As usual, we reduce to the case of G being a p-group using 2.4.12. So suppose G is a p-group of order $> p$, then G has a normal subgroup H of index p and we have the inflation-restriction sequence

$$0 \to H^1(G/H, C_L^H) \to H^1(G, C_L) \to H^1(H, C_L).$$

Since $C_L^H = C_{L^H}$ we conclude by exactness and induction that $H^1(G, C_L) = 0$. □

Corollary 6.1.5 (Second Inequality)**.** *Let L/K be a finite Galois extension of number fields with group G, then the orders of $H^2(G, C_L)$ and $\hat{H}^0(G, C_L) = C_K/N(C_L)$ divide $[L : K]$.*

Proof. For H^2 this is another application of 2.4.12 and 2.4.14. Moreover, from dimension shifting one can derive similar results for $\hat{H}^0$. □

Theorem 6.1.6 (Fundamental exact sequence)**.** *If K is a number field, then there is an exact sequence*

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0,$$

where the first map is induced by the inclusions $K \subset K_v$, the sum is over all places of K and the right map is given by the sum of the local invariant maps. (In the case that $K_v = \mathbb{R}$ we send the class of the quaternions to $1/2$.)

Proof. We only proof injectivity of the first map and for surjectivity we refer the reader to [16]. Let L/K be a finite Galois extension with group G. For each place v of K we have $\prod_{w|v} L_w^\times \cong \mathrm{Ind}_{G_{w_0}}^G L_{w_0}^\times$, where $w_0 \mid v$ is some fixed place above v. Using Shapiro's lemma and that the cohomology of unramified units is trivial one finds $H^2(L/K, \mathbb{I}_L) \cong \bigoplus_v \mathrm{Br}(L_w/K_v)$ where w is any place lying over v. From the exact sequence $0 \to L^\times \to \mathbb{I}_L \to C_L \to 0$ and 6.1.3 we obtain the exact sequence

$$0 \to \mathrm{Br}(L/K) \to \bigoplus_v \mathrm{Br}(L_w/K_v) \to H^2(L/K, C_L).$$

By passing to the limit we conclude that $\mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v)$ is injective. □

Corollary 6.1.7 (Hasse Norm Principle)**.** *Let $a \in K^\times$ be an element of a number field and L/K a finite cyclic extension. Then for all but finitely many places v of K, a is a norm from L_w, where w is a place of L lying over v. If it is a norm in all completions, then a is a norm from L.*

Proof. If L/K is cyclic, then all L_w/K_v is cyclic for all places v. Since its Galois group is isomorphic to the decomposition group of v which is a subgroup of the cyclic group $\mathrm{Gal}(L/K)$. Hence by 2.3.2 we have $\mathrm{Br}(L/K) = K^\times/N(L^\times)$ and $\mathrm{Br}(L_w/K_v) = K_v^\times/N(L_w^\times)$ and by the fundamental exact sequence an injective map

$$K^\times/N(L^\times) \to \bigoplus_v K_v^\times/N(L_w^\times).$$

It remains to show that this map is just given by the natural inclusions $\iota_v : K \hookrightarrow K_v$. Let $\chi : \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ be injective and $H < \mathrm{Gal}(L/K)$ the decomposition group of w. $a \mapsto a \cup \delta\chi$ is an isomorphism $K^\times/N(L^\times) \to H^2(L/K, L^\times)$ by 2.5.12. Now since the cup product and coboundary map are compatible with restriction we find $\mathrm{Res}_H(a \cup \delta\chi) = a \cup \delta(\mathrm{Res}_H \chi)$. But $\mathrm{Res}_H \chi = \chi|_H$ is an injective map $H \to \mathbb{Q}/\mathbb{Z}$ and so again by 2.5.12 $a \mapsto a \cup \delta(\mathrm{Res}_H \chi)$ is a compatible isomorphism $K_v^\times/N(L_w^\times) \to H^2(L_w/K_v, L_w^\times)$. □

Corollary 6.1.8 (Classical Hasse Principle). *A projective plane conic over $\mathbb{Q}$ has a rational point if and only if it has a point in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p.*

Proof. If there is a rational point, then there is obviously a point in all completions of $\mathbb{Q}$. Now suppose the conic has points in all completions of $\mathbb{Q}$. After a change of coordinates we may assume the conic to be of the form $x^2 - ay^2 - bz^2 = 0$ for some $a, b \in \mathbb{Q}$. If $a = 0$ or $b = 0$, then it trivially has a rational point. Hence we may assume a and b to be non-zero. In that case $x^2 - ay^2 - bz^2 = 0$ has a rational point if and only if a is a norm from $\mathbb{Q}(\sqrt{b})$ if and only if a is a norm from $\mathbb{Q}_p(\sqrt{b})$ for all p and from $\mathbb{R}(\sqrt{b})$. □

Remark 6.1.9. *We can now give a funny proof that $x^2 + y^2 + z^2 = 0$ has no non-trivial solutions in $\mathbb{Q}_2$.*

Proof. Note that $x^2 + y^2 + z^2 = 0$ has a non-trivial solution in a field K if and only if -1 is a norm from $K(i)$. We know that the equation has no non-trivial solutions in $\mathbb{R}$. By the fundamental exact sequence there must be another place where the equation has no solutions since otherwise the sum of local invariants is $1/2 \neq 0$. But if p is an odd prime, then a pigeon hole argument shows that $x^2 + y^2 + z^2 = 0$ has a solution in $\mathbb{F}_p$ and by Hensel's lemma also in $\mathbb{Q}_p$. Thus we conclude that $x^2 + y^2 + z^2 = 0$ has no solutions in $\mathbb{Q}_2$ without ever touching the field $\mathbb{Q}_2$. □

Corollary 6.1.10 (Artin Reciprocity). *Let L/K be a finite Galois extension, then*

$$\prod_v \phi_v(x) = 1$$

for all $x \in K^\times$, i.e. $\phi_{L/K}$ factors through C_K.

Proof. Firstly note that only finitely many terms in the product are non-trivial because for all but finitely many places v is unramified and $x \in \mathcal{O}_v$. Moreover, for any character $\chi : \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$ we have $\chi(\phi_v(x)) = \mathrm{inv}_v(x \cup \delta\chi)$ by 5.2.5, thus the fundamental exact sequence shows

$$\sum_v \mathrm{inv}_v(x \cup \delta\chi) = 0$$

and consequently

$$\chi\left(\prod_v \phi_v(x)\right) = 0. \qquad \square$$

Artin reciprocity is an extremely powerful result from which we will later generalise the law of quadratic reciprocity to the power reciprocity law. But first we will show how to concretely find information about solutions to cubic equations modulo primes $p \in \mathbb{Z}$.

Proposition 6.1.11. *Let $f \in \mathbb{Z}[x]$ be a monic cubic whose discriminant Δ is a square with prime divisors $q_1, \dots, q_l \mid \Delta$. If $p \nmid \Delta$ is another prime, then whether $f(x) = 0$ has a solution in $\mathbb{F}_p$ depends only on the residue class of p modulo*

- *$m = q_1 q_2 \dots q_l$ if $3 \nmid \Delta$;*
- *$m = 3q_1 q_2 \dots q_l$ if $3 \mid \Delta$*

and there exist an index 3 subgroup $H < (\mathbb{Z}/m\mathbb{Z})^\times$ such that f has a solution modulo p if and only if $p + m\mathbb{Z} \in H$.

Proof. As above let L be the splitting field of f over $\mathbb{Q}$, then all ramified primes of L divide Δ. If $p \nmid \Delta$, then we can apply the Dedekind-Kummer theorem to show that $f(x) = 0$ has a root in $\mathbb{F}_p$ if and only if p splits in L if and only if $\phi_p(p) = 1$ if and only if $\prod_{i=1}^l \phi_{q_i}(p) = 1$. If $q_i \neq 3$, then it is at worst tamely ramified, has conductor 1 (by 5.2.15) and so $\phi_{q_i}(p)$ only depends on the class of p modulo q_i. If $q_i = 3$, then $\phi_{q_i}(p)$ depends on p modulo 3^c, where c is the conductor of $E/\mathbb{Q}_3$ and E is the splitting field of f over $\mathbb{Q}_3$. But this extension has degree at most 3 so the index $[\mathbb{Z}_3^\times : N(U_E)]$ is at most 3. However, it is well-known that one can lift a generator of $(\mathbb{Z}/3\mathbb{Z})^\times$ to a topological generator of $\mathbb{Z}_3^\times$ and so $\mathbb{Z}_3^\times$ has a unique open index 3 subgroup, namely $\pm(1 + 9\mathbb{Z}_3)$. Thus the conductor of $E/\mathbb{Q}$ is either 0 or 2.

Now that the modulus has been determined we note that $\prod_{i=1}^l \phi_{q_i}$ defines a homomorphism $(\mathbb{Z}/m\mathbb{Z})^\times \to \mathrm{Gal}(L/\mathbb{Q})$. But we also know that one of the ϕ_{q_i} is non-zero since otherwise for all primes p, ϕ_p is zero but then the global Artin map is zero which is a contraction since we prove in the next section that the global Artin map is surjective. It's kernel must therefore be an index 3 subgroup $H < (\mathbb{Z}/m\mathbb{Z})^\times$. $\square$

Example 6.1.12. *From the modulus m in the previous proposition we can explicitly find all the residue classes for which the cubic has a solution by checking small primes using a computer program. Here a list of examples which was produced in this way*

f	Δ	H	m
$x^3 - 7x - 7$	7^2	± 1	7
$x^3 - 3x + 1$	3^4	± 1	9
$x^3 + 4x^2 + x - 1$	13^2	$\pm 1, \pm 5$	13
$x^3 + 5x^2 + 2x - 1$	19^2	$\pm 1, \pm 7, \pm 11$	19
$x^3 + 4x^2 - 7x + 1$	37^2	$\pm 1, \pm 6, \pm 8, \pm 10, \pm 11, \pm 14$	37
$x^3 + 9x^2 + 6x - 1$	$3^4 \cdot 7^2$	$\pm 1, \pm 5, \pm 8, \pm 11, \pm 23, \pm 25$	63
$x^3 + 6x^2 - x - 5$	$5^2 \cdot 13^2$	$\pm 1, \pm 8, \pm 12, \pm 14, \pm 18, \pm 21, \pm 27, \pm 31$	65

Note that if $\Delta = q^r$ is a prime power, then the group of cubes is the unique index 3 subgroup and so we don't actually need to do this computation. Now we investigate what happens if the discriminant of a monic cubic $f \in \mathbb{Z}[x]$ is not a square. Then the splitting field $L = \mathbb{Q}(f)$ is not abelian over $\mathbb{Q}$, but it is still solvable. More concretely $\sqrt{\Delta} \in L$ and $L/\mathbb{Q}(\sqrt{\Delta})$ has degree 3.

Let $p \nmid \Delta$ be a prime. If Δ is not a square modulo p, then f has exactly one solution in $\mathbb{F}_p$. To see this note that $\mathbb{F}_p(f)/\mathbb{F}_p$ has degree at most 3 since any finite extension of finite fields is Galois. But $\mathbb{F}_p(f)$ contains $\mathbb{F}_p(\sqrt{\Delta})$ which has degree 2 over $\mathbb{F}_p$. We conclude $\mathbb{F}(f) = \mathbb{F}_p(\sqrt{\Delta})$ and f must have exactly one root as desired.

If Δ is a square modulo $p > 2$, then either f splits modulo p or is irreducible modulo p. We have $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ and $\mathfrak{p}_1$ splits in L if and only if f splits mod p. The same holds for $\mathfrak{p}_2$, thus $\phi_{\mathfrak{p}_1}(p) = \mathrm{Frob}_{\mathfrak{p}_1}^2 = 1$ if and only if $\phi_{\mathfrak{p}_2}(p) = 1$ if and only if f splits modulo p. However if we naively try to apply Artin reciprocity here, we can only determine the product $\phi_{\mathfrak{p}_1}(p)\phi_{\mathfrak{p}_2}(p)$ and not the individual factors. If the $\mathfrak{p}_i = (\alpha_i)$ are principal, then we can apply Artin Reciprocity to determine $\phi_{\mathfrak{p}_1}(\alpha_1)$ from congruence conditions on α_1. More generally if 3 does not divide the class number $h(K)$, then $\mathfrak{p}_i^h = (\alpha_i)$ is principal and we can get the answer from there since $3 \nmid h$ and the image of the local Artin map is a group of order dividing 3.

Example 6.1.13. *Let $f = x^3 - 5x + 5$, then $\Delta = -5^2 \cdot 7$ and if p is a prime such that -7 is a square $\pmod p$, then whether f splits $\pmod p$ depends only on the class of p modulo 7 and the classes of a, b modulo 5, where $4p = a^2 + 7b^2$. In particular if p is a prime $\equiv 1, 2, 4 \pmod 7$, then f splits $\pmod p$ if and only if $5 \mid ab$.*

Proof. Let $K = \mathbb{Q}(\sqrt{-7})$. This field has class number 1 and so p splits into principal ideals and there exist $a, b \in \mathbb{Z}$ such that $4p = a^2 + 7b^2$. Let $r = (a + b\sqrt{-7})/2 \in \mathcal{O}_K$, then $r\overline{r} = p$ and f splits in $\mathbb{F}_p \cong \mathcal{O}_K/(r)$ if and only if (r) splits in $L = \mathbb{Q}(f)$ if and only if $\phi_r(r) = 1$. By Artin reciprocity this only depends on r modulo cubes in $\mathcal{O}_K/(5)$ and on r modulo cubes in $\mathcal{O}_K/(\sqrt{-7})$. Note that $a \equiv 2r \equiv 2\overline{r}$

(mod $\sqrt{-7}$) and so $r^2 \equiv p$, hence $\phi_7(r) = \phi_7(p^{-1})$ only depends on the class of p mod 7. Moreover, $\phi_5(r)$ only depends on the classes of a, b modulo 5. To check the final statement it suffices to let a computer do the small primes. □

When 3 divides the class number I don't know how to solve this problem. But of course one can also use similar methods to reason about roots of higher degree polynomials modulo primes whenever the extensions involved are abelian or at least solvable. We will later do this for polynomials of the form $x^m - a$.

6.2 Global Norm Groups

We now establish the global analogue to the bijection between norm groups and abelian extensions of a local field. In particular this will give rise to the Hilbert class field of a number field which amongst other things can be used to study primes of the form $p = x^2 + ny^2$ [8].

Let L/K be a finite Galois extension of number fields with group G. Then C_L is a $\mathbb{Z}[G]$-module and we have a natural isomorphism $C_K \cong C_L^G$ induced by the inclusion $C_K \hookrightarrow C_L$.

Theorem 6.2.1. *Let L/K be a finite abelian extension, then $\phi_{L/K} : C_K/N(C_L) \to \mathrm{Gal}(L/K)$ is an isomorphism.*

Proof. This statement is sensible because $\phi_{L/K}$ factors through C_K by 6.1.10 and at each local factor ϕ_v factors through $K_v^\times/N(L_w^\times)$, where w is a place of L above v. By 6.1.5 it suffices to show that $\phi_{L/K}$ is surjective. This is the case since $\mathrm{Gal}(L/K)$ is generated by the decomposition groups. To see this let $H < \mathrm{Gal}(L/K)$ be the subgroup generated by the decomposition groups and $E = L^H$ its fixed field. Then $E_\mathfrak{p} = K_p$ for every prime $\mathfrak{p}$ lying over a prime p of K. Hence every prime of K is inert in E but this implies that $K = E$ as shown in the following lemma. □

Lemma 6.2.2. *Let L/K be a non-trivial extension of number fields, then there are infinitely many primes of K which split in L.*

Proof. [5] By the theorem of the primitive element, there exists $\alpha \in L$ such that $L = K(\alpha)$. We may assume $\alpha \in \mathcal{O}_L$ by scaling with a large integer. Let f be the minimal polynomial of α over K. Then $g(x) = N_{K/\mathbb{Q}}(f(x))$ has coefficients in $\mathbb{Z}$. We show that there exist infinitely many primes p such that g has a root modulo p. Let a_0 be the constant coefficient of g and suppose there were only finitely many such $p_1, \ldots, p_s$, then $g(p_1 \ldots p_s a_0 t)$ takes infinitely many values of the form $a_0 k$, as t runs through $\mathbb{Z}$. So there exists a prime p_{s+1} and $t \in \mathbb{Z}$ such that $p_{s+1} a_0 \mid g(p_1 \ldots p_s a_0 t)$. But $g(p_1 \ldots p_s a_0 t)/a_0 \equiv 1 \pmod{p_i}$ for all $i \in \{1, \ldots, s\}$, hence p_{s+1} is not one of the p_i. Contradiction.

[5] I learned this proof from Wojtek Wawrow.

Then by Dedekind-Kummer, for each such prime which doesn't divide the discriminant of f, any prime $\mathfrak{p}$ of K lying above it splits in L. □

As in the local theory, there is an existence theorem, i.e. for every open finite index subgroup $U < C_K$ there exists a finite abelian extension L/K such that $N_{L/K}(C_L) = U$ and the extension L is unique since $\phi_{L/K}$ is an isomorphism. As a powerful consequence we have

Theorem 6.2.3 (Hilbert Class Field). *Let K be a number field and let L/K be the maximal abelian unramified (also at infinite places) extension of K. Then L/K is called the Hilbert class field of K and there exists a natural isomorphism $\mathrm{Cl}(K) \to \mathrm{Gal}(L/K)$ which maps a prime ideal $\mathfrak{p}$ to its Frobenius element.*

Proof. Let L/K be an abelian extension. By 5.2.15 L/K is unramified at v if and only if $\mathcal{O}_{K,v}^\times \subset N(L_w)$ for a place w above v. Thus L/K is unramified if and only if $\prod_v \mathcal{O}_v^\times \subset N(\mathbb{I}_L)$. On the other hand the map $\mathbb{I}_K \to \mathrm{Cl}(K)$ which maps $(1, \dots, \pi_\mathfrak{p}, 1, \dots)$ to the ideal class of $\mathfrak{p}$ is surjective with kernel $N = K^\times \cdot \prod_v \mathcal{O}_v^\times$. By the existence theorem there exists an abelian extension L/K such that $N(\mathbb{I}_L) = N$ and so this must be the maximal abelian unramified extension of K and the Artin map gives the isomorphism described in the claim. □

Corollary 6.2.4. *Let K be a number field and L/K its Hilbert class field, then a prime ideal $\mathfrak{p}$ of K splits completely in L if and only if it is principal.*

Proof. $\mathfrak{p}$ splits completely if and only if its Frobenius element is the identity. By the isomorphism $\mathrm{Cl}(K) \to \mathrm{Gal}(L/K)$ this happens if and only if $\mathfrak{p}$ is principal. □

Corollary 6.2.5. *Let n be square-free and $\not\equiv 3 \pmod 4$, then a prime $p \nmid 2n$ is of the form $x^2 + ny^2$ with $x, y \in \mathbb{Z}$ if and only if p splits completely in the Hilbert class field of $\mathbb{Q}(\sqrt{-n})$.*

Proof. Let $K = \mathbb{Q}(\sqrt{-n})$, then p is of the form $x^2 + ny^2$ if and only if p splits into principal ideals in K. Let L/K be the Hilbert class field of K, then $L/\mathbb{Q}$ is Galois since if σ is an automorphism of $\overline{\mathbb{Q}}$, then $\sigma(L)$ is another abelian unramified extension of K and $\sigma(L) \subset L$. Now p splits completely in L if and only if $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ of K which splits completely in L, i.e. is principal. In conclusion p splits completely in L if and only if it is of the form $x^2 + ny^2$. □

Example 6.2.6. *A prime $p \neq 2, 5$ is of the form $x^2 + 5y^2$ if and only if $p \equiv 1, 9 \pmod{20}$.*

Proof. We need to find the Hilbert class field of $K = \mathbb{Q}(\sqrt{-5})$. Using the Minkowski bound of $4\sqrt{5}/\pi < 3$ and that $2 = (2, 1 - \sqrt{-5})^2$ one checks that $\mathrm{Cl}(K) \cong \mathbb{Z}/2\mathbb{Z}$. Thus it suffices to find an unramified extension of K of degree 2. Let $L = \mathbb{Q}(i, \sqrt{5}) = K(i)$, then L/K is at most unramified at the prime above 2. But $2\mathbb{Z}$ has ramification index 2 in K and the prime above 2 in $\mathbb{Q}(i)$ is unramified in L, thus $(2, 1-\sqrt{-5})$ is unramified in L as well. Consequently L is the Hilbert class field of K. A prime $p \neq 2, 5$ splits completely in L if and only if both -1 and 5 are squares mod p, i.e. if and only if $p \equiv 1, 9 \pmod{20}$. □

Theorem 6.2.7 (Principal Ideal Theorem)**.** *Let K be a number field and L/K its Hilbert class field, then every ideal of $\mathcal{O}_L$ becomes principal in $\mathcal{O}_L$.*

Proof Sketch. Let E/L be the Hilbert class field of L, then L is the maximal abelian extension of K contained in E and so $N_{E/K}(C_E) = N_{L/K}(C_L)$. We get a commutative diagram

$$\begin{tikzcd}
\mathrm{Cl}(L) = \hat{H}^0(E/L, C_E) \arrow[r, "\phi_{E/L}"] & \hat{H}^{-2}(E/L, \mathbb{Z}) = \mathrm{Gal}(E/L) \\
\mathrm{Cl}(K) = \hat{H}^0(E/K, C_E) \arrow[r, "\phi_{E/K}"] \arrow[u, "\mathrm{Res}"] & \hat{H}^{-2}(E/K, \mathbb{Z}) = \mathrm{Gal}(L/K) \arrow[u, "\mathrm{Res}"]
\end{tikzcd}$$

It turns out that the left vertical map is given by sending an ideal $\mathfrak{a} \mapsto \mathfrak{a}\mathcal{O}_L$ and the right vertical map is always 0 by the following group theoretical theorem. □

Theorem 6.2.8 (Furtwängler)**.** *Let G be a finite group and $H = [G, G]$ its commutator subgroup, then the restriction $\hat{H}^{-2}(G, \mathbb{Z}) \to \hat{H}^{-2}(H, \mathbb{Z})$ is the zero map.*

Proof. See [19] and [29]. □

Thus ideal factorisations in $\mathcal{O}_K$ become actual factorisations in $\mathcal{O}_L$, where L is the Hilbert class field of K. However, in $\mathcal{O}_L$ there are new ideals which are not principal and to study them one might consider taking the Hilbert class field of L as we already did in the proof of the Principal Ideal Theorem. Now a natural question called the class field tower problem arises. Let K be a number field and K^1 its Hilbert class field and K^n the Hilbert class field of K^{n-1}. Is it true that this tower of field extensions $K \subset K^1 \subset K^2 \subset \dots$ stabilises, i.e. eventually K^n has class number one? The answer is negative as was shown in 1964 by Golod and Shafarevich.

Theorem 6.2.9. *Let $d = p_1 \dots p_N$ with p_i distinct primes $\equiv 1 \pmod 4$ and $N \geq 6$, then the class field tower of $K = \mathbb{Q}(\sqrt{-d})$ is infinite.*

Proof. This proof idea is presented in [21, I.5. Proposition 29]: If the class field tower was finite then the maximal unramified ℓ-extension of K for any prime ℓ would be finite because ℓ-groups are solvable. Let G be a the Galois group of the maximal unramified ℓ-extension of K. Now by 2.8.10, $n = \dim H^1(G, \mathbb{Z}/\ell\mathbb{Z})$ is the number of generators needed to generate G as a pro-ℓ group and $r = \dim H^2(G, \mathbb{Z}/\ell\mathbb{Z})$ is the number of relations between these generators. For G to be finite there should be a lot of relations between the generators of G since otherwise there is not enough cancellation. Indeed the Golod-Shafarevich inequality [21, I. Appendix 2] says that for any finite ℓ-group one has $n^2/4 < r$ which will be more than enough to derive a contradiction.

In our case we set $\ell = 2$, L/K the maximal unramified 2-extension of K and G its Galois group which we assume to be finite. The extensions $K(\sqrt{p_i})/K$ are easily seen to be unramified and so by considering the homomorphisms $\sigma \mapsto \sigma(\sqrt{p_i})/\sqrt{p_i}$ we find $n = \dim H^1(G, \mathbb{F}_2) \geq N$. Moreover, we have exact sequences

$$0 \to \mathcal{O}_L^\times \to \mathbb{U}_L \to \mathbb{U}_L/\mathcal{O}_L^\times \to 0$$
$$0 \to \mathbb{U}_L/\mathcal{O}_L^\times \to C_L \to \mathrm{Cl}(L) \to 0,$$

where $\mathbb{U}_L$ is the set of ideles $x \in \mathbb{I}_L$ such that x_v is a unit for all places v of L. L has no unramified 2-extensions and so the Hilbert class field of L has odd degree over L, thus $\#\,\mathrm{Cl}(L)$ is odd and so by 2.4.11, $H^q(G, \mathrm{Cl}(L)) = 0$ for all $q \geq 1$. The restriction-corestriction argument extends to Tate Cohomology by dimension shifting and so $\hat{H}^q(G, \mathrm{Cl}(L)) = 0$ for all q. Further $\hat{H}^q(L/K, \mathbb{U}_L) = \bigoplus_v \hat{H}^q(L_w/K_v, \mathcal{O}_w) = 0$ since L/K is unramified. Thus the long exact sequence gives us isomorphisms $\hat{H}^q(G, \mathcal{O}_L^\times) \to \hat{H}^{q-1}(G, C_L)$. By Tate's theorem $\hat{H}^{q-1}(G, C_L) \cong \hat{H}^{q-3}(G, \mathbb{Z})$. Setting $q = 0$ we get $\hat{H}^{-3}(G, \mathbb{Z}) \cong \hat{H}^0(G, \mathcal{O}_L^\times)$. Since K is an imaginary quadratic field and $d > 3$ it has 2 units and so $\dim_{\mathbb{F}_2} \hat{H}^0(G, \mathcal{O}_L^\times) \leq 1$. $\hat{H}^{-3}(G, \mathbb{Z})$ is dual to $H^2(G, \mathbb{Q}/\mathbb{Z})$ [19, 3.1.1] and hence also $\dim H^2(G, \mathbb{Q}/\mathbb{Z}) \leq 1$. Now consider the exact sequence $0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Q}/\mathbb{Z} \to 0$. It induces the exact sequence

$$\begin{tikzcd}
H^1(G, \mathbb{Z}/2\mathbb{Z}) \arrow[r] & H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[r] & H^1(G, \mathbb{Q}/\mathbb{Z}) \arrow[dll] \\
H^2(G, \mathbb{Z}/2\mathbb{Z}) \arrow[r] & H^2(G, \mathbb{Q}/\mathbb{Z})[2] \arrow[r] & 0
\end{tikzcd}$$

from which we deduce $n - r + \dim H^2(G, \mathbb{Q}/\mathbb{Z})[2] \geq 0$ and hence $r \leq n + 1$. But for $n \geq 6$ this contradicts the Golod-Shafarevich inequality $n^2/4 < r$. □

6.3 The Power Residue Symbol

The sequel is based on the exercises in [5] starting at page 348. The goal is to make the abstract formulation of class field theory more concrete by deriving the reciprocity law for mth powers which for $m = 2$ reduces to quadratic reciprocity. Like the examples we saw in the last section this approach is based on the fact that the global Artin map factors through the idèle class group.

Let K be a number field containing the mth roots of unity μ_m. Let S be the set of infinite primes of K together with the primes dividing m. Moreover, for $a_1, \ldots, a_r \in K^\times$ let $S(a_1, \ldots, a_r)$ be the set of primes in S together with those v such that $v(a_i) \neq 0$ for some i. For $a \in K^\times$ and $\mathfrak{b} \in I^{S(a)}$, where $I^{S(a)}$ denotes the group of fractional ideals of K coprime to the elements of $S(a)$, define the mth power residue symbol $\left(\frac{a}{\mathfrak{b}}\right)_{K,m}$ by

$$\mathrm{Frob}_{L/K}(\mathfrak{b})(\sqrt[m]{a}) = \left(\frac{a}{\mathfrak{b}}\right)_{K,m} \sqrt[m]{a}, \tag{3}$$

where $L = K(\sqrt[m]{a})$ and $\mathrm{Frob}_{L/K} : I^{S(a)} \to \mathrm{Gal}(L/K)$ maps unramified primes to their Frobenius elements. This is well-defined since $K \subset L$ is an abelian extension. If K and m are clear from context, we omit them from the notation. Raising both sides of (3) to the mth power we see that $\left(\frac{a}{\mathfrak{b}}\right) \in \mu_m$ and moreover it is independent of the choice of $\sqrt[m]{a}$ since $\mathrm{Gal}(L/K)$ acts trivially on μ_m. It follows directly from (3) that whenever it is defined, the power residue symbol is multiplicative in both arguments.

Lemma 6.3.1 (Generalised Euler Criterion)**.** *Fix $a \in K^\times$ and let $\mathfrak{q} \notin S(a)$, then $m \mid (N\mathfrak{q} - 1)$ and*

$$\left(\frac{a}{\mathfrak{q}}\right)_{K,m} \equiv a^{\frac{N\mathfrak{q}-1}{m}} \pmod{\mathfrak{q}}$$

and $\left(\frac{a}{\mathfrak{q}}\right)$ is uniquely determined by this congruence. In particular the symbol only depends on the class of a modulo $\mathfrak{q}$.

Proof. Since $\mathfrak{q} \notin S$ we have $\mathfrak{q} \nmid m$ and so there are m distinct mth roots of unity in $\mathcal{O}_K/\mathfrak{q}$ since $x^m - 1$ is a separable polynomial modulo $\mathfrak{q}$. This shows $m \mid (N\mathfrak{q} - 1)$.

By assumption a is integral in $K_\mathfrak{q}$. Let $\alpha^m = a$, $L = K(\alpha)$ and $\mathfrak{Q}$ a prime of L lying over $\mathfrak{q}$, then

$$\left(\frac{a}{\mathfrak{q}}\right) \alpha = \mathrm{Frob}_{L/K}(\mathfrak{q})(\alpha) \equiv \alpha^{N\mathfrak{q}} \pmod{\mathfrak{Q}}$$

by definition of the Frobenius. If $\alpha \in \mathfrak{Q}$, then $a = \alpha^m \in \mathfrak{Q} \cap K = \mathfrak{q}$ which contradicts $\mathfrak{q} \notin S(a)$. Hence α is invertible modulo $\mathfrak{Q}$ and dividing by α yields the desired congruence. Moreover this determines the symbol because $\mathcal{O}_K/\mathfrak{q}$ contains m distinct mth roots of unity. □

Lemma 6.3.2. *Fix $a \in K^\times \cap \mathcal{O}_K$, let $\mathfrak{b} \in I^S$ be integral (i.e. $\mathfrak{b}$ is coprime to m) and $\zeta \in \mu_m$, then*

$$\left(\frac{\zeta}{\mathfrak{b}}\right)_{K,m} = \zeta^{\frac{N\mathfrak{b}-1}{m}}.$$

Proof. We will apply the generalised Euler criterion 6.3.1 and multiplicativity of the power residue symbol. Let $\mathfrak{q}$ be a prime dividing $\mathfrak{b}$, then $\mathfrak{q}$ is coprime to m and as above, the restriction of μ_m to $\mathcal{O}_K/\mathfrak{q}$ is injective and so the congruence in 6.3.1 is actually equality in our situation.

For $\mathfrak{p} \mid \mathfrak{b}$ write $N\mathfrak{p} = 1 + r_\mathfrak{p} m$. Using multiplicativity of the power residue symbol and lemma 6.3.1 we conclude

$$\left(\frac{\zeta}{\mathfrak{b}}\right) = \prod_{\mathfrak{p}} \zeta^{v_{\mathfrak{p}}(\mathfrak{b}) r_{\mathfrak{p}}}.$$

Moreover, we have

$$N\mathfrak{b} = \prod_{\mathfrak{p}} (1 + r_{\mathfrak{p}} m)^{v_{\mathfrak{p}}(\mathfrak{b})} \equiv 1 + m \sum_{\mathfrak{p}} r_{\mathfrak{p}} v_{\mathfrak{p}}(\mathfrak{b}) \pmod{m^2}$$

which completes the proof. □

To be able to use the theorems of class field theory we relate the power residue symbol to the Hilbert symbol. For a place v of K we will write $(\cdot,\cdot)_v$ for the mth Hilbert symbol $(\cdot,\cdot)_{K_v,m}$.

Lemma 6.3.3. *Fix $a \in K^\times, b \in K_{\mathfrak{p}}^\times$ and $\mathfrak{p} \notin S(a)$, then*

$$(a,b)_{\mathfrak{p}} = \left(\frac{a}{\mathfrak{p}}\right)_{K,m}^{v_{\mathfrak{p}}(b)}.$$

Proof. Applying 5.2.4 with the Kummer character of a we get

$$\chi_a(\phi_{\mathfrak{p}}(b)) = \mathrm{inv}_K(b \cup \delta^2 a).$$

The lemmas 2.5.8 and 2.5.10 imply that $\chi_a(\phi_{\mathfrak{p}}(b)) = \mathrm{inv}_K(\delta a \cup \delta b) = (a,b)_{\mathfrak{p}}$ and thus $(a,b)_{\mathfrak{p}} \sqrt[m]{a} = \phi_{\mathfrak{p}}(b)(\sqrt[m]{a})$. Now it suffices to check that $\phi_{\mathfrak{p}}(b) = \mathrm{Frob}_{K(\sqrt[m]{a})/K}(\mathfrak{p})^{v_{\mathfrak{p}}(b)}$ but this follows since $\mathfrak{p} \notin S(a)$ is unramified in $K(\sqrt[m]{a})$. □

For $a, b \in K^\times$ we define

$$\left(\frac{a}{b}\right)_{K,m} := \left(\frac{a}{(b\mathcal{O}_K)^{S(a)}}\right)_{K,m},$$

where $(b\mathcal{O}_K)^{S(a)}$ is obtained from the fractional ideal $b\mathcal{O}_K$ by throwing out all the prime factors from $S(a)$.

Proposition 6.3.4. *For $a, b \in K^\times$ we have the reciprocity law*

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p} \in S(a) \cap S(b)} (b,a)_{\mathfrak{p}}.$$

Proof. By lemma 6.3.3 we have

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p} \notin S(b)} (a,b)_{\mathfrak{p}} \prod_{\mathfrak{p} \notin S(a)} (b,a)_{\mathfrak{p}}^{-1}.$$

The fundamental exact sequence 6.1.6 shows that the product of the Hilbert symbols over all places equals 1. Applying this and skew-symmetry 2.5.8 we obtain

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right)^{-1} = \prod_{\mathfrak{p}\in S(b)} (a,b)_{\mathfrak{p}}^{-1} \prod_{\mathfrak{p}\in S(a)} (b,a)_{\mathfrak{p}} = \left(\prod_{\mathfrak{p}\in S(a)\cap S(b)} (b,a)_{\mathfrak{p}}\right)\left(\prod_{\mathfrak{p}\in S(a)\cup S(b)} (b,a)_{\mathfrak{p}}\right).$$

By lemma 6.3.3, the product over $S(a)\cup S(b)$ includes all nontrivial factors and hence equals 1, again by the fundamental exact sequence. □

Corollary 6.3.5 (Quadratic Reciprocity). *Let p, q be distinct odd primes in $\mathbb{N}$, then*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right),$$

where $\left(\frac{p}{q}\right)$ is the classical Legendre symbol.

Proof. Let $K=\mathbb{Q}$, $m=2$ and p, q be distinct odd primes, then

$$\left(\frac{p}{q}\right)_{\mathbb{Q},2} = (p,q)_2(p,q)_\infty \left(\frac{q}{p}\right)_{\mathbb{Q},2}.$$

$(p,q)_\infty = 1$ since $p>0$ and $q>0$. Moreover, $(p,q)_2 = 1$ if and only if the equation $x^2-py^2-qz^2=0$ has a non-trivial solution in $\mathbb{Q}_2$. Using Hensel's lemma and reduction mod 8 one can check that $(p,q)_2=-1$ if $p\equiv q\equiv -1 \pmod 4$ and $(p,q)_2=1$ otherwise. Finally, by 6.3.1 the second power reside symbol is just the Legendre symbol. □

6.4 Application to Fermat's Last Theorem

Let p be an odd prime number and denote by $\mathrm{FLT}_1(p)$ and $\mathrm{FLT}(p)$ the following properties

$$\mathrm{FLT}(p): \forall x,y,z\in\mathbb{Z}: x^p+y^p=z^p \implies xyz=0;$$
$$\mathrm{FLT}_1(p): \forall x,y,z\in\mathbb{Z}: x^p+y^p=z^p \implies p\mid xyz.$$

In [15] it is shown that $\neg\,\mathrm{FLT}_1(p)$ implies that p belongs to several restrictive classes of primes. For example that p is a Wieferich prime, i.e. that $2^{p-1}\equiv 1 \pmod{p^2}$. The only known Wieferich primes are 1093 and 3511 [1]. Using the theory developed in the previous section we are able to give this proof.

Let ζ be a primitive pth root of unity, $K=\mathbb{Q}(\zeta)$ and $S=\{\mathfrak{p}\}$, where $\mathfrak{p} = (\zeta-1)\mathcal{O}_K$, so that $p\mathcal{O}_K=\mathfrak{p}^{p-1}$ and p is the only rational prime which is ramified in K. To apply the theory of the power residue symbol to this setup we will need to compute some Hilbert symbols and here is our main tool for this:

Lemma 6.4.1. *Let L be a local field containing the mth roots of unity and $a, b \in L^\times$ such that $a+b$ is an mth power, then $(a,b)_{L,m} = 1$.*

Proof. We show that b is a norm from $L(\sqrt[m]{a})$. Indeed let $\alpha^m = a$ and $\mu_d \subset \mu_m$ the image of $\mathrm{Gal}(L(\sqrt[m]{a})/L) \hookrightarrow \mu_m : \sigma \mapsto \sigma(\alpha)/\alpha$. Let $\zeta_1, \dots, \zeta_r$ be coset representatives of μ_d in μ_m and $x^m = a+b$, then $b = x^m - \alpha^m = \prod_{i=1}^r N(x - \zeta_i\alpha)$. □

Lemma 6.4.2. *Let $x, y, z \in \mathbb{Z}$ pairwise coprime such that $x^p + y^p = z^p$ and $p \nmid yz$. Let n be coprime to p and z, then the pth power residue symbol satisfies $\left(\frac{x+y\zeta}{n}\right) = \left(\frac{\zeta}{n}\right)^{y/z}$.*

Proof. This is Lemma 1 in [15] and we give the same proof with a bit more details. By assumption n is coprime to z and hence to $z^p = x^p - (-y)^p = \prod_{k=1}^p (x + y\zeta^k)$. As n is also coprime to p this shows that $(n\mathcal{O}_K)^{S(x+y\zeta)} = n\mathcal{O}_K$. Moreover ζ is a unit, so $S(\zeta) = S = \{\mathfrak{p}\}$ and thus

$$\left(\frac{x+y\zeta}{n}\right)\left(\frac{\zeta}{n}\right)^{-y/z} = \left(\frac{x+y\zeta}{n\mathcal{O}_K}\right)\left(\frac{\zeta}{n\mathcal{O}_K}\right)^{-y/z} = \left(\frac{\alpha}{n\mathcal{O}_K}\right) = \left(\frac{\alpha}{n}\right),$$

where $\alpha = (x+y\zeta)\zeta^{-y/z}$. Hence it remains to show that $\left(\frac{\alpha}{n}\right) = 1$.

$\alpha\mathcal{O}_K = (x+y\zeta)\mathcal{O}_K$ is a pth ideal power. To see this observe that for pth roots of unity $\zeta \neq \zeta'$, any common prime factor of $(x+y\zeta)\mathcal{O}_K$ and $(x+y\zeta')\mathcal{O}_K$ also divides

$$(x+y\zeta) - (x+y\zeta') = y(\zeta - \zeta')\mathcal{O}_K = y\mathfrak{p}$$

and hence does not divide z by assumption. Consequently the formula $(z\mathcal{O}_K)^p = \prod_{k=1}^p (x+y\zeta^k)\mathcal{O}_K$ shows that each $x + y\zeta^k$ is a pth ideal power.

The multiplicativity of the power residue symbol in the second factor now shows $\left(\frac{n}{\alpha}\right) = 1$. The reciprocity law 6.3.4 in our case reads

$$\left(\frac{\alpha}{n}\right)\left(\frac{n}{\alpha}\right)^{-1} = \prod_{\mathfrak{q} \in S(n) \cap S(\alpha)} (n, \alpha)_\mathfrak{q} = (n, \alpha)_\mathfrak{p},$$

where the second equality holds because $S = S(n) \cap S(\alpha)$, as any prime dividing α also divides z which is coprime to n. Thus it remains to show that $(n, \alpha)_\mathfrak{p} = 1$.

To compute this Hilbert symbol it turns out to be useful to know that $\alpha^{p-1} \equiv 1 \pmod{\mathfrak{p}^2}$. Observe that $p \in \mathfrak{p}^{p-1} \subset \mathfrak{p}^2$ and

$$\begin{aligned} \alpha = ((x+y) + y(\zeta - 1))\zeta^{-y/z} &\equiv (z + y(\zeta-1))\zeta^{-y/z} \\ &\equiv z \cdot (1 + (\zeta - 1))^{y/z}\zeta^{-y/z} \equiv z \pmod{\mathfrak{p}^2} \end{aligned}$$

and so $\alpha^{p-1} \equiv z^{p-1} \equiv 1 \pmod{\mathfrak{p}^2}$. Now write $\alpha^{p-1} = 1 - \beta$ with $\beta \in \mathfrak{p}^2$ and $n^{p-1} = 1 - \gamma$ with $\gamma \in \mathfrak{p}^{p-1} = p\mathcal{O}_K$.

We will show that $1-\beta\gamma$ is a pth power in $K_{\mathfrak{p}}$. Then 6.4.1 shows that $(1-\gamma, \gamma-\gamma\beta) = 1$ and so

$$(n, \alpha) = (n^{p-1}, \alpha^{p-1}) = (1-\gamma, 1-\beta) = (1-\gamma, 1-\beta)(1-\gamma, \gamma) = (1-\gamma, \gamma-\gamma\beta) = 1.$$

So let us show that $1-\beta\gamma$ is a pth power in $K_{\mathfrak{p}}$. Let $\lambda = 1-\zeta$ and consider the equation $(1+\lambda x)^p = 1-\beta\gamma$. This is equivalent to

$$\sum_{k=1}^{p} \binom{p}{k} \lambda^{k-p} x^k = -\beta\gamma\lambda^{-p}. \tag{4}$$

Note that

$$\frac{p}{\lambda^{p-1}} = \prod_{l=1}^{p-1} \frac{1-\zeta^l}{1-\zeta} = \prod_{l=1}^{p-1} (1+\zeta+\cdots+\zeta^{l-1}) \equiv (p-1)! \equiv -1 \pmod{\mathfrak{p}}$$

and so (4) modulo $\mathfrak{p}$ becomes $x^p - x = 0$ and by Hensel's lemma there exists $x \in K_{\mathfrak{p}}$ such that $(1+\lambda x)^p = 1-\beta\gamma$, as required. □

Now we are ready to show

Theorem 6.4.3. *Suppose p is an odd prime such that there exists $x, y, z \in \mathbb{Z}$ with $x^p + y^p = z^p$ and $p \nmid xyz$, then $2^{p-1} \equiv 1 \pmod{p^2}$.*

Proof. We can assume that x, y, z are pairwise coprime and after rearranging the equation that y is even and that z and x are odd. Now the conditions of lemma 6.4.2 are satisfied for $n = 2$. As above, $x + y\zeta$ is coprime to 2 and $\mathfrak{p}$ and so

$$\left(\frac{x+y\zeta}{2\mathcal{O}_K}\right) = \left(\frac{x+y\zeta}{2}\right) = \left(\frac{\zeta}{2}\right)^{y/z} = \left(\frac{\zeta}{2\mathcal{O}_K}\right)^{y/z}.$$

The goal is to show that

$$\left(\frac{\zeta}{2\mathcal{O}_K}\right) = 1,$$

because then 6.3.1 shows

$$1 = \zeta^{\frac{2^{p-1}-1}{p}}$$

which implies that $2^{p-1} \equiv 1 \pmod{p^2}$.

By 6.3.1 the power residue symbol $\left(\frac{x+y\zeta}{2\mathcal{O}_K}\right)$ only depends on the class of $x + y\zeta$ modulo 2. Thus

$$1 = \left(\frac{1}{2\mathcal{O}_K}\right) = \left(\frac{x+y\zeta}{2\mathcal{O}_K}\right) = \left(\frac{\zeta}{2\mathcal{O}_K}\right)^{y/z}$$

and since $y/z \not\equiv 0 \pmod{p}$, we have $\left(\frac{\zeta}{2\mathcal{O}_K}\right) = 1$. □

If $2p \mid x$, then we have $y/z \equiv 1 \pmod p$ since $x \equiv z - y \equiv 0 \pmod p$. Thus

$$\left(\frac{\zeta}{2\mathcal{O}_K}\right) = \left(\frac{x + y\zeta}{2\mathcal{O}_K}\right) = \left(\frac{\zeta}{2\mathcal{O}_K}\right)^{y/z}$$

doesn't give us any information, so the assumption $p \nmid xyz$ is essential.

7 The Structure of Absolute Galois Groups

In this final section we indicate some questions in Galois Cohomology which have been studied more recently. The classical inverse Galois problem for a field k asks which finite groups appear as Galois groups of Galois extensions of k. Historically, the particular case $k = \mathbb{Q}$ has sparked a lot of interest. One of the major results in this area is a theorem due to Shafarevich which states that any finite solvable group appears as a Galois group of a finite extension of $\mathbb{Q}$, see [19, Chapter IX] for the proof (which is very involved).

More generally, one can ask which profinite groups appear as absolute Galois groups of some field. This is a widely open problem but some restrictions on such groups are known. For example a classical theorem by Artin-Schreier shows that all finite subgroups of an absolute Galois group are of order at most 2. Another strong restriction on the structure of absolute Galois groups is the Bloch-Kato conjecture, which is now a theorem due to Voevodsky. Beyond that it has recently been shown that all triple Massey products vanish in Galois Cohomology with $\mathbb{F}_p$ coefficients [18] which has some consequences for absolute Galois groups, as well.

7.1 The Bloch-Kato Conjecture

Let k be a field. Then we define the Milnor K-groups as $K_0(k) = \mathbb{Z}$, $K_1(k) = k^\times$ and when $n \geq 2$

$$K_n(k) = k^\times \otimes_{\mathbb{Z}} \cdots \otimes_{\mathbb{Z}} k^\times / \langle a_1 \otimes \cdots \otimes a_n : a_i + a_j = 1 \text{ for some } i \neq j \rangle$$

Fix an integer ℓ which is invertible in k and let μ_ℓ be the ℓth roots of unity in a separable closure of k. Then the Kummer sequence gives us an isomorphism $\partial^1 : K_1(k)/\ell = k^\times/(k^\times)^\ell \to H^1(k, \mu_\ell)$. Together with an isomorphism $\mu_\ell^{\otimes n} \to \mu_\ell$, the cup product induces a map $\partial^n : (k^\times)^{\otimes n} \to H^n(k, \mu_\ell) : x_1 \otimes \cdots \otimes x_n \mapsto \partial^1(x_1) \cup \cdots \cup \partial^1(x_n)$. Similarly to lemma 6.3.3 one can show that ∂^n factors through $K_n(k)/\ell$ [9, Proposition 4.6.1]. Now we can formulate the Bloch-Kato conjecture:

Theorem 7.1.1. *Let k be a field and ℓ an integer coprime to the characteristic of k, then the map $\partial^n : K_n(k)/\ell \to H^n(k, \mu_\ell)$ is an isomorphism for $n \geq 1$.*

Proof. The case $n = 2$ is the Merkurjev-Suslin theorem [9]. The general case was finally proven by Voevodsky [25]. □

Corollary 7.1.2. *For k and ℓ as in the theorem, the cohomology ring $H^*(k, \mu_\ell)$ is generated by elements in degrees* 1 *and* 0 *and the relations are generated by relations of degree* 2*.*

Theorem 7.1.1 is a fundamental result on the structure of the Galois Cohomology of a field and has many implications, for example for central simple algebras [9, Theorem 2.5.7]. It is also used in [12] to bound $\mathrm{cd}_p(k)$ in terms of the diophantine dimension of k, which is the least r such that k has property C_r. Furthermore we can recover the Artin-Schreier theorem of which there is an elementary proof [6] but which is hard to remember.

Corollary 7.1.3 (Artin-Schreier theorem)**.** *Let k be a field and G_k its absolute Galois group, then every finite subgroup of G_k has order at most 2.*

Proof. Let ℓ be an odd prime different from the characteristic of k. Suppose $G = G_k$ has an element σ of order ℓ. Let C be a separable closure of k, then C/C^σ is a Galois extension with Galois group $H = \langle\sigma\rangle$. The degree $C^\sigma(\mu_\ell)/C^\sigma$ divides $\ell - 1$ and hence is coprime to ℓ and $\mu_\ell \subset C^\sigma$. H is cyclic and both $N : \mu_\ell \to \mu_\ell$ and $(1-\sigma) : \mu_\ell \to \mu_\ell$ are the zero map, so $H^1(H, \mu_\ell) \cong \mathbb{F}_\ell$ and $H^2(H, \mu_\ell) \cong \mathbb{F}_\ell$ by 2.3.2. The cup product is an antisymmetric bilinear map $\mathbb{F}_\ell \times \mathbb{F}_\ell \to \mathbb{F}_\ell$. Since $\ell > 2$, the only such map is the zero map. But then $H^2(H, \mu_\ell)$ is not generated by degree 1 elements, contradicting the Merkurjev-Suslin theorem.

If $\mathrm{char}(k) = p$ and G has an element σ of order p, then the short exact sequence

$$0 \to \mathbb{F}_p \to C \xrightarrow{x^p - x} C \to 0$$

induces an exact sequence

$$H^1(C^\sigma, C) \to H^2(C^\sigma, \mathbb{F}_p) \to H^2(C^\sigma, C),$$

so by additive Hilbert 90, $H^2(C^\sigma, \mathbb{F}_p) = 0$. On the other hand $\mathrm{Gal}(C/C^\sigma) \cong \langle\sigma\rangle \cong \mathbb{F}_p$ and $H^2(\mathbb{F}_p, \mathbb{F}_p) = \mathbb{F}_p$ which is a contradiction.

Consequently any finite subgroup of G must be a 2-group and if $\mathrm{char}(k) = 2$, then there are no nontrivial finite subgroups by the argument above.

If K is a field of characteristic $\neq 2$ such that $[C : K] = 2$, then -1 is not a square in K. Suppose otherwise and let $C = K(\beta)$ with $\beta^2 \in K$ and $\beta \notin K$. Then since C is algebraically closed, there are $x, y \in K$ such that $(x + y\beta)^2 = \beta$. Hence $x^2 + \beta^2 y^2 = 0$ and so $\beta = \pm xi/y \in K$ where $i \in K$ is a square-root of -1. Absurd.

Now suppose $H < G$ is a finite subgroup, then $|H|$ is a power of 2 and in particular H is solvable. Thus if $|H| > 2$, there are fields $E \subset K \subset C$ such that $[C : K] = [K : E] = 2$. Then $i \notin K$ shows that $[E(i) : E] = [C : E(i)] = 2$ but by the observation above, $i \notin E(i)$ which is a contradiction. Hence all finite subgroups of G have order at most 2. □

References

[1] Oeis foundation inc. (2019), the on-line encyclopedia of integer sequences, `http://oeis.org/A001220`.

[2] J. Ax. Proof of some conjectures on cohomological dimension. *Proceedings of the American Mathematical Society*, 16(6):1214–1221, 1965.

[3] N. Bourbaki. *Topologie generale.* Bourbaki, Nicolas. Elements de mathematique. 1st ed. 2007. edition, 2007.

[4] H. Cartan and S. Eilenberg. *Homological Algebra.* Princeton mathematical series ; 19. Oxford University Press ; Princeton University Press, London : Princeton ;, 1956.

[5] J. Cassels and A. Froehlich. *Algebraic number theory.* London Mathematical Society, London, 1967.

[6] K. Conrad. The artin-schreier theorem, 2019. Accessed 07/09/2019 at `https://kconrad.math.uconn.edu/blurbs/galoistheory/artinschreier.pdf`.

[7] K. Conrad. Galois descent, 2019. Accessed 07/09/2019 at `https://kconrad.math.uconn.edu/blurbs/galoistheory/galoisdescent.pdf`.

[8] D. A. Cox. *Primes of the form $x^2 + ny^2$ fermat, class field theory, and complex multiplication / David A. Cox.* Pure and applied mathematics: a wiley series of texts, monographs and tracts. John Wiley & Sons Inc, Hoboken (NJ), 2nd ed. edition, 2013.

[9] P. Gille and T. Szamuely. *Central Simple Algebras and Galois Cohomology.* Cambridge Studies in Advanced Mathematics ; 101. 2006.

[10] A. Grothendieck. Sur quelques points d'algèbre homologique. *Tohoku Mathematical Journal, Second Series*, 9(2):119–183, 1957.

[11] G. Hochschild and J. P. Serre. Cohomology of group extensions. *Transactions of the American Mathematical Society*, 74(1):110–134, 1953.

[12] D. Krashen and E. Matzri. Diophantine and cohomological dimensions. *Proceedings of the American Mathematical Society*, 143(7):2779–2788, 2015.

[13] S. Lang. On quasi algebraic closure. *Annals of Mathematics*, 55(2):373–390, 1952.

[14] S. Lang and J. Tate. Principal homogeneous spaces over abelian varieties. *American Journal of Mathematics*, 80(3):659–684, 1958.

[15] H. Lenstra and P. Stevenhagen. Class field theory and the first case of fermat's last theorem. *Modular forms and Fermat's last theorem*, 1997.

[16] J. Milne. Class field theory (v4.02), 2013. Accessed 07/09/2019 at `www.jmilne.org/math/`.

[17] J. S. Milne. Algebraic number theory (v3.07), 2017. Accessed 07/09/2019 at `www.jmilne.org/math/`.

[18] J. Minac and N. D. Tan. Triple massey products vanish over all fields. *Journal of the London Mathematical Society*, 94(3):909–932, 2016.

[19] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*, volume 323 of *Grundlehren der mathematischen Wissenschaften*. Springer Berlin Heidelberg, Berlin, Heidelberg, second edition edition, 2008.

[20] J. P. Serre. *Local fields*. Graduate texts in mathematics ; 67. Springer-Verlag, New York, 1979.

[21] J. P. Serre. *Galois cohomology*. Springer monographs in mathematics. Springer, Berlin, corrected 2nd print. edition, 2002.

[22] . Silverman, Joseph H. The arithmetic of elliptic curves, 2009.

[23] A. Sutherland. The Kronecker-Weber theorem. Accessed 07/09/2019 at `http://math.mit.edu/classes/18.785/2015fa/LectureNotes19.pdf`.

[24] R. Vakil. Foundations of algebraic geometry, 2017. Accessed 07/09/2019 at `http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf`.

[25] V. Voevodsky. On motivic cohomology with $\mathbb{Z}/\ell$-coefficients. *Annals of Mathematics*, 174(1):401–438, 2011.

[26] P. Webb. *A Course in Finite Group Representation Theory*. Cambridge University Press, 2016.

[27] A. Weil. The field of definition of a variety. *American Journal of Mathematics*, 78(3):509–524, 1956.

[28] A. Weil. *Basic Number Theory*. Springer Berlin Heidelberg, Berlin, Heidelberg, 1995.

[29] E. Witt. Verlagerung von Gruppen und Hauptidealsatz. *Proceedings of the International Congress of Mathematicians*, 2, 1954.