Distribution Agreement

Signature:

______________________________________ _____________

Yazan Alamoudi Date

The Hasse norm theorem and a local-global principle for multinorms

By

Yazan Alamoudi
Master of science

Mathematics

Raman Parimala, Ph.D.
Advisor

Suresh Venapally, Ph.D.
Committee Member

David Zureick-Brown , Ph.D.
Committee Member

Accepted:

Lisa A. Tedesco, Ph.D.
Dean of the James T. Laney School of Graduate Studies

Date

The Hasse norm theorem and a local-global principle for multinorms

By

Yazan Alamoudi
B.A., UC Berkeley, CA, 2018

Advisor: Raman Parimala, Ph.D.

An abstract of
A thesis submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of science
in Mathematics
2021

Abstract

The Hasse norm theorem and a local-global principle for multinorms
By Yazan Alamoudi

While a local-global principle for norms from cyclic extensions of number fields is the classical Hasse Norm Theorem, such a local-global principle fails for non cyclic extensions in general. There has been a host of results in the direction of a local-global principle for multinorms, namely norms from a finite product of finite separable field extensions, the so-called étale algebras. In this thesis, we prove the following.

Theorem:
Let $E|k$ be a dihedral extension of degree $2n$. Let $E_i, 1 \leq i \leq n$ be the n distinct subextensions of E of degree n which are fixed fields under the reflections. Let $L = \prod_{1\leq i\leq n} E_i$ and $N_{L/k}$ the norm from the étale algebra L to k. Then an element $c \in k$ is a value of $N_{L/k}$ if it is locally a norm at all places of k.

The proof is via the use of the Hasse norm theorem. We give an exposition of some of the relevant class field theory results leading to the Hasse Norm Theorem in the thesis. In addition, we also prove a weak approximation result as a consequence of the above theorem.

The Hasse norm theorem and a local-global principle for multinorms

By

Yazan Alamoudi
B.A., UC Berkeley, CA, 2018

Advisor: Raman Parimala, Ph.D.

A thesis submitted to the Faculty of the
James T. Laney School of Graduate Studies of Emory University
in partial fulfillment of the requirements for the degree of
Master of science
in Mathematics
2021

Acknowledgments

I would like to first thank my family for supporting me through this journey. I would also like to thank my advisor professor Parimla for helping me throughout this process.

I would also like to acknowledge that I used the ”Emory Laney Graduate School Dissertation Template” posted on Overleaf by Blair J. Rossetti.

Contents

Chapter 1

Introduction

1.1 Setting and motivation

We begin with a general setting.

Let k be a number field and let Ω be the set of places of k. For $v \in \Omega$, let k_v be the completion of k at v. Let X be a variety defined over k. One is interested in the set of rational points. Such questions could be the existence of rational and how many rational points are there. We have an inclusion $X(k) \hookrightarrow X(k_v)$ for every $v \in \Omega$. A natural question is the following. If we have that $X(k_v) \neq \emptyset$ for every $v \in \Omega$, does it follow that $X(k_v)$ is non Empty? Such an implication would be interesting since solving for rational points of X over k_v is somewhat easier because of things like Hensel's Lemma.

Unfortunately, we do not always have a Hasse principle for an arbitrary variety. In fact, there are genus one curves to which this principle fails. Therefore we would like to restrict ourselves with a more specific class.

One class we could look at are principal homogeneous spaces under connected linear algebraic groups.

More specifically, let G be a connected linear algebraic group defined over a number field K. Let X be a principal homogeneous space under G, i.e., there is an action

$$G \times X \xrightarrow{m} X$$

such that the action

$$G(\bar{k}) \times X(\bar{k}) \to X(\bar{k})$$

is simply transitive.

However, upon examination, we see that even in this case the Hasse principle is not always true.

For example, let T be the norm 1 torus associated to the extension $\mathbb{Q}(\sqrt{13}, \sqrt{17})$ over $\mathbb{Q}$. Then the norm equation $N_{\mathbb{Q}(\sqrt{13},\sqrt{17})|\mathbb{Q}}(x) = 25$ defines a principal homogeneous space X_λ under T. Then X admits a point over K_v for every place $v \in \Omega$ but does not admit a global point.

However, if $L|K$ is a cyclic extension of number fields and $T_{L|K}$ is the associated norm one torus, then the Hasse principle holds for principle homogeneous spaces under $T_{L|K}$ so that if an element is a norm everywhere locally then it is a norm globally.

In this thesis we present an exposition of a proof of the Hasse norm theorem and extend some aspects of it to discuss multinorm equations. More specifically, for a dihedral extension $E|k$, let $L = \prod_{1 \leq i \leq n} E_i$ where E_i are the fields fixed by a reflection. We will prove that a Hasse principal holds for the multinorm equation $N_{L|k}(x) = \lambda$ for $\lambda \in k^\times$. We also prove a related weak approximation result.

This question was related to a study of Parimala and Suresh related to reduced Whitehead Groups. Many other questions related multinorms have been studied in the field. One example is a paper[1] by Eva Bayer-Fluckiger, Ting-Yu Lee, and Raman Parimala which constructs obstructions to the Hasse principle for multinorm equations.

Interestingly, the Hasse principle for multinorms from $L|k$ reduces to the Hasse principle for norms coming from cyclic extensions which is characterized by the Hasse norm theorem. We will give an exposition of the related class field theory to prove the Hasse norm theorem.

1.2 Structure of paper

The thesis is structured as follows. Chapters two to five are expositions of relevant notions of class field theory leading to the Hasse norm theorem. They are meant to be somewhat self contained so as to require only basic algebraic number theory and some background in group cohomology which can be found in chapter two of Milne's notes [5]. The last chapter is an application to multinorm equations.

In the last chapter we will introduce the multinorm equation associated to a certain étale algebra. We prove a Hasse principle for a multinorm equation we associate to a dihedral extension. We also prove as a consequence a weak approximation result.

Chapter 2

Some results on the cohomology of groups

In this chapter we will follow Kedlaya [3] and Milne [5]. This chapter should be supplemented by chapter 2 of Milne's notes [5].

2.1 Homology, cohomology and Tate groups

In this section we recall some basic results from the cohomology of groups.

Definition. Let G be a group. A G-module M is a module over $\mathbb{Z}[G]$.

We start by defining the Tate cohomology group. This is an important sequence of groups for our study.

Definition. For a finite group G the augmentation ideal $I_G \subseteq \mathbb{Z}[G]$ is defined as

$$I_G = \{\sum_{\sigma\in G} n_\sigma \sigma : \sum_{\sigma\in G} n_\sigma = 0\}$$

.

Let G be a finite group, M a G-module and M^G the G invariant submodule. For $n \geq 1$ let $H^n(G,M)$ and $H_n(G,M)$ be the cohomology and homology groups for the G-module M. For $x \in M$ define $N_G(x) = \sum_{\sigma \in G} \sigma(x)$. The norm map induces a homomorphism $N_G : H_0(G,M) \to H^0(G,M)$. Then the Tate cohomology groups, denoted $\hat{H}^n$ are defined as follows:

- $\hat{H}^n(G,M) = H^n(G,M)$ if $n > 0$
- $\hat{H}^0(G,M) = M^G/N_G(M)$
- $\hat{H}^{-1}(G,M) = \ker(N_G)/I_G M$
- $\hat{H}^n(G,M) = H_{-n-1}(G,M)$ if $n \leq -2$.

We now introduce a computationally useful construction.

Definition. Let M be a G-module. The group $C^n(G,M)$ of inhomogeneous n-cochains of G with values in M is the group of all maps $\phi : G^n \to M$. Here we define $G^0 = \{1\}$ from which we see that $C^0(G,M) = M$.

Define the maps

$$d^n : C^n(G,M) \to C^{n+1}(G,M)$$

by $(d^n\phi)(g_1, \cdots, g_{n+1}) =$

$$g_1\phi(g_2, \cdots, g_{n+1}) + \sum_{i=1}^{n} (-1)^i \phi(g_1, \cdots, g_i g_{i+1}, \cdots, g_{n+1}) + (-1)^{n+1}\phi(g_1, \cdots, g_n).$$

Define $Z^n(G,M) = \mathrm{Ker}(d^n)$ and $B^n(G,M) = \mathrm{Im}(d^{n-1})$ as the groups of **n-cocycles** and **n-coboundaries** respectively. We have the following.

Proposition 2.1.1.

$$H^n(G,M) \simeq \frac{Z^n(G,M)}{B^n(G,M)}.$$

Proof. See [5]. □

For the case $H^1(G, M)$ we have the following explicit description. It can be defined as the set of functions $f : G \to M$ such that $f(\sigma\tau) = \sigma f(\tau) + f(\sigma)$ modulo the set of functions $h_m(\sigma) = m - \sigma m$ for $m \in M$. The first kind of functions will be called **crossed homomorphisms** while the second will be called **principal crossed homomorphisms**.

As a first observation we have the famous Hilbert 90 below.

Theorem 2.1.2 (Hilbert 90)**.** *Let $L|K$ be Galois with $G = G(L|K)$. Then* $|H^1(G, L^\times)| = 1$.

Proof. For this proof we will use the multiplicative notation. Let ϕ be a crossed homomorphism. For $\alpha \in L^\times$ define $\beta = \sum_{\sigma \in G} \phi(\sigma) \cdot \sigma\alpha$. Assume that $\beta \neq 0$. Then $\tau\beta = \phi(\tau)^{-1}\beta$ so that $\phi(\tau) = \frac{\beta}{\tau\beta}$ and ϕ is indeed a principal crossed homomorphism.

It remains to show that there exists a $\alpha \in L^\times$ such that $\beta \neq 0$. This is a consequence of the linear Independence of characters.

□

If $0 \to A \to B \to C \to 0$ is an exact sequence of modules we get the following three long exact sequences.

1- $0 \to H^0(G, A) \to \cdots H^i(G, A) \to H^i(G, B) \to H^i(G, C) \to H^{i+1}(G, A) \cdots$ for $i \geq 0$.

2- $\cdots H_i(G, A) \to H_i(G, B) \to H_i(G, C) \to H_{i-1}(G, A) \cdots \to H_0(G, C) \to 0$ for $i \geq 0$.

3- $\cdots \hat{H}^i(G, A) \to \hat{H}^i(G, B) \to \hat{H}^i(G, C) \to \hat{H}^{i+1}(G, A) \cdots$ for $i \in \mathbb{Z}$.

See [5] for more details.

The Hasse norm theorem concerns cyclic Galois groups. Thus, it makes sense to focus on the case when G is a cyclic group which we now do. It turns out that the

Tate groups exhibit a particularly simple pattern when G is cyclic.

Proposition 2.1.3. *Let G be a cyclic group and M a G-module. Then, there are isomorphisms*

$$\hat{H}^n(G, M) \xrightarrow{\sim} \hat{H}^{n+2}(G, M).$$

The aforementioned isomorphisms are determined by the choice of generator of G.

Proof. Let σ be a generator of G. We have the following exact sequence.

$$0 \to \mathbb{Z} \xrightarrow{n \to \sum_{g \in G} gm} \mathbb{Z}[G] \xrightarrow{\sigma - 1} \mathbb{Z}[G] \xrightarrow{\sigma^i \to 1} \mathbb{Z} \to 0$$

All the groups above are free $\mathbb{Z}$ modules and so is I_G which is the kernel of the map $\sigma^i \to 1$. It follows that we may tensor with M over $\mathbb{Z}$ and still obtain an exact sequence. Thus, the following sequence is exact.

$$0 \to M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to \mathbb{Z}[G] \otimes_{\mathbb{Z}} M \to M \to 0$$

The terms in the middle are just $\mathrm{Ind}_1^G(M)$. Thus all the Tate groups for the middle terms vanish. We get the desired result from the following general fact. If

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \to 0$$

is an exact sequence of G-modules, where the Tate groups for B and C all vanish, then there is an isomorphism $\hat{H}^{r+2}(G, A) \xrightarrow{\sim} \hat{H}^r(G, D)$. This is seen in the following way. First, notice that the exact sequence gives rise to the following two exact sequences.

$$0 \to A \to B \to B/\mathrm{Im}(f) \to 0$$

$$0 \to B/\mathrm{Ker}(g) \to C \to D \to 0$$

But then the long exact sequences on the Tate groups gives

$$\hat{H}^{i+2}(G,A) \simeq \hat{H}^{i+1}(G,B/\mathrm{Im}(f)) \simeq \hat{H}^{i+1}(G,B/\mathrm{Ker}(g)) \simeq \hat{H}^{i}(G,D)$$

as claimed.

□

Another such pattern, when G is cyclic, is summarized in the proposition below

Theorem 2.1.4. *Suppose that* $1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1$ *is an exact sequence of* G*-modules with* G *cyclic. Then, we obtain the following exact hexagon.*

$$\begin{tikzcd}
 & \hat{H}^0(G,A) \arrow[r, "f_1"] & \hat{H}^0(G,B) \arrow[dr, "f_2"] & \\
\hat{H}^{-1}(G,C) \arrow[ur, "f_6"] & & & \hat{H}^0(G,C) \arrow[dl, "f_3"] \\
 & \hat{H}^{-1}(G,B) \arrow[ul, "f_5"] & \hat{H}^{-1}(G,A) \arrow[l, "f_4"] &
\end{tikzcd}$$

Proof. This follows directly from the periodicity of the Tate groups and the long exact sequence in the Tate groups. For a proof that does not use the periodicity nor the long exact sequence, see [7]. □

We now introduce the Herbrand quotient. A quantity that will play a crucial role in many of our arguments.

Definition. Let G be a cyclic group. The Herbrand quotient for a G-module M is the following number provided that its well defined in the sense that both groups in the numerator and denominator are finite.

$$h(M) = \frac{|\hat{H}^0(G,M)|}{|\hat{H}^{-1}(G,M)|}$$

Theorem 2.1.5. *Let G be a cyclic group. If $1 \to A \to B \to C \to 1$ is an exact sequence of G-modules then $h(B) = h(A)h(C)$. Furthermore, if two are well defined the so is the third.*

Proof. (Outline)Let $n_i = |\mathrm{Im}(f_i)|$. Then $h(A) = \frac{n_6 n_1}{n_3 n_4}$, $h(B) = \frac{n_1 n_2}{n_4 n_5}$ and $h(C) = \frac{n_2 n_3}{n_5 n_6}$. The first conclusion follows. To see that second notice that any two of them contain all six variables and hence if two are well defined so is the third. □

When computing $H^i(G, M)$ it will often times be convenient to change G to G' or M to M' possibly having to change both. For the remainder of this section, we introduce two key tools that enable us to do just that. The first is Shapiro's lemma and the second is the inflation restriction exact sequence.

Given a G-modules M and a subgroup $H \leq G$. We can construct an H module as in the following definition.

Definition. Let H be a subgroup of G. Then $\mathrm{Ind}_H^G(M)$ is defined as $M \otimes_{\mathbb{Z}[H]} \mathbb{Z}[G]$. Furthermore, we say that a module is induced if $M = \mathrm{Ind}_e^G(N)$ for some abelian group N.

One notices that $\mathrm{Ind}_H^G(M) = \prod_{g \in G/H} M^g$. We now state a useful result regrading modules of the form discussed in the previous definition.

Theorem 2.1.6 (Shapiro's lemma)**.** *For $H \leq G$ and an H-module M then there are canonical isomorphisms*

$$H^n(G, Ind_H^G(M)) \to H^n(H, M)$$

for all $n \geq 0$

Proof. (Outline) For the case $n = 0$ we have

$$M^H \cong \mathrm{Hom}_H(\mathbb{Z}, M) \cong \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}_H^G(M)) \cong \mathrm{Ind}_H^G(M)^G.$$

Now, notice that if I is an injective H-module, then $\operatorname{Ind}_H^G(I)$ is an injective G-module. Furthermore, Ind_H^G preserves exactness. Therefore, applying Ind_H^G to an injective resolution of N gives an injective resolution of $\operatorname{Ind}_H^G(N)$ from which we get the remaining isomorphisms. □

We call a G-module M **acyclic** if $H^i(G, M) = 0$ of all $i > 0$. It directly follows from Shapiro's lemma that induced modules are acyclic.

We end this section by introducing an exact sequence that will be incredibly useful for us. But first we need to introduce some terms.

Definition. Let M be a G-module and M' be a G'-module. Let $\alpha : G' \to G$ be a homomorphism of groups and $\beta : M \to M'$ be a homomorphism of abelian groups. We say that α and β are compatible if $\beta(\alpha(g)m) = g\beta(m)$.

Proposition 2.1.7. *Let M be a G-module and M' be a G'-module. Let $\alpha : G' \to G$ be a homomorphism of groups and $\beta : M \to M'$ be a homomorphism of abelian groups. If α and β are compatible then they define homomorphisms*

$$H^i(G, M) \to H^i(G', M').$$

Proof. See [5]. □

Definition. Let H be a subgroup of G. Let α be the inclusion map $H \hookrightarrow G$ and $\beta : M \to M$ be the identity. The map $\operatorname{Res} : H^i(G, M) \to H^i(H, M)$ given by the previous proposition is called the restriction homomorphism.

Definition. Let H be a normal subgroup of G. Let α be the qoutient map $G \to G/H$ and $\beta : M^H \to M$ be the inclusion map. The map $\operatorname{Inf} : H^i(G/H, M^H) \to H^i(G, M)$ given by the previous proposition is called the inflation homomorphism.

We can now introduce the following key exact sequence.

Proposition 2.1.8 (inflation-restriction exact sequence)**.** *Let M be a G-module and let H be a normal subgroup of G. Suppose that $H^i(H,M)$ is zero for all $i \in \{1,..,n-1\}$. Then we have the following exact sequence.*

$$1 \longrightarrow H^n(G/H,M) \xrightarrow{Inf} H^n(G,M) \xrightarrow{Res} H^n(H,M)$$

Proof. See [5]. □

2.2 Tate's theorem

In this section we prove Tate's theorem. It is a very powerful result which we will use to extract key information in Local class field Theory. Namely, it will allow us to establish $K^\times/N_{L|K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L|K)^{ab}$ for a finite Galois extension $L|K$ of local fields.

Theorem 2.2.1 (Tate's theorem)**.** *Suppose that G is a finite solvable group and suppose that we have the following for each subgroup $H \leq G$.*
a)$H^1(H,M)$ is zero.
b)$H^2(H,M)$ is cyclic of order $|H|$.
Then there are isomorphisms $\hat{H}^n(G,\mathbb{Z}) \xrightarrow{\sim} \hat{H}^{n+2}(G,M)$ that depend only on the choice of generator for $\hat{H}^2(G,M)$.

To prove Tate's theorem we first need to show the following lemma.

Lemma 2.2.2. *Let G be a finite solvable group and M a G-module. Suppose that $H^i(H,M) = 0$ for $i \in \{1,2\}$ for every subgroup H of G including G itself. Then $\hat{H}^i(G,M)$ is zero for every $i \in \mathbb{Z}$.*

Proof. For G cyclic this follows from the periodicity of the Tate groups. We will first prove this for the H^i, with $i > 0$, by strong induction and the inflation restriction exact sequence. Since G is solvable there is a subgroup H such that G/H is cyclic.

By the strong induction hypothesis $H^i(H, M)$ is zero. We have the following inflation restriction exact sequence

$$0 \to H^i(G/H, M^H) \to H^i(G, M) \to H^i(H, M).$$

Now the last term is zero so we get and isomorphism of the middle two terms for all $i > 0$. On the other hand, $H^i(G/H, M^H)$ is periodic and $H^i(G, M)$ is zero for $i \in \{1, 2\}$. Hence, $H^i(G, M)$ is zero for all $i > 0$.

We now show that $\hat{H}^0(G, M)$ is zero. Let $x \in M^G$. Since $\hat{H}^0(G/H, M^H)$ is zero, we have a $y \in M^H$ such that $N_{G/H}(y) = x$. Moreover, since $\hat{H}^0(H, M)$ is zero, we have a $z \in M$ such that $N_H(z) = y$. Thus,

$$N_G(z) = N_{G/H}(N_G(z)) = x.$$

Since x was an arbitrary element in M^G we get $M^G = N_G(M)$ and so $\hat{H}^0(G, M)$ is zero as claimed.

We will now prove the lemma for general n. We proceed by dimension shifting. Find a G-module N making the following sequence exact.

$$0 \to N \to \mathrm{Ind}_1^G(M) \to M \to 0$$

Where the map $\mathrm{Ind}_1^G(M) \to M$ sends $M \otimes [g]$ to m^g. The term in the middle is acyclic so we get isomorphisms $\hat{H}^{i+1}(H, N) \simeq \hat{H}^i(H, M)$ for any subgroup H of G. But then $H^i(H, N)$ is zero for $i \in \{1, 2\}$ for any subgroup H of G. Then the previous argument gives that $\hat{H}^i(G, N)$ is zero for all $i \geq 0$. Then $\hat{H}^{-1}(G, M) = \hat{H}^0(G, N)$ is zero. The same argument applies to N so $\hat{H}^{-1}(G, N)$ is zero. Hence, $\hat{H}^{-2}(G, M)$ is zero and so on.

□

Proof of Tate's theorem. Let γ be a generator of $H^2(G, M)$. The fact that $\mathrm{Cor} \circ \mathrm{Res}$ is multiplication by $[G : H]$ implies that $\mathrm{Res}(\gamma)$ generates $H^2(H, M)$ for any subgroup $H \subseteq G$. Let ϕ be the cocycle representing γ. Now define the module $M(\phi)$ to be the direct sum of M and the free abelian group consisting of symbols x_σ for every $\sigma \in G$ with $\sigma \neq 1$. We extend the action on M to an action on $M(\phi)$ by setting

$$\sigma x_\tau = x_{\sigma\tau} - x_\sigma + \phi(\sigma, \tau)$$

and x_1 should be interpreted as $\phi(1, 1)$. We, will first show that both $H^1(H, M(\phi))$ and $H^2(H, M(\phi))$ are zero for any subgroup H of G. First, consider the following exact sequence.

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

From the fact that $\mathbb{Z}[G]$ is induced we see that the $H^r(G, \mathbb{Z}[G]) = 0$ for all $r > 0$. It follows that $H^1(H, I_G) = H^0(H, \mathbb{Z}) = \mathbb{Z}/|H|\mathbb{Z}$ and $H^2(H, I_G) = H^1(H, \mathbb{Z}) = 0$.

Define the additive map $\alpha : M(\phi) \to \mathbb{Z}[G]$ to be such that $\alpha(m) = 0$ for all $m \in M$ and $\alpha(x_\sigma) = \sigma - 1$. We have the following exact sequence of G-modules.

$$0 \to M \to M(\phi) \xrightarrow{\alpha} I_G \to 0$$

From the corresponding long exact sequence on the cohomology groups we get the following exact sequence.

$$0 \to H^1(H, M(\phi)) \to H^1(H, I_G) \to H^2(H, M) \to H^2(H, M(\phi)) \to 0$$

Here we used the fact that $H^1(H, M) = 0$ and $H^2(H, I_G) = 0$ to get the zero end terms. The map $H^2(H,M) \to H^2(H,M(\phi))$ is zero because $H^2(H,M)$ is generated by $\mathrm{Res}(\gamma)$ and this maps to the restriction of the image of γ in $H^2(G,M(\phi))$, which is zero. Thus, $H^1(H,I_G) \to H^2(H,M)$ is onto and hence an isomorphism since they both have the same order. Then, both its kernel and cokernel, namely, $H^1(H,M(\phi))$ and $H^2(H,M(\phi))$ are both zero. Thus, the previous lemma gives $H^n(H,M(\phi))$ is zero for all n. This, combined with the splicing of the four term exact sequence

$$0 \to M \to M(\phi) \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

(the same way we proved periodicity) gives the isomorphisms

$$\hat{H}^n(G,\mathbb{Z}) \to \hat{H}^{n+2}(G,M)$$

as desired.

□

We will lastly make an essential observation that will supplement Tate's theorem in helping us with proving the important result in local class field theory mentioned earlier.

Proposition 2.2.3. $H_1(G,\mathbb{Z}) = G/[G,G]$

Proof. From the exact sequence

$$1 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 1$$

we obtain a long exact sequence on the homology groups. From the long exact sequence on the homology groups and the fact that $H_1(G,\mathbb{Z}[G])$ is zero, we obtain the exact sequence

$$1 \to H_1(G,\mathbb{Z}) \to H_0(G,I_G) \to H_0(G,\mathbb{Z}[G])$$

which can be rewritten as

$$1 \to H_1(G, \mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z}[G]/I_G.$$

The middle map $I_G/I_G^2 \to \mathbb{Z}[G]/I_G$ is induced by $I_G \hookrightarrow \mathbb{Z}[G]$ and is thus the zero map. So we obtain an isomorphism

$$H_1(G, \mathbb{Z}) \xrightarrow{\sim} I_G/I_G^2$$

However, $G/[G, G]$ is isomorphic to I_G/I_G^2 via the map ϕ induced by $g \to g - 1 + I_G^2$. The conclusion follows. □

Chapter 3

Further preliminaries

The first section of this chapter mainly follows [5] and [3]. The second mainly follows [7]. Both sections have arguments from [5] and [7].

3.1 Some results from local class field theory

We will first calculate the order of $\hat{H}^n(G(L|K), L^\times)$ for $n \in \{0, -1\}$ when $G = \mathrm{Gal}(L|K)$ is cyclic. This is already an important fact which Neukirch refers to as the class field axiom.

Lemma 3.1.1. *Let $L|K$ be a finite Galois extension of local fields. Then there is an open Galois stable subgroup V of $\mathcal{O}_L$ such that $H^i(Gal(L|K), V) = 0$ for all $i > 0$.*

Proof. By the normal basis theorem we have that there is an $\alpha \in L$ such that $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L|K)\}$ is a basis of L over K. Clearing out the common denominator we can ensure that $\alpha \in \mathcal{O}_L$. Let $V = \sum_{\sigma \in \mathrm{Gal}(L|K)} \sigma(\alpha)\mathcal{O}_L$. Then V is open in $\mathcal{O}_L$. Furthermore, $V = \mathrm{Ind}_e^G(\mathcal{O}_K)$ and hence is acyclic. It follows that $H^i(\mathrm{Gal}(L|K), V) = 0$ for all $i > 0$ and thus V satisfies the claim of the proposition. □

Lemma 3.1.2. *Let $L|K$ be a finite Galois extension of local fields. Then there is an open Galois stable subgroup W of U_L such that $H^i(G(L|K), W) = 0$ for all $i > 0$.*

Proof. We will prove this only for the case where the characteristic of K is zero. Let V be as in the previous proof then then we can choose an integer n sufficiently large so that $\pi^n V$ lies in the radius of convergence of

$$\exp(x) = \sum_{i=0}^{\infty} \frac{x^i}{i!}$$

and set $W = \exp(\pi^n V)$. □

Theorem 3.1.3. *If $L|K$ is a cyclic extension of local fields then the Herbrand quotient satisfies*

$$h(U_L) = 1.$$

Proof. Let W be as in the last proof. From the exact sequence

$$1 \to W \to U_L \to U_L/W \to 1$$

we get $h(U_L) = h(W)h(U_L/W)$. However, since U_L is compact U_L/W is finite and it follows that $h(U_L/W) = 1$ (cf [4] chapter 1 exercises 45.c). However we had $H^i(G(L|K), W) = 0$ for all $i > 0$ so $h(W) = 1$. Thus, $h(U_L) = 1$. □

Theorem 3.1.4 (Local Class Field Axiom)**.** *Let $L|K$ be a cyclic extension of local fields. Then, we have*

$$|\hat{H}^n(G(L|K), L^\times)| = \begin{cases} [L:K] & \textit{if } n = 0 \\ 1 & \textit{if } n = -1 \end{cases}$$

Proof of the Local Class Field Axiom. From the exact sequence

$$1 \to U_L \to L^\times \to \mathbb{Z} \to 1$$

we get $h(U_L)h(\mathbb{Z}) = h(L^\times)$. However, we have $h(U_L) = 1$ and $h(\mathbb{Z}) = |G(L|K)| = [L : K]$. Moreover, the fact that G is cyclic along with Hilbert 90 already tells us that $|\hat{H}^{-1}(G(L|K), L^\times)| = |\hat{H}^1(G(L|K), L^\times)| = 1$.

It follows that $|\hat{H}^0(G(L|K), L^\times)| = [L : K]$. This completes the proof of the claim. □

We know move to the main goal of this section which is to establish the isomorphism $K^\times/N_{L|K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L|K)^{ab}$. It is easiest to begin investigating the case where $L|K$ is unramified.

Theorem 3.1.5. *Let $L|K$ be an unramified extension. $H^1(Gal(L|K), U_L) = 0$.*

Proof. Since $L|K$ is unramified we can choose a uniformizer $\pi \in K$ and write $L^\times = U_L \cdot \pi$ which is equivalent to saying that we have a decomposition of G modules $L^\times = U_L \times \mathbb{Z}$. It follows $H^1(\mathrm{Gal}(L|K), U_L)$ is a direct summand of $H^1(\mathrm{Gal}(L|K), L^\times)$ which is zero by Hilbert 90. □

We actually directly obtain an important corollary

Corollary 3.1.6. *Let $L|K$ be unramified. Then the norm map $N_{L|K} : U_L \to U_K$ is surjective.*

Proof. Since $L|K$ is unramified it's cyclic. But we have already shown that $H^1(\mathrm{Gal}(L|K), U_L) = \hat{H}^{-1}(G(L|K), U_L)$ is zero. Furthermore, we also showed that $h(U_L) = 1$ since $L|K$ is cyclic. It follows that $\hat{H}^0(G(L|K), U_L)$ is zero which is the desired conclusion. □

We know prove another important result when $L|K$ is unramified which will help us prove that $H^2(\mathrm{Gal}(L|K), L^\times)$ is always cyclic of order $[L : K]$.

Theorem 3.1.7. *Let $L|K$ be unramified. Then $H^2(Gal(L|K), L^\times) = \hat{H}^0(G(L|K), L^\times)$ is cyclic of order $[L : K]$*

Proof. From the exact sequence $1 \to U_L \to L^\times \to \mathbb{Z} \to 1$ we obtain an exact hexagon from which we see that

$$\hat{H}^0(G(L|K), U_L) = 1 \to \hat{H}^0(G(L|K), L^\times) \to \hat{H}^0(G(L|K), \mathbb{Z}) \to 1 = \hat{H}^{-1}(G(L|K), U_L)$$

But $\hat{H}^0(G(L|K), \mathbb{Z})$ is cyclic of order $[L : K]$. The conclusion follows. □

Theorem 3.1.8. *For any finite Galois extension of local fields $|H^2(Gal(L|K), L^\times)| \leq [L : K]$.*

Proof. We proceed by strong induction. We already have $|H^2(\mathrm{Gal}(L|K))| = [L : K]$ for cyclic extensions so we have a base case. If $L|K$ is not cyclic then it's solvable since it is an extension of local fields. Then there is a Galois sub extension $M|K$. We have the following exact sequence.

$$0 \to H^2(\mathrm{Gal}(M|K), M^\times) \xrightarrow{\text{inf}} H^2(\mathrm{Gal}(L|K), L^\times) \xrightarrow{\text{res}} H^2(\mathrm{Gal}(L|M), L^\times)$$

Exactness gives $|H^2(\mathrm{Gal}(L|K), L^\times)| \leq |H^2(\mathrm{Gal}(L|M), L^\times)||H^2(\mathrm{Gal}(M|K), M^\times)| \leq [L : M][M : K] = [L : K]$

□

Theorem 3.1.9. *Let $L|K$ be a Galois extension of local fields then $H^2(Gal(L|K), L^\times)$ is cyclic of order $[L : K]$.*

Proof. It suffices to prove that $H^2(\mathrm{Gal}(L|K), L^\times)$ has an element of order $[L : K]$. Let $M|K$ be an unramified extension of order $[L : K]$ consider the diagram below.

$$\begin{tikzcd}
 & & H^2(\mathrm{Gal}(M|K), M^\times) \arrow[d, "\mathrm{Inf}"] \arrow[dr] & \\
0 \arrow[r] & H^2(\mathrm{Gal}(L|K), L^\times) \arrow[r, "\mathrm{Inf}"] & H^2(\mathrm{Gal}(ML|K), ML^\times) \arrow[r, "\mathrm{Res}"] & H^2(\mathrm{Gal}(ML|L), ML^\times)
\end{tikzcd}$$

The inflation-restriction exact sequence shows that the row is exact and it can be used to show that the vertical arrow is injective. If we show that the diagonal arrow is the zero map then the fact that $H^2(\mathrm{Gal}(M|K), M^\times) \cong \mathbb{Z}/[L:K]\mathbb{Z}$ and exactness will give us an element in $H^2(\mathrm{Gal}(L|K), L^\times)$ of order $[L:K]$.

Let e, f and U be the ramification index, inertia degree and the maximal unramified subextension of $L|K$. Then we have the following canonical isomorphism $\mathrm{Gal}(ML|L) \cong \mathrm{Gal}(M|U)$ of cyclic groups of order e. By using the same generator for both groups we can obtain the following commutative diagram.

$$\begin{tikzcd}
\hat{H}^0(\mathrm{Gal}(M|K), M^\times) \arrow[r, "\mathrm{Res}"] \arrow[d] & \hat{H}^0(\mathrm{Gal}(M|U), M^\times) \arrow[r] \arrow[d] & \hat{H}^0(\mathrm{Gal}(ML|L), ML^\times) \arrow[d] \\
H^2(\mathrm{Gal}(M|K), M^\times) \arrow[r, "\mathrm{Res}"] & H^2(\mathrm{Gal}(M|U), M^\times) \arrow[r] & H^2(\mathrm{Gal}(ML|L), ML^\times)
\end{tikzcd}$$

In the above diagram the vertical arrows are isomorphisms we obtain from the fact that all the aforementioned Galois groups are cyclic. The composition in the bottom row is the same as the diagonal arrow which we want to be zero. To prove this it suffices to check that the composition in the top row is zero. The map on the top row is the canonical map $K^\times/N_{M|K}(M^\times) \to L^\times/N_{ML|L}(ML)^\times$. $K^\times/N_{M|K}(M^\times)$ is cyclic of order ef and is generated by a uniformizer π_K of K. On the other hand, $L^\times/N_{ML|L}(ML)^\times$ is cyclic of order e and is generated by a uniformizer π_L of L. However, $\pi_K = u\pi_L^e$ for some unit $u \in U_L$. Thus, the map is indeed the zero map. The conclusion follows. □

Theorem 3.1.10. *Let $L|K$ be any finite Galois extension of local fields. Then there is a canonical isomorphism*

$$\hat{H}^i(Gal(L|K), \mathbb{Z}) \xrightarrow{\sim} \hat{H}^{i+2}(Gal(L|K), L^\times).$$

In particular,

$$K^\times/N_{L|K}(L^\times) \xrightarrow{\sim} Gal(L|K)^{ab}.$$

Proof. This follows from Tate's theorem since we have already shown that $H^2(\mathrm{Gal}(L|M), L^\times)$ is cyclic of order $[L : M]$ and $H^1(\mathrm{Gal}(L|M), L^\times)$ is zero by Hilbert 90. □

We know state an important implication which we will use in our proof of the second inequality.

Proposition 3.1.11. *If K contains an n-th root of unity and if n is not divisible by $Char(K)$ then the extension $L = K(K^{1/n})|K$ is finite and we have $N_{L|K}(L^\times) = (K^\times)^n$*

Proof. By Kummer theory

$$\mathrm{Hom}(G(L|K), \mu_n) \simeq K^\times/(K^\times)^n.$$

This gives that $\mathrm{Gal}(L|K)$ is finite because $K^\times/(K^\times)^n$ is finite. Since L is abelian and finite over K, $\mathrm{Gal}(L|K) = K^\times/N_{L|K}(L^\times)$ by the previous theorem. We have $K^\times/N_{L|K}(L^\times)$ has exponent n so $(K^\times)^n \subseteq N_{L|K}(L^\times)$. Now, the first isomorphism already tells us that $|K^\times/(K^\times)^n| = |G(L|K)|$. It follows that

$$|K^\times/(K^\times)^n| = |G(L|K)| = |K^\times/N_{L|K}(L^\times)|.$$

Hence $N_{L|K}(L^\times) = (K^\times)^n$ as claimed. □

3.2 The idèles and some facts about local fields

Recall that two absolute values on K are called **equivalent** if they define the same topology on K.

Definition. A prime or place (denoted $\mathfrak{p}$ or v) of an algebraic number field is a class of equivalent absolute values on K. The nonarchimedean classes will be called finite primes and the archimedean ones will be called infinite.

For a place $\mathfrak{p}$, denote by $K_{\mathfrak{p}}$ the completion of K at $\mathfrak{p}$.

If $\mathfrak{p}$ is finite, we write $\mathfrak{p}|p$ if p is the characteristic of the residue class field $\kappa(\mathfrak{p})$. If $\mathfrak{p}$ is infinite, we write $\mathfrak{p}|\infty$ and we also define $\kappa(\mathfrak{p}) := K_{\mathfrak{p}}$.

When $\mathfrak{p}$ is finite, $v_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic valuation which we normalize by requiring $v_{\mathfrak{p}}(K^{\times}) = \mathbb{Z}$. On the other hand, if $\mathfrak{p}$ is infinite then we set

$$v_{\mathfrak{p}}(a) = -\log(|\tau(a)|)$$

where τ is the associated embedding $K \hookrightarrow \mathbb{C}$ that defines $\mathfrak{p}$.

Define $f_{\mathfrak{p}} = [\kappa(\mathfrak{p}) : \kappa(p)]$ and

$$\mathfrak{N}(\mathfrak{p}) = \begin{cases} p^{f_{\mathfrak{p}}} & \text{if } \mathfrak{p} \text{ is finite that lies over p} \\ e^{f_{\mathfrak{p}}} & \text{if } \mathfrak{p} \text{ is infinite} \end{cases}$$

where e is just Euler's number. We note that if $\mathfrak{p}$ is infinite then $f_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{R}]$.

We now define the normalized absolute value for $a \in K$ by

$$|a|_{\mathfrak{p}} = \mathfrak{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(a)}$$

Let $L|K$ be a finite extension. As a convention we will denote the primes of L be $\mathfrak{P}$ and we will write $\mathfrak{P}|\mathfrak{p}$ whenever the restriction of $\mathfrak{P}$ to K gives $\mathfrak{p}$. In the case the prime is infinite we define the inertia degree to be $f_{\mathfrak{P}|\mathfrak{p}} = [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ and $e_{\mathfrak{P}|\mathfrak{p}} = 1$.

Remark. We will sometimes use $w|v$ instead of $\mathfrak{P}|\mathfrak{p}$.

We have the following.

Proposition 3.2.1. *For any primes* $\mathfrak{P}|\mathfrak{p}$

1. $\sum_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}|\mathfrak{p}} = \sum_{\mathfrak{P}|\mathfrak{p}} [L_{\mathfrak{P}} : K_{\mathfrak{p}}] = [L : K]$,

2. $\mathfrak{N}(\mathfrak{P}) = \mathfrak{N}(\mathfrak{p})^{f_{\mathfrak{P}|\mathfrak{p}}}$,

3. $v_{\mathfrak{P}}(a) = e_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(a)$ *for* $a \in K^{\times}$,

4. $v_{\mathfrak{P}}(N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}(a)) = f_{\mathfrak{P}|\mathfrak{p}} v_{\mathfrak{P}}(a)$ *for* $a \in L^{\times}$,

5. $|a|_{\mathfrak{P}} = |N_{L_{\mathfrak{P}}|K_{\mathfrak{p}}}(a)|_{\mathfrak{p}}$ *for* $a \in L$.

We first state a key result related to valuations normalized as above.

Proposition 3.2.2. *Let* $x \in K^{\times}$ *then* $|x|_{\mathfrak{p}} = 1$ *for all but finitely many places and* $\prod_{\mathfrak{p}} |x|_{\mathfrak{p}} = 1$ *where the product runs over all places of the algebraic number field* K.

Proof. First notice that we have that $|x|_{\mathfrak{p}} = 1$ for any prime that does not appear in the prime factorization of (x). So the first claim is true. Then,

$$\prod_{\mathfrak{p}} |a|_{\mathfrak{p}} = \prod_{p} \prod_{\mathfrak{p}|p} |a|_{\mathfrak{p}} = \prod_{p} \prod_{\mathfrak{p}|p} |N_{K_{\mathfrak{p}}|\mathbb{Q}_p}(a)|_p = \prod_{p} |N_{K|\mathbb{Q}}(a)|_p = 1$$

□

We know introduce an object that is central to our arguments in the first and second inequality.

Definition. The idèle group I_K of K is given by

$$I_K = \{(a_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} K_{\mathfrak{p}} | a_{\mathfrak{p}} \in \mathcal{O}_{K_{\mathfrak{p}}}^{\times} \text{ for all but finitely many } \mathfrak{p}\}.$$

The above product runs over all places $\mathfrak{p}$ of K.

Let $L|K$ be a finite Galois extension of number fields with Galois group G. We make I_L into a G-module by defining for $\alpha \in I_L$ the element $\sigma(\alpha) \in I_L$ whose components are given by

$$\sigma(\alpha)_{\sigma(\mathfrak{P})} = \sigma(\alpha_{\mathfrak{P}})$$

For a finite set S we can specialize the idèles.

Definition. For and finite set of primes S define the group S-idèles, denoted $I_{K,S}$ as $I_{K,S} = \prod_{\mathfrak{p} \in S} K_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{K_{\mathfrak{p}}}^{\times}$.

Let S_∞ be the set of infinite primes. We relate the simplified notion to the original notion via the lemma below

Lemma 3.2.3. *Let $S \supset S_\infty$ be a finite set of primes containing the generators of the ideal class group of K then $I_K = I_{K,S} \cdot K^\times$*

Proof. The conditions on S imply the following. Every fractional ideal $\mathfrak{a}$ can be written as $\mathfrak{a} = \mathfrak{b} \cdot (c)$ with $c \in K^\times$ and $\mathfrak{b}$ in the group generated by S. Thus, $\mathfrak{a} = (c)$ in the group $I^S = I/\langle S \rangle$ where I is the group of fractional ideals. Now, let $i : K^\times \to I$ be the map sending $a \in K^\times$ to the principle ideal (a). Then the previous observation gives $I^S/i(K)$ is the zero group. On the other hand, for such an $S \supset S_\infty$ we get a natural map $I_K \to I^S$ which defines an isomorphism $I_K/I_{K,S} \cong I^S$. Quotienting both sides by $K^\times$ we get $I_K/(I_S \cdot K^\times) \cong I^S/i(K^\times) = 0$. This directly implies $I_S = I_{K,S} \cdot K^\times$. □

We define the S units as $K_S = I_S \cap K$. We have the following result extending the Dirichlet unit theorem. Let H denote the $(s-1)$ dimensional vector spaces that appears as the kernel of the trace map $\mathrm{Tr} : \prod_{\mathfrak{p} \in S} \mathbb{R} \to \mathbb{R}$.

Proposition 3.2.4. *If S contains all infinite primes then the homomorphism*

$$\rho : K_S \longrightarrow \prod_{\mathfrak{p} \in S} \mathbb{R} \cong \mathbb{R}^s$$

given by $\rho(x) = (log\ (|x|_{\mathfrak{p}}))_{\mathfrak{p}\in S}$ *has kernel* $\mu(K)$*, and its image is a complete lattice in* H*. In particular,* $K_S \cong \mathbb{Z}^{s-1} \times \mu(K)$*.*

Proof. See [7]. □

A central object for the next two chapters is the following group.

Definition. The idèle class group of K is $C_K = \frac{I_K}{K^\times}$.

We end this section by mentioning two results on fields that are equipped with absolute values. Both of these will come handy in the proofs of the first and second inequality.

Theorem 3.2.5 (Approximation theorem)**.** *Let* $|\ \ |_1, \dots, |\ \ |_n$ *be* n *non equivalent absolute values and let* $x_1, \dots, x_n \in K$ *be given elements. Then for every* $\epsilon > 0$ *there exists an* $x \in K$ *such that*

$$|x - a_i|_i < \epsilon$$

for all $i \in \{1, \dots, n\}$*.*

Proof. See [7]. □

For the proposition below let K be local field, different from $\mathbb{R}$ and $\mathbb{C}$, whose residue characteristic is p.

Proposition 3.2.6. *Let* $gcd(p, n) = 1$ *and* $x \in K^\times$*. Then* $K(\sqrt[n]{x})|K$ *is unramified if and only if* $x \in U_K K^{\times n}$*.*

Proof. Let $x = uy^n$ with $u \in U_K$ and $y \in K^\times$. In this case, $K(\sqrt[n]{x}) = K(\sqrt[n]{u})$. Let κ' be the splitting field for $X^n - u$ mod $\mathfrak{p}$ over the residue class field $\mathfrak{p}$. Furthermore, let $K'|K$ be the unramified extension with residue class field κ'. By Hensel's lemma, $X^n - u$ splits in to linear factors in K'. It follows that $K(\sqrt[n]{x})$ is unramified. To prove the converse suppose that $K(\sqrt[n]{x})|K$ is unramified and let $L = K(\sqrt[n]{x})$. Write $x = u\pi^r$ with π a prime element in K and $u \in U_K$. Then, $v_L(\sqrt[n]{u\pi^r}) = \frac{v_L(\pi^r)}{n} = \frac{r}{n} \in \mathbb{Z}$. It follows that $n|r$ and so $x \in U_K K^{\times n}$. This completes the proof. □

Chapter 4

The first inequality

This section is mainly based on Kedlayas notes[3] which itself also references both Milne[5] and Neukirch[7].

4.1 The statement and the plan

We will show that for a cyclic extension $L|K$ of number fields we have that
$h(C_L) = [L : K]$ when C_L is regarded as a $\mathrm{Gal}(L|K)$-module in the usual way. This will imply the first inequality which is stated below.

Theorem 4.1.1 (The first inequality)**.** *Let $L|K$ be a cyclic extension of number fields then $h(C_L) = [L : K]$. In particular*

$$|\hat{H}^0(G(L|K), C_L)| \geq [L : K].$$

4.2 A relevant result on certain lattices

In this section we compute the Herbrand quotient of a G-lattice (which is just a G-stable lattice) in $\mathbb{R}$-vector space with a G action, for a finite group G. More specifically, it will reduce the problem of computing $h(L_{\widetilde{S}})$, where $\widetilde{S}$ is a set of places which we will specify in the following section, to computing a much simpler Herbrand quotient.

Lemma 4.2.1. *Let V be a $\mathbb{Q}$-vector space with a G-linear action. Let $L_1, L_2 \subseteq V$ be full G-lattices so that rank(L_1) = rank(L_2) = dim(V). Then if $h(L_1)$ exists then $h(L_2)$ exists and $h(L_1) = h(L_2)$.*

Proof. Since L_1 and L_2 are G- lattices in V with $\text{rank}(L_1) = \text{rank}(L_2) = \dim(V)$, there is an integer $n > 0$ such that $nL_2 \subseteq L_1$ and so $\frac{L_1}{nL_2} = \mu$ is a finite group. For a finite group μ we always have $h(\mu) = 1$ (cf [4] chapter 1 exercises 45.c). Moreover, since $nL_2 \cong L_2$ we have $h(L_2) = h(nL_2)$.

Now, the sequence

$$1 \to nL_2 \to L_1 \to \mu \to 1$$

is exact so the Herbrand quotients multiply. Thus,

$$h(L_1) = h(nL_2)h(\mu) = h(nL_2) = h(L_2)$$

as claimed.

□

We know state the main result which will help us compute the Herbrand quotient.

Theorem 4.2.2. *Let V be a $\mathbb{R}$-vector space with a G-linear action. Let $L_1, L_2 \subseteq V$ be full G-lattices so that rank(L_1) = rank(L_2) = dim(V). Then if $h(L_1)$ exists then $h(L_2)$ exists and $h(L_1) = h(L_2)$.*

Proof. We have $L_1 \otimes_{\mathbb{Z}} \mathbb{R} \cong V$ and $L_2 \otimes_{\mathbb{Z}} \mathbb{R} \cong V$ as G-modules. So there exists a G-module isomorphism $\phi : L_2 \otimes_{\mathbb{Z}} \mathbb{R} \to L_1 \otimes_{\mathbb{Z}} \mathbb{R}$. Let $\text{Hom}_{\mathbb{Z}}(L_1, L_2) = M$ and note that we can make M a G-module with G action given by $\phi^g(x) = g\phi(g^{-1}(x))$.

Now, let

$$W = \text{Hom}_{\mathbb{Q}}(L_1 \otimes_{\mathbb{Z}} \mathbb{Q}, L_2 \otimes_{\mathbb{Z}} \mathbb{Q})$$

and $H \subset W$ be the linear subspace defined by the linear equations

$$y \in H \Longleftrightarrow y = g(y) \forall g \in G.$$

We have $H_{\mathbb{R}} \hookrightarrow W_{\mathbb{R}}$ and $H_{\mathbb{R}}$ contains a nonzero element ϕ; Hence, $H \neq 0$. The determinant map on H,

$$f \to \wedge^n f : \wedge^n (L_1 \otimes_{\mathbb{Z}} \mathbb{Q}) \to \wedge^n (L_1 \otimes_{\mathbb{Z}} \mathbb{Q})$$

is a polynomial map and this map does not identically vanish on H. It follows that H contains a G-isomorphism $L_1 \otimes_Z \mathbb{Q} \xrightarrow{\sim} L_2 \otimes_Z \mathbb{Q}$. Thus both L_1 and L_2 are full lattices of $L_1 \otimes_Z \mathbb{Q} \simeq L_2 \otimes_Z \mathbb{Q}$. Hence we can apply the previous result. □

4.3 The computation of the Herbrand quotients

Now we go back to the main problem of this section. Let $L|K$ be a cyclic extension of number fields.

Now pick a set S such that S contains the following:
a)S contains the primes v_i underneath w_i with $\{w_i\}$ a set generators of the ideal class group of L.
b)S contains all infinite places.
c)S contains all the primes that ramify in L.

Let $\widetilde{S}$ be the set of primes in L above the primes in S. Then for $w \in \widetilde{S}$, we always have $\sigma(w) \in \widetilde{S}$ for every $\sigma \in \mathrm{Gal}(L|K)$. Furthermore, we have $I_L = I_{L,\widetilde{S}} \cdot L^{\times}$.

Starting from the exact sequence

$$1 \to L \to I_L \to C_L \to 1$$

By choice of $\widetilde{S}$ we have $I_L = I_{L,\widetilde{S}} \cdot L^\times$. Since, by definition, $L_{\widetilde{S}} = I_{L,\widetilde{S}} \cap L^\times$, we get an exact sequence

$$1 \to L_{\widetilde{S}} \to I_{L,\widetilde{S}} \to C_L \to 1$$

Since the Herbrand quotients in an exact sequence multiply, we get $h(C_L)h(L_{\widetilde{S}}) = h(I_{L,\widetilde{S}})$ or equivalently $h(C_L) = \frac{h(I_{L,\widetilde{S}})}{h(L_{\widetilde{S}})}$.

Proposition 4.3.1. *Let w_0 be a prime above v_0 and let $G = Gal\ (L|K)$. We have*

$$\prod_{w|v_0} L_w = Ind\,{}^G_{G_{w_0}}(L^\times_{w_0}), \quad \prod_{w|v_0} U_w = Ind\,{}^G_{G_{w_0}}(U^\times_{w_0})$$

where G_{w_0} is the decomposition group of $w_0|v$. (Here we identify $G_{w_0} = Gal\ (L_{w_0}|K_{v_0})$)

Proof.

$$L \otimes_K K_{v_0} \simeq \prod_{w|v_0} L_w \simeq \bigoplus_{\sigma \in G/G_{w_0}} L_{w_0} \simeq \text{Ind}\,{}^G_{G_{w_0}}(L^\times_{w_0})$$

This yields

$$\prod_{w|v_0} L_w = \text{Ind}\,{}^G_{G_{w_0}}(L^\times_{w_0})$$

and

$$\prod_{w|v_0} U_w = \text{Ind}\,{}^G_{G_{w_0}}(U^\times_{w_0}).$$

□

Now we write $I_{L,\widetilde{S}} = \prod_{v \in S}(\prod_{w|v} L^\times_w) \times \prod_{v \notin S}(\prod_{w|v} U_w)$

Corollary 4.3.2. *For $i \in \{0, -1\}$ we have that $\hat{H}^i(G(L|K), I_{L,\widetilde{S}}) = \oplus_{v_0 \in S}\hat{H}^i(G_{w_0}, L^\times_{w_0})$ where for each $v_0 \in S$ we choose a $w_0 \in \widetilde{S}$ that lies above it.*

Proof. This follows directly from Shapiro's lemma. We have

$$I_{L,\widetilde{S}} = \prod_{v\in S}(\prod_{w|v} L_w^\times) \times \prod_{v\notin S}(\prod_{w|v} U_w)$$

for a given $v_0 \notin S$,

$$\hat{H}^i(G(L|K), \prod_{w|v_0} U_w) \simeq \hat{H}^i(G_{w_0}, U_{w_0}) = 0$$

by Shapiro's lemma, Theorem 3.1.5, Corollary 3.1.6 and the fact that the Tate groups are periodic in the case $G = G(L|K)$ is cyclic.

Hence, $\hat{H}^i(G(L|K), I_{L,\widetilde{S}}) = \oplus_{v_0\in S}\hat{H}^i(G_{w_0}, L_{w_0}^\times)$ where for each $v_0 \in S$ we choose a $w_0 \in \widetilde{S}$ that lies above it.

□

Corollary 4.3.3. *For $i \in \{0, -1\}$ we have that $\hat{H}^i(G(L|K), I_L) = \oplus_{v_0}\hat{H}^i(G_{w_0}, L_{w_0}^\times)$ where for each v_0 we choose a w_0 that lies above it and the sum is over all places v_0 of K.*

Proof. This follows directly from the previous result by taking direct limits as $\widetilde{S}$ varies. □

Corollary 4.3.4. *We have that $h(I_{L,\widetilde{S}}) = \prod_{v_0\in S}[L_{w_0} : K_{v_0}]$ where for each $v_0 \in S$ we choose a $w_0 \in \widetilde{S}$ that lies above it.*

Proof. From the earlier proposition we have $|\hat{H}^i(G(L|K), I_{L,\widetilde{S}})| = \prod_{v_0\in S} |\hat{H}^i(G_{w_0}, L_{w_0}^\times)|$ for $i \in \{0, -1\}$. However, from the Local Class Field Axiom we have $|\hat{H}^0(G_{w_0}, L_{w_0}^\times)| = [L_{w_0} : K_{v_0}]$ and $|\hat{H}^{-1}(G_{w_0}, L_{w_0}^\times)| = 1$. Hence,

$$h(I_{L,\widetilde{S}}) = \frac{\prod_{v_0\in S} |\hat{H}^0(G_{w_0}, L_{w_0}^\times)|}{\prod_{v_0\in S} |\hat{H}^{-1}(G_{w_0}, L_{w_0}^\times)|} = \prod_{v_0\in S}[L_{w_0} : K_{v_0}]$$

as claimed. □

Proposition 4.3.5. *We have that* $h(L_{\widetilde{S}}) = \frac{\prod_{v\in S}[L_w:K_v]}{[L:K]}$.

Proof. First recall that the map from proposition 3.2.4

$$\rho : K_S \longrightarrow \prod_{v\in S} \mathbb{R} \cong \mathbb{R}^s$$

has image a full lattice in the trace zero space H and has kernel $\mu(K)$. We thus have $h(L_{\widetilde{S}}) = h(\rho(L_{\widetilde{S}}))h(\mu(K)) = h(\rho(L_{\widetilde{S}}))$ since $\mu(K)$ is a finite G-module. Now let $v = (1, 1, .., 1)$ be the vector in $\mathbb{R}^s$. Since $v \notin H$ we have that $\rho(L_{\widetilde{S}}) \oplus v\mathbb{Z}$ is a full lattice in $\prod_{v\in S} \mathbb{R}$. We make this into a G-module by giving $\rho(L_{\widetilde{S}})$ the action it inherits from $L_{\widetilde{S}}$ and giving v the trivial action and extending by $\mathbb{Z}$ linearity. We note that $h(v\mathbb{Z}) = h(\mathbb{Z}) = |G|$ since $v\mathbb{Z}$ has the trivial action. We therefore get $h(\rho(L_{\widetilde{S}}) \oplus v\mathbb{Z}) = h(\rho(L_{\widetilde{S}}))h(v\mathbb{Z}) = h(\rho(L_{\widetilde{S}}))|G| = h(\rho(L_{\widetilde{S}}))[L : K]$. On the other hand, we can define another lattice $\bigoplus_{w\in\widetilde{S}} \mathbb{Z}$ with G action given by permuting the coordinates in accordance with how the places get permuted. This means that $\sigma(e_w) = e_{\sigma(w)}$. Now notice that for any w_0 above v_0 we have that $\bigoplus_{w|v_0} e_w\mathbb{Z} = \mathrm{Ind}_{G_{w_0}}^{G}(e_{w_0}\mathbb{Z})$. Then for $i \in \{0, -1\}$ we have $h(\bigoplus_{w\in\widetilde{S}} \mathbb{Z}) = \prod_{v_0\in S} h(G_{w_0}, e_{w_0}\mathbb{Z}) = \prod_{v_0\in S}[L_{w_0} : K_{v_0}]$. But then by what we said earlier

$$h(\rho(L_{\widetilde{S}}))[L : K] = h(\bigoplus_{w\in\widetilde{S}} \mathbb{Z}) = \prod_{v_0\in S}[L_{w_0} : K_{v_0}] \Longleftrightarrow h(L_{\widetilde{S}}) = h(\rho(L_{\widetilde{S}})) = \frac{\prod_{v\in S}[L_w : K_v]}{[L : K]}$$

as claimed. □

Corollary 4.3.6. $h(C_L) = [L : K]$.

4.4 Some implications

Corollary 4.4.1. *Let* $L|K$ *be a cyclic extension of prime power order. Then there are infinitely many primes in* K *that do not split completely in* L.

Proof. Let X be the set containing all ramified primes as well as all primes that do not split in $L|K$. Suppose X is finite and let $M|K$ be the subextension of $L|K$ of degree p.

We will deduce from this that $N_{M|K}(C_M) = C_K$ which will contradict the first inequality. Notice that $\frac{C_k}{N_{M|K}(C_M)} = \frac{I_k}{K^\times N_{M|K}(I_M)}$ so it suffices to show that for every $x \in I_K$ there is an $a \in K^\times$ such that $xa^{-1} \in N_{M|K}(I_M)$. Since X is finite the approximation theorem tells us that $x_v a^{-1}$ is contained in an open subgroup of $N_{M_w|K_v}(M_w)$ for all $v \in X$. For $v \notin X$ this is always true since $M_w = K_v$. Now the isomorphism

$$\frac{I_K}{N_{M|K}(I_M)} = \bigoplus_v \frac{K_v^\times}{N_{M_w|K_v}(M_w^\times)}$$

tells us that there is a $y \in I_M$ such that $xa^{-1} = N_{M|K}(y)$. This shows that
$I_K = K^\times N_{M|K}(I_M)$ and hence $C_K = N_{M|K}(C_M)$. This contradicts the first inequality.

□

The above result actually generalizes to a considerably wider context and is not much more difficult to prove.

Corollary 4.4.2. *Let $L|K$ be a finite extension of algebraic number fields. If almost all the primes of K split completely in L, then $K = L$.*

Proof. See Neukirch [7]. □

Chapter 5

The second inequality for cyclic extensions and the Hasse norm theorem

This section will mainly follow the presentation Neukirch[7] and Kedlaya[3] but will also follow Milne[5] in some arguments.

5.1 The statement and the plan

Lets first state what we are trying to prove.

Theorem 5.1.1 (The second inequality for cyclic extensions)**.** *If $L|K$ is a cyclic extension of number fields then $[I_K : K^\times N(I_L)] = \hat{H}^0(G(L|K), C_L)$ is finite and divides $[L : K]$.*

Lemma 5.1.2. *If $L|K$ is cyclic then the fallowing are equivalent:*
a)$[I_K : K^\times N(I_L)]$ is finite and divides $[L : K]$.
b)$|H^2(G(L|K), C_L)|$ is finite and divides $[L : K]$.
c)$H^1(G(L|K), C_L) = 0$.

Proof. Form the fact that the Tate groups are periodic for G cyclic we see that a) and b) are equivalent. This is because $\hat{H}^0(G(L|K), C_L) = I_K/K^\times N(I_L)$. The fact that they are equivalent to c) follows from the first inequality.

□

The plan: We will reduce our theorem for the case where $[L : K] = p$ for some prime and K contains a p-th root of unity. We will prove the reduced case by explicitly constructing a subgroup $H \leq C_L$ such that $[C_K : H] = p$ and $H \leq N_{L|K}(C_L)$. This means that $[C_K : N_{L|K}(C_L)] = \frac{[C_K:H]}{[N_{L|K}(C_L):H]}$ divides p. This also proves statement a) from the lemma in the reduced case since $[C_K : N_{L|K}(C_L)] = [I_K : K^\times N(I_L)]$ which will also prove all three statements since the reduced case has cyclic Galois group.

5.2 the reductions

Theorem 5.2.1. *To establish the second inequality for cyclic extensions, it suffices to prove it for the case for $G = G(L|K)$ cyclic of prime order.*

Proof. Assume that we already know this for cyclic groups of prime order. We proceed by strong induction. Suppose, for the sake of induction, that we proved this for all cyclic $|G| < n$. If n is prime then we are done by the reduction assumption. If n is not prime take a subgroup H such that $[G : H]$ is prime. Then, consider the exact sequence

$$0 \to H^1(G/H, C_{K'}) \to H^1(G, C_L) \to H^1(H, C_L)$$

where $K' = L^H$. By our reduction assumption we have $H^1(G/H, C_{K'})$ is zero and by the induction hypothesis we have $H^1(H, C_L)$ is zero. It follows that $H^1(G, C_L)$ is zero. □

Theorem 5.2.2. *It suffices to prove the case for G cyclic of prime order and K containing a p-th root of unity.*

Proof. Let $L' = L(\zeta)$ and $K' = K(\zeta)$. Set $G = \mathrm{Gal}(L|K)$ and $G' = \mathrm{Gal}(L'|K')$. We check that the map $\hat{H}^0(G, C_L) \to \hat{H}^0(G', C_{L'})$ induced by the inclusion $C_L \to C_{L'}$ is injective. Both these groups have exponent dividing p since $[L : K] = [L' : K'] = p$. Since $[K' : K] = d|(p-1)$ is coprime to p we have that the map $x \to x^d$ is an automorphism on $\hat{H}^0(G, C_L)$ and $\hat{H}^0(G', C_{L'})$. Consider a $\bar{x} = x \bmod N_{L|K}(C_L)$ that maps to the identity in $\hat{H}^0(G', C_{L'})$. There is a $\bar{y} = y \bmod N_{L|K}(C_L)$ satisfying $\bar{x} = \bar{y}^d$. Such a $\bar{y}$ must also map to the identity and hence $y = N_{L'|K'}(z)$ with $z \in C_{L'}$. Then we get

$$y^d = N_{K'|K}(y) = N_{L'|K}(z) = N_{L|K}(N_{L'|L}(z)) \in N_{L|K}(C_K)$$

Hence, $\bar{x} = \bar{y}^d = 1$ and the map is injective. Since the map is injective $|\hat{H}^0(G, C_L)| = [I_K : K^* N(I_L)]$ divides $|\hat{H}^0(G', C_{L'})| = [I_{K'} : (K')^\times N(I_L)]$. So if we prove that $[I_{K'} : (K')^\times N(I_L)]$ divides $[L' : K'] = p$ then so does $[I_K : K^* N(I_L)]$. Thus it suffices to prove the latter as claimed. □

5.3 The proof of the reduced case

We are now reduced to the case where $[L : K] = p$ and K contains a p-th root of unity.

Now pick a set S such that S contains the following:

a)S contains the generators of the ideal class group of K so that $I_K = I_{K,S} K^\times$

b)S contains all infinite places.

c)S contains all the primes that ramify in L.

d)S contains all the primes over (p) with $p = [L : K]$.

Theorem 5.3.1. *Let $\Delta = (L^\times)^p \cap K_S$. We have $L = K(\Delta^{1/p})$*

Proof. Since $[L : K] = p$ and K contains a p-th root of unity, Kummer theory gives us that $L = K(D^{1/p})$ for $D = (L^\times)^p \cap K^\times$. It is clear that $\Delta \subseteq D$ and the fact that $[L : K]$ is prime gives no room for an intermediate extension. Thus, it suffices to prove $K \neq K(\Delta^{1/p})$. First we can write $L = K(x^{1/p})$. Then for $v \notin S$ we have that $K_v(x^{1/p})|K_v$ is unramified. Hence, we can we can write x as a unit times a p-th power so that $x = u_v y_v^p$. Define an idèle $y \in I_K$ as follows.

$$(y)_v = \begin{cases} y_v & \text{if } v \notin S \\ 1 & \text{if } v \in S \end{cases}$$

Then since $I_K = K^\times I_{K,S}$ we can write $y = zw$ for $z \in K^\times$ and $w \in I_{K,S}$. Then, for $v \notin S$, we have $(x/z^p)_v = u_v y_v^p / z^p = u_v w_v^p \in \mathcal{O}_{K_v}^\times$. Thus $x/z^p \in (L^\times)^p \cap K_S = \Delta$ but $x \notin (K^\times)^p$ since $L = K(x^{1/p})$ and it follows that $L = K(\Delta^{1/p})$ □

Theorem 5.3.2. *There exists a set of places T that is disjoint from S with $|T| = s-1$ such that Δ is the kernel of the map $K_S \to \prod_{v\in T} K_v^\times/(K_v^\times)^p$;*

Proof. Let $N = K(K_S^{1/p})$ then Kummer theory gives us that

$$Gal(N/K) = Hom(K_S/K_S^p, \mathbb{Z}/p\mathbb{Z})$$

the unit theorem gives us that $K_S = \mathbb{Z}^{s-1} \times \mu(K)$. Since K contains an p-th root of unity $p \mid |\mu(K)|$. It follows that $K_S/K_S^p = (\mathbb{Z}/p\mathbb{Z})^s$ and hence $Gal(N/K) = Hom(K_S/K_S^p, \mathbb{Z}/p\mathbb{Z}) = (\mathbb{Z}/p\mathbb{Z})^s$. Now let $\sigma_1, ..., \sigma_{s-1}$ be a generating set for $Gal(N/L)$ and let $N_i = N_i^\sigma$ for $i \in \{1, ..., s-1\}$. By the corollary to the first inequality there are infinitely many primes of N_i that do not split completely in N. So we can choose for each N_i a place w_i, that does not split in N, such that the restrictions v_i to K are all distinct, and not contained in S. Let $T = \{v_1, ..., v_{s-1}\}$.

Now we show that such a T satisfies the claim. To do this we first show that the N_i are the decomposition field of $N|K$ at the unique w_i' in N that above w_i. First, since w_i is non split the decomposition field Z_i is contained in N_i and in particular $Gal(N|N_i) \subseteq Gal(N|Z_i)$. On the other hand, v_i is unramified in N so $Gal(N|Z_i)$ is cyclic. Since every element of $Gal(N|K)$ has order p we get $Gal(N|N_i) = Gal(N|Z_i)$ and $Z_i = N_i$.

From $L = \cup_{i=1}^{s-1} N_i$ we see that $L|K$ is the largest subextension of $N|K$ such that all the v_i split completely. Thus, for $x \in K_S$ we have

$$x \in \Delta \Leftrightarrow K_{v_i} = K_{v_i}(x^{1/p}) \text{ for all } v_i \in T \Leftrightarrow x \in (K_{v_i}^\times)^p \text{ for all } v_i \in T$$

This shows that Δ is the kernel of the map $K_S \to \prod_{v\in T} K_v^\times/(K_v^\times)^p$. We note also that under this map K_S maps to the units. □

For the set of primes T in the previous theorem let

$$J = \prod_{v\in S} (K_v^\times)^p \times \prod_{v\in T} K_v^\times \times \prod_{v\notin S\cup T} \mathcal{O}_{K_v}^\times.$$

Lemma 5.3.3. $J \cap K^\times = (K_{S\cup T})^p$

Proof. The inclusion $(K_{S\cup T})^p \subseteq J\cap K^\times$ is clear. To show the other inclusion we need to show that for any $y \in J \cap K^\times$ we have $C_K = N_{M|K}(C_M) \Leftrightarrow I_K = K^\times N_{M|K}(I_M)$ where $M = K(y^{1/p})$. From $I_K = K^\times I_{K,S}$ we are reduced to showing that for any $\alpha \in I_{K,S}$ there is an $x \in K^\times$ such that $\alpha/x \in N_{M|K}(I_M)$. The map

$$K_S \to \prod_{v\in T} \frac{U_v}{U_v^p}$$

is surjective and $|K_S/\Delta| = p^{s-1}$. This is also the order of the product so we get an isomorphism. Thus, we can find an $x \in K_S$ such that $(a/x)_v = (u_v)^p$ for every $v \in T$. These are all norms of their p-th root. For $v \in S$ we already had $y \in J\cap K^\times \subseteq (K_v^\times)^p$

so $M_w = K_v$. For $v \notin S \cup T$ we have that $M_w|K_v$ is unramified so every unit is a norm. It follows that α/x is a norm. Hence $C_K = N_{M|K}(C_M)$ and $M = K$ by the first inequality. Thus, $J \cap K^\times = (K_{S\cup T})^p$ as claimed.

□

Theorem 5.3.4. *Let T be as in the previous theorem and set $C_{K,S,T} = JK^\times/K^\times$. Then we have that $[C_K : C_{K,S,T}] = p$.*

Proof.

$$1 \longrightarrow (I_{K,S\cup T} \cap K^\times)/(J \cap K^\times) \longrightarrow I_{K,S\cup T}/J \longrightarrow (I_{K,S\cup T}K^\times)/(JK^\times) \longrightarrow 1$$

From the lemma and definitions this exact sequence can be rewritten as

$$1 \longrightarrow K_{S\cup T}/(K_{S\cup T})^p \longrightarrow \prod_{v\in S} K_v^\times/(K_v^\times)^p \longrightarrow C_K/C_{K,S,T} \longrightarrow 1$$

By the generalization of the unit theorem we have that $K_{S\cup T} \cong \mathbb{Z}^{2s-2} \times \mu(K)$ so $K_{S\cup T}/(K_{S\cup T})^p \cong (\mathbb{Z}/p\mathbb{Z})^{2s-1}$. The group in the middle has order $\prod_{v\in S} \frac{p^2}{|p|_v} = p^{2s}\prod_{v\in S}\frac{1}{|p|_v} = p^{2s}$. It follows that the order of the last group is $\frac{p^{2s}}{p^{2s-1}} = p$ as claimed. □

Theorem 5.3.5. *Let $C_{K,S,T}$ be as in the previous theorem. Then $C_{K,S,T} \subseteq N_{L|K}(C_L)$.*

Proof. It suffices to check $J \subseteq N_{L|K}(I_L)$. We can check this component by component. This is true for places $v \notin S \cup T$ as all such places are unramified and hence every unit is a norm. For the places $v \in S$ proposition 3.1.11 tells us that every element of $(K_v^\times)^p$ is a norm from $K_v(K_v^{1/p})$ and hence a norm from $L_w|K_v$. For the places $v \in T$ we see that $\Delta \in (K_v^\times)^p$ so $L_w = K_v$ so that every element of K_v is a norm. □

We have already outlined the proof earlier but its good to be explicit.

Proof of the second inequality in the reduced case. By the previous two results $[C_K : C_{K,S,T}] = p$ and $C_{K,S,T} \subseteq N_{L|K}(C_L)$. Thus,

$$p = [C_K : C_{K,S,T}] = [C_K : N_{L|K}(C_L)][N_{L|K}(C_L) : C_{K,S,T}]$$

from which it follows that $|\hat{H}^0(G(L|K), C_L)| = [C_K : N_{L|K}(C_L)]$ is finite and divides p as claimed.

□

5.4 An implication and the Hasse Norm

We immediately obtain what Neukirch calls the Global class field axiom.

Theorem 5.4.1 (Global Class Field Axiom). *Let $L|K$ be a cyclic extension of algebraic number fields. Then we have*

$$|\hat{H}^n(G(L|K), C_L)| = \begin{cases} [L : K] & \text{if } n = 0 \\ 1 & \text{if } n = -1 \end{cases}$$

Proof. Form the first and second inequality we get that $|\hat{H}^0(G(L|K), C_L)| = [L : K]$. This, combined with the fact that $h(C_L) = [L : K]$ gives the desired result. □

The Hasse norm theorem follows straight away

Theorem 5.4.2 (The Hasse norm theorem). *Let $L|K$ be a cyclic extension of algebraic number fields. An element $x \in K^\times$ is a norm if and only if it is a norm locally everywhere.*

Proof of the Hasse norm theorem. The short exact sequence

$$1 \longrightarrow L^\times \longrightarrow I_L \longrightarrow C_L \longrightarrow 1$$

Gives an exact Hexagon on the Tate cohomology groups and thus we get an exact sequence

$$\hat{H}^{-1}(G(L|K), C_L) \longrightarrow \hat{H}^0(G(L|K), I_L) \longrightarrow \hat{H}^0(G(L|K), L^\times).$$

However, we have $|\hat{H}^{-1}(G(L|K), C_L)| = 1$ by the Global Class Field Axiom. Moreover, we have already shown $\hat{H}^0(G(L|K), I_L) = \bigoplus_v \hat{H}^0(G_w, L_w^\times)$ in chapter 4.

It follows that the map

$$K^\times / N_{L|K} L^\times \longrightarrow \bigoplus_v K_v^* / N_{L_w|K_v} L_w^\times$$

is injective which is the claim of the theorem.

□

Chapter 6

The multinorm application

In this chapter we introduce some of the key definitions and facts and our main results.

6.1 The multinorm result

Definition. An étale algebra over a field k is a finite product of separable field extensions of k. It is also an algebra over k.

Definition. For an étale algebra L, the variety X_λ determined by the equation $N_{L|k}(x) = \lambda$ will be called a norm variety. In the case $\lambda = 1$ we will call the a norm one torus and denote it as $T_{L|k}$.

One observes $T_{L|k}$ acts transitively on X_λ for any λ. Indeed if $x, y \in X_\lambda$ then $z = xy^{-1} \in T_{L|k}$ and $zy = x$. Furthermore, this action is simply transitive since the stabilizer group of any element is the identity.

Definition. Let $L = \prod_{i=1}^{n} E_i$ be an etale algebra over k. Then the norm from L to k is defined as $N_{L|k}(x) = \prod_{i=1}^{n} N_{E_i|k}(x_i)$. This norm is also called a multinorm.

Definition. Let $L = \prod_{i=1}^{n} E_i$ be an etale algebra over k. An element $x \in k$ is said to be a local norm for the place v if it is a multinorm from $L \otimes_k k_v$.

Theorem 6.1.1 (Main Theorem)**.** *Let E/k be a dihedral extension of degree $2n$. Let E_i for $1 \leq i \leq n$ be the fields fixed by a reflection and let L be the étale algebra given by $L = \prod_{1 \leq i \leq n} E_i$. Then an element $x \in k$ is in the image of $N_{L/k}$ if it is a norm at every place of k.*

Before we prove this we state the following lemma and theorem which we will use in the proof.

Lemma 6.1.2. *Suppose that $\lambda \in k_v$ is a norm from $E_i \otimes k_v$. Then $\lambda \in K \otimes k_v$ is a norm from $E \otimes k_v$*

Proof. For an element $\alpha \in k$ the norm could be thought of as the determinant of the transformation $x \to x\alpha$. But the representation of this transformation remains the same under base change $k_v \to K \otimes k_v$ and hence the determinant also remains the same. □

We know introduce one of our key results which will help us prove our main theorem.

Theorem 6.1.3. *Let $E|k$ be a Galois extension with Galois group the dihedral group of order $2n$ so that $Gal(E|k) =< \sigma, \tau >$ with relations $\sigma^n = \tau^2 = 1$ and $\sigma\tau = \tau\sigma^{-1}$. Let $K = E^{\sigma}$, $E_1 = E^{\tau}$ and $E_2 = E^{\tau\sigma}$. Then if $c \in k$ with $c = N_{E|K}(\alpha)$ there is an $x \in E_1$ and $y \in E_2$ such that*

$$c = N_{E|K}(\alpha) = N_{E_1|k}(x) N_{E_2|k}(y)$$

Moreover, we can choose x and y so that $\alpha = xy$.

Proof. Let $f(x) = \prod_{i=1}^{n} \sigma^i(x)$ and $g(x) = x\tau(x)$.

We have $c = N_{E|K}(\alpha) = N_{E|K}(\tau(\alpha)) = \tau(c) = c$

It follows that $N_{E|K}(\frac{\alpha}{\tau(\alpha)}) = 1$ but then Hilbert 90 gives $\frac{\alpha}{\tau(\alpha)} = \frac{y'}{\sigma(y')}$ for some $y' \in E$

Now

$$\tau(\frac{\alpha}{\tau(\alpha)}) = \frac{\tau(\alpha)}{\alpha} = \frac{\tau(y')}{\tau\sigma(y')} = \frac{\sigma(y')}{y'}$$

But then

$$\frac{y'}{\tau\sigma(y')} = \frac{\sigma(y')}{\tau(y')} = \frac{\sigma(y')}{\sigma\tau\sigma(y')} = \sigma(\frac{y'}{\tau\sigma(y')})$$

It follows $\frac{y'}{\tau\sigma(y')} \in K$. Now notice that $\tau(\frac{y'}{\tau\sigma(y')}) = \frac{\tau(y')}{\sigma(y')} = \frac{\tau\sigma(y')}{y'}$ so we get

$$N_{K|k}(\frac{y'}{\tau\sigma(y')}) = g(\frac{y'}{\tau\sigma(y')}) = 1$$

then Hilbert 90 gives $\frac{y'}{\tau\sigma(y')} = \frac{\beta}{\tau(\beta)}$ for some $\beta \in K$. Now $\beta = \sigma(\beta)$ so we actually have $\frac{y'}{\tau\sigma(y')} = \frac{\beta}{\tau\sigma(\beta)}$ so that $\tau\sigma(\frac{y'}{\beta}) = \frac{y'}{\beta} \in E_2$. Set $y = \frac{y'}{\beta}$.

Then

$$\frac{\alpha}{\tau(\alpha)} = \frac{y'}{\sigma(y')} = \frac{y'(1/\beta)}{\sigma(y')(1/\beta)} = \frac{y}{\sigma(y)}$$

Now notice that $y \in E_2 = E^{\tau\sigma}$ gives $\sigma(y) = \sigma\tau\sigma(y) = \tau(y)$.

Then we have

$$\frac{\alpha}{\tau(\alpha)} = \frac{y}{\sigma(y)} = \frac{y}{\tau(y)} \implies \frac{\tau(\alpha)}{\tau(y)} = \frac{\alpha}{y} \in E_1$$

Set $x = \frac{\alpha}{y}$ then $\alpha = xy$ and it follows that

$$c = N_{E|K}(\alpha) = f(\alpha) = f(xy) = f(x)f(y) = N_{E_1|k}(x)N_{E_2|k}(y)$$

□

Remark. We actually also get $\{\alpha \in E | N_{E|K}(\alpha) \in k\} = \{ab | a \in E_1, b \in E_2\}$.

Proof of the main theorem. Suppose that $\lambda \in k$ is a norm locally from L for every place v of k. Then the lemma implies that its also a norm locally from E for every place v' of K. Now, the Hasse norm theorem implies implies that λ is a norm from $E|K$. Lastly, the previous theorem implies that λ is a norm from $L|k$. □

6.2 Weak approximation

Let k be a number field and X a variety defined over k.

Definition. We say that X satisfies weak approximation, if given a finite set of places S of k, the map

$$X(k) \to \prod_{v \in S}(X(k_v))$$

has a dense image.

Here, for $v \in S$ we give $X(k_v)$ the v-adic topology.

Example. Suppose that $X|k$ is a rational variety, i.e. $k(X)$ is a rational function field. Then X satisfies weak approximation.

We are interested in the question of which families of connected linear algebraic groups satisfy weak approximation.

Example. The group PGL_n is k-rational and hence satisfies weak approximation.

Example. Let $L|k$ be a cyclic extension of number fields and $T_{L|k}$ the norm 1 torus associated to $L|k$. Then $T_{L|k}$ is rational and satisfies weak approximation.

Unfortunately, even among the class of tori, there are examples of non-rational tori. For instance, the torus $T_{L|\mathbb{Q}}$ associated to $\mathbb{Q}(\sqrt{13}, \sqrt{17})|\mathbb{Q}$ is not rational. We now state the main result of this section.

Theorem 6.2.1 (Main weak approximation result)**.** *Let $E|k$ be a dihedral extension of degree $2n$ and E_i, for $1 \leq i \leq n$, be the fields fixed by reflection in $G = Gal(E|k)$. Let $L = \prod_{1 \leq i \leq n} E_i$. Then, the norm one torus $T_{L|k}$ satisfies weak approximation.*

This is a direct consequence of the main theorem in [2]. We indicate the main fact which enables us to use [2] and our theorem on the Hesse principle for multinorm to conclude the theorem above.

Definition. Let Γ_k denote the absolute Galois group of k so that $\Gamma_k = \mathrm{Gal}(k_s/k)$ with k_s the separable closure of k. A lattice is a finitely generated free abelian group. Given a finite group G, a G lattice is a lattice which is a $\mathbb{Z}[G]$-module. A Galois lattice is a lattice M on which Γ_k acts on continuously. Here we give Γ_k the pro-finite topology and we give M the discrete topology.

Given a torus T defined over k there is a Galois lattice over k namely the character lattice $T^* = \mathrm{Hom}(T, G_m)$. The torus T is determined by the the lattice T^* and this is an equivalence of categories between the category of k-tori and the category of Γ_k lattices. There is a minimal Galois extension $E|k$ which splits T. This extension has Galois group $G = \mathrm{Gal}(E|k)$ which is a finite quotient of Γ_k. Then the character lattice M becomes a G-lattice. Thus, to T we associated the algebraic object, namely, the G-lattice M, where G is a finite group.

Theorem 6.2.2 (Bayer-Fluckiger, Parimala)**.** *Let G be a finite group and M a G-lattice. Suppose for every torus T over a number field k with Galois splitting field $L|k$ with an isomorphism $\phi : G \to Gal(L|k)$ and character lattice M, Hasse principle holds for principal homogeneous space under T. Then weak approximation holds for T.*

We apply the theorem in the following set up. Let G be a dihedral group of order $2n$ and let $E|k$ be a dihedral extension and $\phi : G \to \mathrm{Gal}(L|k)$ an isomorphism. Let E_i for $1 \leq i \leq n$ be the fields fixed by a reflection and let L be the étale algebra over k given by $L = \prod_{1\leq i\leq n} E_i$ and let $T_{L|k}$ be the associated norm torus. Then $E|k$ is the minimal Galois splitting field over of $T_{L|k}$. Let M be the character lattice of $T_{L|k}$ which is a G-lattice. For any dihedral extension $E'|k'$ with $G(E'|k') \xrightarrow{\sim} G$ the lattice associated to the associated multinorm torus is isomorphic to M. In view of this, along with the theorem of Bayer-Parimala and our Hasse principle theorem we get the main weak approximation result.

Appendix A

Kummer theory

This section will closely follow chapter 1 section 5 of [6]. In fact, it will essentially be a summery of that chapter specializing to what we need for the thesis. The reader is certainly encouraged to read that section for a more in depth presentation.

Definition. Let K be a field containing the group μ_n of n-th roots of unity with n relatively prime to the characteristic of K. Then by a Kummer extension we mean an extension taking the form $L = K(\Delta^{1/n})$ with Δ a subgroup of $K^\times$ such that $(K^\times)^n \subseteq \Delta$.

One sees that the Kummer extension L of K is generated by $\alpha^{1/n}$ with $\alpha \in \Delta$. A Kummer extension is abelian of exponent n. This means that it is Galois with an abelian Galois group of exponent n. As a converse, we have the following proposition.

Proposition A.0.1. *If $L|K$ is an abelian extension of exponent n, then $L = K(\Delta^{1/n})$ with $\Delta = (L^\times)^n \cap K^\times$*

Proof. It's clear that $K(\Delta^{1/n}) \subseteq L$ so all we have to do is prove $L \subseteq K(\Delta^{1/n})$. We claim that that $L|K$ is the composite of its cyclic subextensions. Indeed, this is because it is the composite of all its abelian subextensions $L'|K$ each of which is the composite of its cyclic subextensions. This follows from the fact that $\mathrm{Gal}(L'|K)$ is a direct product of cyclic groups by the fundamental theorem of finitely generated abelian groups. Now, let $M|K$ be a cyclic subextension of $L|K$. Since $\mathrm{Gal}(L|K)$ has exponent n, we have $|\mathrm{Gal}(M|K)|$ divides n. It follows that $M = K(\alpha^{1/n})$ with $\alpha \in (L^\times)^n \cap K^\times$. Thus, $M \subseteq K(\Delta^{1/n})$ and we get $L \subseteq K(\Delta^{1/n})$. □

We know state the main result which we use in this thesis.

Theorem A.0.2. *The Kummer extensions $L|K$ are in one to one correspondence with subgroups Δ of $K^\times$ that contain $K^{\times n}$. If $L = K(\Delta^{1/n})$ then $\Delta = L^{\times n} \cap K$ and we have the following canonical isomorphism.*

$$Hom(Gal(L|K), \mu_n) \cong \Delta/K^{\times n}$$

Proof. See Neukirch [6]. □

Bibliography

[1] E. Bayer-Fluckiger, T.-Y. Lee, and R. Parimala. Hasse principles for multinorm equations. *Adv. Math. 356 (2019)*, pages 106818, 35 pp.

[2] Eva Bayer-Fluckiger and Raman Parimala. On unramified brauer groups of torsors over tori. *Doc. Math. 25 (2020)*, page 1263–1284.

[3] Kiran Kedlaya. Notes on class field theory, 2017.

[4] Serge Lang. *Algebra*. Springer, New York, NY, 2002. ISBN 9781461300410 146130041X.

[5] J.S. Milne. Class field theory (v4.03), 2020. Available at www.jmilne.org/math/.

[6] J. Neukirch. *Class Field Theory*. Grundlehren der mathematischen Wissenschaften. Springer Berlin Heidelberg, 2012. ISBN 9783642824654. URL `https://books.google.com/books?id=epLsCAAAQBAJ`.

[7] Jürgen Neukirch. *Algebraic Number Theory*. Grundlehren der Mathematischen Wissenschaften 322. Springer Berlin Heidelberg, 1999. ISBN 3-540-65399-6.