MASTER THESIS

CLASS FIELD THEORY
ARTIN RECIPROCITY LAW

Author: Loukas Papadogiannis

Supervisor: Univ.-Prof. Dipl.-Ing. Dr.
Michael Drmota

Institute of Discrete Mathematics and
Geometry
Vienna University of Technology

April 2018

Acknowledgements

This thesis was written under the supervision of Prof Michael Drmota (TU Vienna) as a work towards completion of my master in Mathematics studies. I also would like to mention my introduction to this very interesting mathematical area by Prof Joachim Mahnkopf (U Vienna).

We prefered not to give an introduction to cohomology theory, it would be meaningless since the reader may refer very easily to the literature, ie Neukirch [1], which is an excellent text, actually the reader may find out that we followed to a great extend his approach in the section of global class field theory. Also some structures of basic Algebra are a prerequisite for our text (for instance, some Galois theory), finally a rigorous approach of profinite groups is given by Neukirch [2].

The chapters of the text may be read sequentially of course, but still as soon as we have gained a background on the language of cohomology theory, the chapters of abstract class field theory followed by the chapter of global class field theory, constitute the main body of this work. Of course one should have an understanding on valuation theory. The chapter refering to L-series is an interesting approach, but analytical methods are not used nowadays any more in a purely algebraic topic. Also the parenthetical chapter 5 (Main theorems in terms of ideals) is not necessary for the following chapters.

Abstract

In this Thesis we give an introduction in Class Field Theory, proving Artin reciprocity law. The goal of class field theory is to describe the Galois extensions of a local or global field in terms of the arithmetic of the field itself. Apart from a few remarks about the more general cases, these notes will concentrate on the case of abelian extensions, which is the basic case. We give the framework of the theory introducing Abstract class field theory and we can see how this can be translated in the case of global class field theory using idele class groups as modules or multiplicative groups in the case of local class field theory. The language that we use is purely algebraic, with the exception of an analytic approach which is mostly redundant nowadays after much effort of the pioneers in that field to confront such a defect, as it was considered.

Contents

I have been reading Chevalley's new book on class field theory; I am not really doing research, just trying to cultivate myself.

Grothendieck, 1956

Chapter 1

Introduction

1.1 Class field theory

We first give the following definitions, before giving a short introduction of the motivation that led to the initiation of class field theory [7], and the scope of this thesis.

Definition 1.1.1. *A number field K is a finite degree field extension of the field of rational numbers $\mathbb{Q}$. Degree means the dimension of the field considered as a vector space over $\mathbb{Q}$.*

Definition 1.1.2. *Let L/K be extension of number fields. This extension is called abelian (cyclic), if L/K is Galois and $Gal(L/K)$ is abelian (cyclic).*

Class Field theory (CFT) emerged in the nineteenth century from at least three lines of inquiry. The first was the question of solvability by radicals: which algebraic numbers in $\overline{\mathbb{Q}}$ could be expressed using nth roots, sums, etc.? Abel and Galois showed that an irreducible polynomial $f(x) \in K[x]$ for some number field K, has roots that can be expressed via radicals if and only if the Galois group of the splitting field of f is solvable, that is, the splitting field of f is an iterated extension of abelian extensions such as

$$\mathbb{Q} \subseteq^{\mathbb{Z}/2\mathbb{Z}} \mathbb{Q}(\zeta_3) \subseteq^{\mathbb{Z}/3\mathbb{Z}} \mathbb{Q}(\zeta_3, \sqrt[3]{2})$$

where we have written the Galois group of each subextension above its respective inclusion. This criterion reduces the problem of identifying which algebraic numbers can be written in terms of radicals to understanding abelian (or even cyclic) extensions of number fields. Unfortunately, this problem has not been solved, though one can dream that cutting edge research is coming closer. However, abelian extensions of $\mathbb{Q}$ are known:

Theorem 1.1.3 (Kronecker-Weber)**.** *Every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some n, where ζ_n is a primitive nth root of unity.*

That is, if the splitting field of $f \in \mathbb{Q}[x]$ has an abelian Galois group, then all (equivalently, some) roots of f can be written as rational functions of ζ_n for some n. As a brief reminder, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$ (ie, the Euler totient function), and $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*$, with an element $m \in (\mathbb{Z}/n\mathbb{Z})^*$ acting as

$\zeta_n \mapsto \zeta_n^m$. CFT is essentially equivalent to the Kronecker-Weber theorem for $\mathbb{Q}$, but gives additional (though inexplicit) control of the situation for general number fields.

The second question was that of finding identities for algebraic numbers. As we will see, Gauss explained that non-obvious identities in $\overline{\mathbb{Q}}$ have non-trivial arithmetic consequences. For instance, identities like

$$\sqrt{2} = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \overline{\zeta_8} = (1+i)/\sqrt{2} + (1-i)/\sqrt{2}$$

$$\sqrt{-3} = \zeta_3 - \zeta_3^{-1} = \zeta_3 + \overline{\zeta_3} = (-1+\sqrt{-3})/2 + (-1-\sqrt{-3})/2$$

are predicted by the Kronecker-Weber theorem (since these numbers have an associated abelian Galois group $\mathbb{Z}/2\mathbb{Z}$). These arithmetic consequences indicate that we should attempt to understand such identities more fully.

Finally, the third area was solvability of Diophantine equations. The following is an example of a typical theorem:

Theorem 1.1.4 (Hasse Principle)**.** *Let K be a number field, and*

$$q(x_1, .., x_n) = \sum_i a_i x_i^2 + \sum_{i \neq i} a_{ij} x_i x_j$$

for $a_i, a_{ij} \in K$. Then for any $y \in K$, the equation

$$q(x_1, .., x_n) = y$$

has a solution if and only if it does in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p.

Checking for solutions over $\mathbb{R}$ is easy, and over $\mathbb{Q}_p$ the problem reduces to elementary congruence properties; it turns out that this problem can be solved entirely algorithmically. We can recast such problems as asking if $y \in \mathbb{Q}$ is a norm in a quadratic extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, at least for the norm $N(x+y\sqrt{d}) = x^2 - dy^2$ (where $x, y \in \mathbb{Q}$), which is the hardest case of the above anyways. This question, and the broader idea of connecting local and global, will make a reappearance.

1.2 Aim of Class field theory

The aim of class field theory is the following[1]:

Let $K/\mathbb{Q}$ be a number field, then:
• clarify all abelian extensions L of K by data which are attached to K.
• describe the splitting of primes in an abelian extension L of K by the datum in K which is attached to L.

[1]The object of class field theory is to show how the abelian extensions of an algebraic number field K can be determined by objects drawn from our knowledge of K itself; or if one prefers to present things in dialectic terms, how a field contains within itself the elements of its own transcending.

Chevalley 1940

• describe the Galois group of an abelian extension L of K by the datum in K which is attached to L, this obtained by **Artin reciprocity law**.

At the centre of our analysis are the **Norm inequalities**:

Let L/K be a cyclic extension, then:

• 1) $[J_K(\mathfrak{m}) : N_{L/K} J_L(\mathfrak{m}) P_K(\mathfrak{m})] \geqslant [L : K]$

• 2) $[J_K(\mathfrak{m}) : N_{L/K} J_L(\mathfrak{m}) P_K(\mathfrak{m})] \leqslant [L : K]$

In these, $J_K(\mathfrak{m})$ means the group of fractional ideal "prime to $\mathfrak{m}$" and $P_K(\mathfrak{m})$ means the group of principal ideal "prime to $\mathfrak{m}$" and $\equiv 1 \ (mod\ \mathfrak{m})$" (ie locally the elements are units at all places v dividing $\mathfrak{m}$ and are even $\equiv 1 \ (mod\ v^{\mathfrak{m}_v})$, the ideal $\mathfrak{m}$ is defined in 5.1.1. We can also identify in our later analysis $i(K_{\mathfrak{m},1})$ with $P_K(\mathfrak{m})$. In chapter 5, we give the relevant details. The proof of these inequalities lies at the centre of CFT!

Our first goal is to prove the second Norm index inequality using analytic methods. For the first inequality we would have to use techniques from

• Ideles theoretic foundations of number theory
• (some) group cohomology
• number theory of extensions of local fields...

we will skip that second step and proceed further instead, to another approach based absolutely on cohomology theory..

Towards this task we shall give some introduction to valuation theory and proceed further to abstract class field theory, where we introduce the notion of "profinite group" and define "class formation". The main framework of our theory is thus established abstractly and the difficulty will be to prove that the properties of "class formation" can be transfered from the G-module A of abstract class field theory, to the idele class group of global class field theory, or multiplicatice group in the case of local class field theory. We start with..

Chapter 2

L-series

We shall prove now the second Norm index inequality, following the ideas of Lang [6] and a very nice lecture that I attended at the university of Vienna by Prof. Joachim Mahnkopf [8], using analytic methods and extracting in this framework our relevant theorem 2.2.4. Analytic methods to be given to theorems that are purely algebraic in form are mostly redundant nowadays and were considered as a defect until 1940, were purely algebraic proofs were given after much effort by Chevalley.

Let $K/\mathbb{Q}$ be a number field, and O_K be the ring of integers in our number field K.

Definition 2.0.1. *Let R be a commutative ring. An ideal $\mathfrak{p} \in R$ is a prime ideal if*

$\mathfrak{p} \neq R$ *and*

$ab \in \mathfrak{p} \Rightarrow \quad a \in \mathfrak{p}$ *or* $b \in \mathfrak{p} \quad$ *for* $a, b \in R$

Definition 2.0.2. *Let $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{m}_{\mathfrak{p}}} \leq O_K$ be an ideal.*

A Dirichlet character of level $\mathfrak{m}$ or modulo $\mathfrak{m}$ is a morphism of groups

$$\chi : J(\mathfrak{m})/P_{\mathfrak{m}} \to S^1 = \{z \in \mathbb{C} : |z| = 1\} \tag{2.1}$$

Definition 2.0.3. *: Let χ be a Dirichlet character of level $\mathfrak{m}$. Then the series*

$$L(\chi, s) = L_{\mathfrak{m}}(\chi, s) = \sum_{\mathfrak{u} \leq O_K, (\mathfrak{u}, \mathfrak{m}) = 1} \chi(\mathfrak{u})/N(\mathfrak{u})^s \tag{2.2}$$

$s \in \mathbb{C}$

is called the Dirichlet series attached to χ, ($N = N_{\mathbb{Q}}^K$).

Remark 2.0.4. *: If $\chi = id$ is the trivial Dirichlet character of level 1, then*

$$L(\chi, s) = L_1(id, s) = \sum_{\mathfrak{u} \leq O_K} 1/N(\mathfrak{u})^s =: Z_K(s)$$

is the Dedekind zeta function $Z_K(s)$ of K.

If in addition $K = \mathbb{Q}$, we obtain

$$L(\chi, s) = L_1(id, s) = \sum_{n \in N} 1/n^s =: \zeta(s)$$

the Riemann zeta function.

2.1 Some analytic methods

Lemma 2.1.1. *Let $\delta \in \mathbb{R}$, $\delta > 0$, then the infinite product*

$$\prod_{\mathfrak{p} \leq O_K, \mathfrak{p}\ primideal} \frac{1}{1 - N(\mathfrak{p})^{-s}}$$

converges absolutely and uniformly for $s \in \mathbb{C}$ satisfying $Re(s) \geqslant 1 + \delta$.

Proof. We write $s = \sigma + it$,we have to show that the infinite series

$$\sum_{\mathfrak{p} \leq O_K, \mathfrak{p}\ primideal} \frac{1}{1 - N(\mathfrak{p})^{-s}} - 1$$

converges absolutely and uniformly for $s \in \mathbb{C}$ with $Re(s) \geqslant 1 + \delta$.

Remark: $\prod_{k=1}^{\infty} 1 + a_k$ converges absolutely $\Leftrightarrow \sum_{k=1}^{\infty} a_k$ converge absolutely.

and we want to show that

$$\sum_{\mathfrak{p} \leq O_K, \mathfrak{p} primideal} \frac{1}{1 - N(\mathfrak{p})^{-s}} - 1 \tag{2.3}$$

converges absolutely and uniformly in $\{s \in \mathbb{C} : Re(s) \geqslant 1 + \delta, \delta > 0\}$.

Let $\mathfrak{p} \leq O_K$ be prime ideal with $\mathfrak{p}|p$, $(p \in \mathbb{N})$ and put $f = f_{\mathfrak{p}|p}$. Then we obtain

$$|\frac{1}{1 - N(\mathfrak{p})^{-s}} - 1| = |\frac{N(\mathfrak{p})^{-s}}{1 - N(\mathfrak{p})^{-s}}| = |\frac{1}{\underbrace{N(\mathfrak{p})^{s}}_{p^{fs}} - 1}| = |\frac{1}{p^{fs} - 1}| \leqslant |\frac{1}{p^{f\sigma} - 1}| \leqslant$$

$$\frac{1}{p^{\sigma} - 1} \leqslant \frac{1}{(p-1)^{\sigma}}$$

Since for any prime number $p \in \mathbb{N}$ there are at most $n = [K : \mathbb{Q}]$ many prime ideals $\mathfrak{p} \leq O_K$, sth $\mathfrak{p}|p$, we obtain

$$\sum_{\mathfrak{p} \leq O_K} |\frac{1}{1 - N(\mathfrak{p})^{-s}} - 1| \tag{2.4}$$

$$= \sum_{p \in N, p\ prime} \sum_{\mathfrak{p}|p} |\frac{1}{1 - N(\mathfrak{p})^{-s}} - 1| \leqslant \sum_{p} \sum_{\mathfrak{p}|p} \frac{1}{(p-1)^{\sigma}} \leqslant$$

$$n \cdot \sum_{p \in N} \frac{1}{(p-1)^{\sigma}} \leqslant n \cdot \sum_{k \in N} \frac{1}{k^{\sigma}} \leqslant n \cdot \sum_{k \in N} \frac{1}{k^{1+\delta}}$$

The last sum converges $\Rightarrow$ 2.4 converges absolutely and does not depend on s when $(Re(s) \geqslant 1+\delta) \Rightarrow$ 2.4 converges uniformly. $\square$

Proposition 2.1.2. *Let χ be a Dirichlet character of level $\mathfrak{m}$*

- *1) Let $\delta \in \mathbb{R}$, $\delta > 0$. Then the Dirichlet series*

$$\sum_{\substack{\mathfrak{u} \leq \mathcal{O}_K \\ (\mathfrak{u},\mathfrak{m})=1}} \frac{\chi(\mathfrak{u})}{N(\mathfrak{u})^s} = L_{\mathfrak{m}}(\chi, s)$$

  $\mathfrak{u}$ are integral ideals, not prime ideals

  converges absolutely and uniformly in the set $\{s \in \mathbb{C} : Re(s) \geqslant 1+\delta\}$

- *2) For all $s \in \mathbb{C}$ sth $Re(s) > 1$ we have*

$$L(\chi, s) = \prod_{\mathfrak{p} \leq O_K, (\mathfrak{p},\mathfrak{m})=1, \mathfrak{p} prime ideal} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}}$$

this product localizes over prime ideals.. and is the "Euler product expansion of $L(\chi, s)$".

Proof. 1) Let A_N, $N \in \mathbb{N}$ be the set of all ideals $\mathfrak{u} \leq O_K$ sth $(\mathfrak{u}, \mathfrak{m}) = 1$ and $\mathfrak{u}$ divisible only by prime ideals $\mathfrak{p} \leq O_K$ sth $N(\mathfrak{p}) \leqslant N$. We denote by $\mathfrak{p}_1, .., \mathfrak{p}_r \leq O_K$ the prime ideals with $N(\mathfrak{p}_i) \leqslant N$ and $(\mathfrak{p}, \mathfrak{m}) = 1$
then we obtain

$$\prod_{\mathfrak{p}, (\mathfrak{p},\mathfrak{m})=1, N(\mathfrak{p}) \leqslant N} \frac{1}{1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}} =$$

$$\prod_{\mathfrak{p}, (\mathfrak{p},\mathfrak{m})=1, N(\mathfrak{p}) \leqslant N} \sum_{k \in N} \chi(\mathfrak{p})^k N(\mathfrak{p})^{-ks} =$$

$$\sum_{k_1, .., k_r \in N_0} \prod_{i=1}^{r} \chi(\mathfrak{p}_i)^{k_i} N(\mathfrak{p}_i)^{-k_i s} =$$

$$\sum_{k_1, .., k_r \in N_0} \chi(\underbrace{\prod_{i=1}^{r} \mathfrak{p}_i^{k_i}}_{=: \mathfrak{u} \leq O_K}) N(\prod_{i=1}^{r} (\mathfrak{p}_i^{k_i})^{-s}) =$$

(by definition χ, N are multiplicative and the sum runs exactly over A_N)

$$= \sum_{\mathfrak{u} \in A_N} \chi(\mathfrak{u}) N(\mathfrak{u})^{-s} \tag{2.5}$$

Let now $s \in \mathbb{C}$ with $\sigma = Re(s) \geqslant 1 + \delta$, we obtain

$\sum_{\mathfrak{u}\in A_N} |\chi(\mathfrak{u})N(\mathfrak{u})^{-s}| = \sum_{\mathfrak{u}\in A_N} |N(\mathfrak{u})^{-\sigma}| \leqslant \sum_{\mathfrak{u}\in A_N} N(\mathfrak{u})^{-(1+\delta)}$

$\underbrace{=}_{2.5} \prod_{\mathfrak{p},(\mathfrak{p},\mathfrak{m})=1,N(\mathfrak{p})\leqslant N} \frac{1}{1-N(\mathfrak{p})^{-(1+\delta)}}$

This product converges absolutely and uniformly in $\{s \in \mathbb{C} : Re(s) \geqslant 1+\delta\}$ by the above Lemma for $N \to \infty$. Hence $\sum_{\mathfrak{u}\in A_N} \chi(\mathfrak{u})N(\mathfrak{u})^{-s}$ converges absolutely and uniformly for $N \to \infty$.

2)

$$\prod_{\mathfrak{p}\leq O_K,(\mathfrak{p},\mathfrak{m})=1,N(\mathfrak{p})\leqslant N} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}} = \sum_{\mathfrak{u}\in A_N,\mathfrak{u}\leq O_K} \frac{\chi(\mathfrak{u})}{N(\mathfrak{u})^s} \tag{2.6}$$

In the above Lemma and in part 1) we have seen that both sides of 2.6 converge for $N \to \infty$. In fact, the left hand side converges obviously to $\prod_{\mathfrak{p}\leq O_K,(\mathfrak{p},\mathfrak{m})=1} \frac{1}{1-\chi(\mathfrak{p})N(\mathfrak{p})^{-s}}$ and the right hand side converges obviously to $\sum_{\mathfrak{u}\leqslant O_K,(\mathfrak{u},\mathfrak{m})=1} \frac{\chi(\mathfrak{u})}{N(\mathfrak{u})^s}$

$\Rightarrow$ claim. □

Corollary 2.1.3. *For any Dirichlet character χ of level m it holds that the Dirichlet series $L(\chi, s)$ represents a holomorphic function in the set $Re(s) > 1$*

Proof. Use that

- $\cdot$ $L(\chi, s) = \sum_{\mathfrak{u}} \frac{\chi(\mathfrak{u})}{N(\mathfrak{u})^s}$ converges uniformly in any $Re(s) \geqslant 1+\delta$, $(\delta > 0)$
- $\cdot$ uniform limit of holomorphic functions is again holomorphic. □

Notation 2.1.4. *: The holomorphic function in $Re(s) > 1$ which is defined by $L(\chi, s)$ is called the Dirichlet L-function attached to χ.*

Theorem 2.1.5. *1) Let $\chi : J(\mathfrak{m})/P_{\mathfrak{m}} \to S^1$ be a Dirichlet character, $\chi \neq id$. Then $L(\chi, s)$ has a holomorphic continuation to $s \in C$*
2) If $\chi = id$ of level m then $Z_K(s) := L(\chi, s)$ ("Zeta function of K") has a meromorphic continuation to $s \in C$ with only a simple pole at $s = 1$ with Residue equal to $|J(\mathfrak{m})/P_{\mathfrak{m}}|$.

Remark 2.1.6. *: The proof of 2.1.5 is long deep and difficult.*
we will only need existence of an analytic continuation to a set $Re(s) \geqslant 1-\delta$, $(\delta > 0)$.
Analytic continuation to some range $Re(s) \geqslant 1-\delta$, $(\delta > 0)$ is much easier but still difficult (we will save the time of doing this).
In particular we can study the value $L(\chi, s)$ at $s = 1$.

Notation 2.1.7. *: If f, g are meromorphic functions in a neighbourhood of $s = 1$, then we write $f \backsim g$ to denote that there is a holomorphic function $\xi(s)$ sth*

$$f(s) = g(s) + \xi(s)$$

(ie) f and g have the same principal part in their Laurent expansions.

Proposition 2.1.8. *For all Dirichlet characters χ of level m it holds that*

$$\underbrace{\log L(\chi, s)}_{is\ \ analytic\ \ in\ \ neighbourhood\ \ of\ \ s=1} \backsim \sum_{\mathfrak{p} \leq O_K, Primideal, (\mathfrak{p},\mathfrak{m})=1} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$$

Proof. Applying log to Euler product of $L(\chi, s)$ we obtain for $s \in \mathbb{C}$ with $Re(s) > 1$

$$\log L(\chi, s) = - \sum_{\mathfrak{p} \leq O_K, (\mathfrak{p},\mathfrak{m})=1} \log(1 - \chi(\mathfrak{p}) N(\mathfrak{p})^{-s})$$

since the

$$|\chi(\mathfrak{p}) N(\mathfrak{p})^{-s}| = N(\mathfrak{p})^{-\sigma} = p^{-\sigma f} \leqslant p^{-\sigma} \leqslant 1 \ \ since \ \ (\sigma > 1)$$

we see that the logarithm series

$$\log(1 - z) = - \sum_{k \geqslant 1} \frac{1}{k} z^k$$

converges at $z = \chi(\mathfrak{p}) N(\mathfrak{p})^{-s}$

plugging in the power series of log we further obtain

$$\log L(\chi, s) = \sum_{\mathfrak{p} \leq O_K, (\mathfrak{p},\mathfrak{m})=1} \sum_{k \geqslant 1} \frac{1}{k} (\chi(\mathfrak{p}) N(\mathfrak{p})^{-s})^k$$

For $Re(s) > 1$ the sum $\sum_{\mathfrak{p} \leq O_K} ...$ as well as the sum $\sum_{k \geqslant 1} \frac{1}{k} z^k$ converge absolutely, therefore we may rearrange as follows

$$\log L(\chi, s) = \sum_{(\mathfrak{p},\mathfrak{m})=1} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} + \sum_{k \geqslant 2} \sum_{(\mathfrak{p},\mathfrak{m})=1} \frac{1}{k} \frac{\chi(\mathfrak{p})^k}{N(\mathfrak{p})^{sk}} \tag{2.7}$$

since

- 1) $|\frac{1}{k} \frac{\chi(\mathfrak{p})^k}{N(\mathfrak{p})^{sk}}| \leqslant \frac{1}{k} \frac{1}{p^{k\sigma}}$ where $(\mathfrak{p}|p)$
- 2) The series $\sum_{k \geqslant 2} \frac{1}{k} \frac{1}{p^{k\sigma}}$ converges (absolutely) by the quotient criterion for $\sigma > \frac{1}{2} + \delta$, $(\delta > 0)$
- 3) there are at most $N = [K : \mathbb{Q}]$ many prime ideals lying above $p \in \mathbb{N}$

we obtain that

$$\sum_{k \geqslant 2} \sum_{(\mathfrak{p},m)=1} |\frac{1}{k} \frac{\chi(\mathfrak{p})^k}{N(\mathfrak{p})^{sk}}| \leqslant N \cdot \sum_{k \geqslant 2} \frac{1}{k} \frac{1}{p^{k\sigma}} < \infty$$

hence the series converges absolutely and uniformly in $Re(s) > \frac{1}{2} + \delta$

Thus the second summand in 2.7 is holomorphic in $Re(s) > \frac{1}{2} + \delta$

$\Rightarrow$ claim. $\square$

2.2 The second Norm index inequality

We now come to the statement of our main theorem, the proof of the second norm index inequality in terms of ideals using analysis, we shall prove later on that this index is equal to the analogous index in terms of idele class groups. For the first norm index inequaity we shall have to use techniques from ideles theoretic foundations of number theory, (some) group cohomology and number theory of extensions of local fields. We shall avoid to do so following the framework of abstract class field theory as we develop in the next chapters, proving both inequalities through cohomology theory.

Let L/K extension of number fields with $Gal(L/K) = G$ and let

$$\mathfrak{m} = \prod_{\mathfrak{p} \leq O_K, prime} \mathfrak{p}^{\mathfrak{m}_\mathfrak{p}} \in J_K \tag{2.8}$$

Aim: Prove

$$[J_K(\mathfrak{m}) : P_\mathfrak{m} N_K^L J_L(\mathfrak{m})] \leqslant [L : K]$$

to simplify notation we put $N(\mathfrak{m}) = N_K^L J_L(\mathfrak{m})$

Definition 2.2.1. *: Let G be a finite abelian group. A character of G is a morphism of groups $\chi : G \to S^1$. We denote $\widehat{G}$ the set of all characters of G.*

Remark 2.2.2. *:*

- *1) Dirichlet characters are characters of the (finite abelian) group $J_K(\mathfrak{m})/P_\mathfrak{m}$*
- *2) $\widehat{G}$ is group wrt $(\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g)$*

Lemma 2.2.3. *1) Let $g \in G$ then*

$$\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} |G| & if \quad g = 1 \\ 0 & else \end{cases}$$

2) Let $\chi \in \widehat{G}$, then

$$\sum_{g \in G} \chi(g) = \begin{cases} |G| & if \quad \chi = id \\ 0 & else \end{cases}$$

Proof. : we omit the first proof, we will not need it.. as to the second we have..

assume $\chi \neq id$. Then there is $h \in G$ sth $\chi(h) \neq 1$, we then obtain trivially

$$\sum_{g\in G}\chi(g) \underbrace{=}_{g\mapsto gh} \sum_{g\in G} \underbrace{\chi(gh)}_{runs\ again\ over\ the\ whole\ group} = \underbrace{\chi(h)}_{\neq 1}\sum_{g\in G}\chi(g)$$

$$\Rightarrow \sum_{g\in G}\chi(g) = 0 \qquad \square$$

and now we can come to our final

Theorem 2.2.4. *Let L/K be any extension of number fields and assume that the cycle $\mathfrak{m} = \prod_{\mathfrak{p}\leq O_K} \mathfrak{p}^{m_\mathfrak{p}}$ is divisible by all prime ideals $\mathfrak{p} \leq O_K$ which ramify in L. Then*

$$[J_K(\mathfrak{m}) : P_\mathfrak{m} N_K^L J_L(\mathfrak{m})] \leqslant [L : K]$$

Proof. We put $H := P_\mathfrak{m} N_K^L J_L(\mathfrak{m}) \leq J_K(\mathfrak{m})$ and $h := [J_K(\mathfrak{m}) : H]$

Let χ be an arbitrary character of the (finite and abelian) group $J_K(\mathfrak{m})/H$. Then χ induce a character of the generalized class group $J_K(\mathfrak{m})/P_\mathfrak{m}$ of level $\mathfrak{m}$. We assume $\chi \neq id$, hence the L-series $L(\chi, s)$ is holomorphic at $s = 1$. Thus we can write

$$L(\chi, s) = (s-1)^{m_\chi} \cdot g(s,\chi) \quad m_\chi \geqslant 0 \ \ (because\ it\ is\ holomorphic)$$

where $g(s,\chi)$ is holomorphic at $s = 1$.

Applying log we obtain

$$\log L(s,\chi) = m_\chi \log(s-1) + \underbrace{\log(g(s,\chi))}_{holomorphic} \sim -m_\chi \cdot \log\frac{1}{s-1} \qquad (\chi \neq id)$$

On the other hand we have seen in the Proposition of the previous section that for all characters χ

$$\log L(s,\chi) \sim \sum_{\mathfrak{p}\leq O_K, prime, (\mathfrak{p},\mathfrak{m})=1} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} =$$

$$\sum_{\mathfrak{p}\in J_K(\mathfrak{m}), \mathfrak{p}\ prime\ ideal} \chi(\mathfrak{p})N(\mathfrak{p})^{-s} =$$

$$\underbrace{\sum_{\mathbb{k}\in J_K(\mathfrak{m})/H}}_{sum\ over\ cosets} \sum_{\mathfrak{p}\in\mathbb{k},\ prime\ ideals} \underbrace{\chi(\mathfrak{p})}_{constant\ on\ \mathbb{k}=\mathfrak{p}\cdot H} \cdot N(\mathfrak{p})^{-s} =$$

$$\sum_{\mathbb{k}\in J_K(\mathfrak{m})/H} \chi(\mathbb{k}) \sum_{\mathfrak{p}\in\mathbb{k}, primeideal} N(\mathfrak{p})^{-s}$$

Summing over all characters $\chi \in \widehat{J_K(\mathfrak{m})/H}$ we thus obtain

$$\log \zeta_K(s) + \sum_{\chi \neq id} \log L(\chi, s) \sim$$

$$\sum_{\chi \in \widehat{J_K(\mathfrak{m})/H}} \sum_{\Bbbk \in J_K(\mathfrak{m})/H} \chi(\Bbbk) \sum_{\mathfrak{p} \in \Bbbk, prime ideal} N(\mathfrak{p})^{-s} = \begin{cases} h & \Bbbk = 1 = H (\in J_K(\mathfrak{m})/H) \\ 0 & \Bbbk \neq 1 = H \end{cases}$$

$$= h \cdot \sum_{\mathfrak{p} \in H, \mathfrak{p} \text{ prime ideal}} N(\mathfrak{p})^{-s}$$

Combining now we have.. (note that $\log \zeta_K(s) \sim \frac{1}{s-1}$)

$$(1 - \sum_{\chi \neq id} m_\chi) \log \frac{1}{s-1} \sim h \cdot \sum_{\mathfrak{p} \in H, \mathfrak{p} \, prime ideal} N(\mathfrak{p})^{-s} \tag{2.9}$$

we denote by $S_{L/K} = S^{\mathfrak{m}}_{L/K}$ the set of all prime ideals $\mathfrak{p} \leq O_K$ sth $(\mathfrak{p}, \mathfrak{m}) = 1$ and $\mathfrak{p}$ is fully decomposed in L.

Then

- $\mathfrak{p} \in S_{L/K} \Leftrightarrow degk := e_{k|\mathfrak{p}} f_{k|\mathfrak{p}} = 1$ for all $k|\mathfrak{p}$
- if $\mathfrak{p} \in S_{L/K}$ and $k|\mathfrak{p}$ then $N^L_K(k) (= \mathfrak{p}^{f_{k|\mathfrak{p}}}) = \mathfrak{p}$

Thus $\mathfrak{p} \in N^L_K J_L(\mathfrak{m}) \leq H$

$\Rightarrow S_{L/K} \subseteq H$

ie H contains all fully decomposed prime ideals.

Using this we obtain

$$h \cdot \sum_{\mathfrak{p} \in H, \mathfrak{p} \, prime} N(\mathfrak{p})^{-s} \geqslant h \cdot \sum_{\mathfrak{p} \in S_{L/K} (\subseteq H)} N(\mathfrak{p})^{-s} = \frac{h}{N} \sum_{k \leq O_L, degk = 1, (k, \mathfrak{m}) = 1} N(k)^{-s} \tag{2.10}$$

where $N := [L : K]$, note that over any $\mathfrak{p} \in S_{L/K}$ there are precisely $N-$many prime ideals $k \leq O_L$ and any such k has degree $degk = 1$.

As in Proposition in previous section (and its proof) we see that the following holds

$$\log \frac{1}{1-s} \sim \log \zeta_L(s) \sim \sum_{k \leq O_L, k \, prime} N(k)^{-s}$$

$$= \sum_{k \leq O_L, degk = 1} N(\mathfrak{p})^{-s} + \underbrace{\sum_{k \leq O_L, degk \geqslant 2} \underbrace{N(\mathfrak{p})^{-s}}_{p^{-fs}, f \geqslant 2}}_{holomorphic \, in \, Re(s) \geqslant \frac{1}{2}}$$

Thus we obtain

$$\sum_{k\leq O_L, deg k=1} N(k)^{-s} \sim \log \frac{1}{s-1}$$

if we plug this in equation 2.10 we obtain

$$h \cdot \sum_{\mathfrak{p}\in H, \mathfrak{p}\ prime\ ideal} N(\mathfrak{p})^{-s} \geqslant \frac{h}{N} \cdot \log \frac{1}{s-1} + \underbrace{g_1(s)}_{holomorphic\ \ at\ s=1}$$

Together with 2.9 this yields

$$(1 - \sum_{\chi\neq id, \chi\in \widehat{J(\mathfrak{m})/H}} m_\chi) \log \frac{1}{s-1} \geqslant \frac{h}{N} \log \frac{1}{s-1} + \underbrace{g_2(s)}_{holomorphic\ at\ s=1}$$

we obtain

$$(1 - \sum_{\chi\neq id} m_\chi) \geqslant \frac{h}{N} - \frac{g_2(s)}{\log(s-1)}$$

we now let $s \to 1+$, thus $\log(s-1) \to -\infty$, but $g_2(s)$ is holomorphic in the neighborhood of $s = 1$ thus bounded and we further obtain

$$\frac{g_2(s)}{\log(s-1)} \to 0$$

$$\Rightarrow (1 - \sum_{\chi\neq id, \chi\in \widehat{J(\mathfrak{m})/H}} m_\chi) \geqslant \underbrace{\frac{h}{N}}_{>0}$$

since $\frac{h}{N} > 0$ (strictly bigger) and $m_\chi \geqslant 0$ for all $\chi \neq id$, this implies that $m_\chi = 0$ for all $\chi \neq id$ and thus we find

$$1 \geqslant \frac{h}{N} \quad or \quad N \geqslant h$$

ie

$$[L : K] \geqslant [J_K(\mathfrak{m}) : P_{\mathfrak{m}} N_K^L J_L(\mathfrak{m})]$$

□

The ideal-theoretic versions of these inequalities were already used in the proof of the main theorems of class field theory by Takagi. These analytic methods are redundant when working with ideles.

2.3 Artin map

The goal of class field theory is to describe the Galois extensions of a local or global field in terms of the arithmetic of the field itself. For abelian extensions the theory was developed between roughly 1850 and 1930 by Kronecker[1],

[1] **KRONECKER** (1823–1891). He developed an alternative to Dedekind's ideals. He also had one of the most beautiful ideas in mathematics for generating abelian extensions of number fields (the Kronecker liebster Jugendtraum)

Weber[2], Hilbert[3], Takagi[4], Artin[5], Hasse[6] and others, we refer to [4]. For nonabelian extensions the first indication of the shape the theory should take is in a letter from Langlands to Weil in 1967. In recent years there has been much progress in the nonabelian local and function field cases, but less in the number field case. Beginning about 1980, abelian class field theory has been succesfully extended to higher dimensional fields. Throughout by an extension L of a number field K we mean that L is contained in some fixed algebraically closed field containing K. For this and the next section we can refer to Milne [4] for more details.

Let's recall that a prime $\mathfrak{p}$ of O_K factors in an extension L of K as

$$\mathfrak{p}O_L = \mathfrak{F}_1^{e_1}..\mathfrak{F}_g^{e_g}$$

where $\mathfrak{F}_i$ are the prime ideals of O_L such that $\mathfrak{F}_i \cap O_K = \mathfrak{p}$ and $e_i \geq 1$ moreover $n = e_1 f_1 + .. + e_g f_g$, $n = [L : K]$, $f_i = [O_L/\mathfrak{F}_i : O_K/\mathfrak{p}]$ called the inertia degree and e_i the ramification index. When $e_i > 1$ for some i, the prime $\mathfrak{p}$ is said to ramify in L, when $e_i = f_i = 1\ \forall i : \mathfrak{p} = \mathfrak{F}_1..\mathfrak{F}_n$ the prime $\mathfrak{p}$ is said to split in L (completely).
When L/K is Galois the $e_i{}'s$ are equal to say e and $f_i{}'s$ to say f, and

$$\mathfrak{p}O_L = (\mathfrak{F}_1..\mathfrak{F}_g)^e, \quad n = efg$$

Let $Spl(L/K)$ be the set of primes of K splitting in L. Towards the end of the 19^{th} century Frobenius proved the following statement:

Theorem 2.3.1. *when L/K is Galois, the set $Spl(L/K)$ has density $1/[L : K]$ in the set of all primes*

Note: For any Galois extension L/K of number fields, Frobenius attached a conjugacy class $(\mathfrak{p}, L/K)$ of elements in $G = Gal(L/K)$ to each prime ideal $\mathfrak{p}$ of K unramified in L and conjectured that the density of the primes giving a fixed conjugacy class C is $|C|/|G|$. By construction the elements in $(\mathfrak{p}, L/K)$ have order $f(\mathfrak{p})$ in G and so the statement applied to the trivial conjugacy class gives 2.3.1. Frobenius was only able to prove a weaker statement than his conjecture (sufficient for 2.3.1), in which certain conjugacy classes are grouped together, and the conjecture was proved by Chebotarev in 1926.

If K is a finite algebraic number field, we mean by the primes $\mathfrak{p}$ of K, the classes of equivalent valuations of K, where we distinguish between the finite $\mathfrak{p}$ associated with the nonarchimedean valuations of K, that correspond bijectively to the prime ideals of K (we use the same symbol $\mathfrak{p}$), and the infinite

[2]**WEBER** (1842–1913). He found the correct generalization of "class group" to allow for ramification. Made important progress in class field theory and the Kronecker Jugendtraum

[3]**HILBERT** (1862–1943). He wrote a very influential book on algebraic number theory in 1897, which gave the first systematic account of the theory. Some of his famous problems were on number theory, and have also been influential

[4]**TAKAGI** (1875–1960). He proved the fundamental theorems of abelian class field theory, as conjectured by Weber and Hilbert

[5]**ARTIN** (1898–1962). He found the "Artin reciprocity law", which is the main theorem of class field theory (improvement of Takagi's results). Introduced the Artin L-series

[6]**HASSE** (1898–1979). He gave the first proof of local class field theory, proved the Hasse (local-global) principle for all quadratic forms over number fields, and contributed to the classification of central simple algebras over number fields

primes,that distinguish further between the real and complex ones.
The real primes correspond bijectively to the different embeddings of K into $\mathbb{R}$, and the complex primes correspond bijectively to the pairs of complex conjugate embeddings of K into $\mathbb{C}$, we observe that two conjugate embeddings of K into $\mathbb{C}$ produce the same valuation of K (we write $\mathfrak{p}|\infty$, $\mathfrak{p} \nmid \infty$ for infinite, finite respectively).

2.3.1 Density theorems

We want now to prove 2.3.1 for cyclotomic extentions of $\mathbb{Q}$. Let $m \geqslant 2$ $(\in \mathbb{Z})$ and $(a, m) = 1$, consider now the sequence

$$..a - m, a, a + m, a + 2m, .., a + km.. \tag{2.11}$$

clearly there are $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$ distinct sequences. Dirichlet showed that the prime numbers are equidistributed among these sequences.
We want to interpret this in terms of Galois groups. Let L/K be a finite extention of number fields with Galois group G. For every prime ideal $\mathfrak{F}$ in O_L, there exists a unique $\sigma \in G$, called the **Frobenius element** sth

a) $\sigma \in G(\mathfrak{F})$ ie $\sigma(\mathfrak{F}) = \mathfrak{F}$

b) $\forall \alpha \in O_L$, $\sigma\alpha \equiv \alpha^q \, mod \, \mathfrak{F}$, where q=number of elements in the residue field $O_K/\mathfrak{p}$, $\mathfrak{p} = \mathfrak{F} \cap K$

it is denoted as $(\mathfrak{F}, L/K) \equiv \sigma$, when $\mathfrak{F}$ is unramified over $\mathfrak{p}$, because in this case σ is uniquely determined by these conditions.

Let now $\tau\mathfrak{F}$ a second prime dividing $\mathfrak{p}$, $\tau \in G$, then $G(\tau\mathfrak{F}) = \tau G(\mathfrak{F})\tau^{-1}$ and $(\tau\mathfrak{F}, L/K) = \tau(\mathfrak{F}, L/K)\tau^{-1}$, the proof is easy... Thus if $\mathrm{Gal}(L/K)$ is abelian we have $(\mathfrak{F}, L/K) = (\mathfrak{F}', L/K)$ $\forall \mathfrak{F}, \mathfrak{F}' \mid \mathfrak{p}$, we write thus $(\mathfrak{p}, L/K)$.

If $\mathrm{Gal}(L/K)$ is not abelian we denote by $(\mathfrak{p}, L/K)$, the conjugacy class in G $\{(\mathfrak{F}, L/K) \, : \, \mathfrak{F}|\mathfrak{p}\}$

Now consider $\mathbb{Q}[\zeta_m]/\mathbb{Q}$, m either odd integer > 1 or a positive integer divisible by 4. We have the result $Gal(\mathbb{Q}[\zeta_m]/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$
with [n] acting as $\zeta \mapsto \zeta^n$. A prime p not dividing m is unramified in $\mathbb{Q}[\zeta_m]$ and $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q}) = [p]$

Now let $\tau = [\alpha] \in Gal(\mathbb{Q}[\zeta_m]/\mathbb{Q})$,then $(p, \mathbb{Q}[\zeta_m]/\mathbb{Q}) = [\tau]$ has density $1/\varphi(m)$ in the set of prime numbers.

As we mentioned Frobenius conjectured that for every conjugacy class C in G, the density of $\{\mathfrak{p} \mid (\mathfrak{p}, L/K) = C\}$ is $|C|/|G|$.

2.3.2 Local class field theory and infinite extentions

By 1930 the abelian extentions of both number fields and local fields had been classified. However there were aspects of the theory that were considered un-

satisfactory, which Chevalley with his new notion of an idele was able to solve. Let K^{ab} denote the composite of all finite abelian extentions of K. The full statement of local class field theory is that for every p-adic field K, there exists a well defined homomorphism $\varphi : K^* \to Gal(K^{ab}/K)$ (now called the **local Artin map**) that induces the isomorphism

$$K^*/Nm(L^*) \xrightarrow{\sim} Gal(L/K)$$

for every finite abelian extention L/K; moreover all (open) subgroups of finite index are norm groups. This suggests that it might be possible to define a global Artin map whose components are the local Artin maps, in the sense that the following diagram commutes for all primes $\mathfrak{p}$ of K

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \xrightarrow{\phi_{\mathfrak{p}}} & Gal(K_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ \prod_{\mathfrak{p}} K_{\mathfrak{p}}^* & \xrightarrow{\phi \quad ??} & Gal(K^{ab}/K) \end{array}$$

One problem is that $\prod_{\mathfrak{p}} K_{\mathfrak{p}}^*$ is not locally compact, this would be true only for compact groups, and the groups $K_{\mathfrak{p}}^*$ are only locally compact. In fact $\prod_{\mathfrak{p}} K_{\mathfrak{p}}^*$ is too big for there exist a ϕ. Chevalley solved this by defining the group of ideles I_K to be the subgroup of $\prod_{\mathfrak{p}} K_{\mathfrak{p}}^*$ sth it consists of families $(a_{\mathfrak{p}})$, $a_{\mathfrak{p}} \in O_{\mathfrak{p}}^*$ for almost all nonarchimedean primes.

When endowed with the topology for which

$$\prod_{\mathfrak{p}|\infty} K_{\mathfrak{p}}^* \times \prod_{\mathfrak{p}\nmid\infty} O_{\mathfrak{p}}^*$$

is an open subgroup, I_K becomes a locally compact group. Embed K^* in I_K as the diagonal subgroup.

In the Chevalley[7] approach, one proves first local class field theory directly, then defines a global Artin map $\varphi_K : I_K \to Gal(K^{ab}/K)$ whose components are the local Artin maps and shows that K^* is contained in the kernel of φ_K and that the homomorphism

$$I_K/K^* \to Gal(K^{ab}/K)$$

induced by φ is surjective with kernel equal to the identity connected component of the group $I_K/i(K^*)$. In other words the homomorphism φ_K fits into a commutative diagram

$$\begin{array}{ccc} K_{\mathfrak{p}}^* & \xrightarrow{\phi_{\mathfrak{p}}} & Gal(K_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}}) \\ \downarrow & & \downarrow \\ I_K & \xrightarrow{\phi_K} & Gal(K^{ab}/K) \end{array}$$

[7] **CHEVALLEY** (1909–84). The main statements of class field theory are purely algebraic, but all the earlier proofs used analysis; Chevalley gave a purely algebraic proof. With his introduction of idèles he was able to give a natural formulation of class field theory for infinite abelian extensions

for all primes $\mathfrak{p}$ of K and φ_K induces an isomorphism

$$C_K/C_K^\circ \xrightarrow{\sim} Gal(K^{ab}/K) \qquad C_K \triangleq I_K/K^*$$

we can interpret this as follows:

there is a canonical isomorphism $C/C^\circ \simeq \varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$, and for every finite abelian extension L of K and sufficiently large modulus $\mathfrak{m}$ there is a commutative diagram

$$\begin{array}{ccc} C & \xrightarrow{\phi_K} & Gal(K^{ab}/K) \\ \downarrow & & \downarrow{\scriptstyle \tau \mapsto \tau|L} \\ C_{\mathfrak{m}} & \xrightarrow{\psi_{L/K}} & Gal(L/K) \end{array}$$

By 1950 the local Artin map could be characterized locally, or it could be described as the local component of the global Artin map, but it was not until 1965 that Lubin and Tate found an explicit local description of it.

Notation 2.3.2. *.. in the previous, we define*

$$i : K^* \to J$$

$$a \longmapsto (a)$$

sending $a \in K^*$ to the principal ideal (a).

Note: Mac Lane recalls that Artin (about 1948) pointed out in conversations that the cohomology of groups should have use in class field theory. Hochschild (1950) and Hochschild and Nakayama (1952) showed how the Brauer group arguments of class field theory could be replaced by cohomological arguments. In 1952, Tate proved that the homology and cohomology groups for a finite group G could be suitably combined in a single long exact sequence. He used this sequence, together with properties of transfer and restriction, to give an elegant reformulation of class field theory.

2.4 Non Abelian Class Field Theory

In the same talk at the ICM 1920 in which he announced his proof of the main theorems of abelian class field theory to the world, Takagi raised the question of a nonabelian class field theory.. Non abelian class field theory is part of Langland's program, which is a vast interlocking series of conjectures, and some progress has been made, especially in the local case and the function field case [4].
The norm limitation theorem shows that the subgroups of the (ray) class groups do not distinguish between an extension field and its largest abelian subextension.
For several decades it was unclear what form a nonabelian class field theory should take, or even whether it existed. In 1946, Artin speculated that finding

the correct statements was the *only* problem: once we knew what they were, it would be possible to deduce them from abelian class field theory. Weil[8] relates that, a year later, Artin said that he had lost faith in the existence of a non-abelian class field theory.

Instead of studying the set $Spl_S(L/K)$, we should study the Artin L-series $L(s,\rho)$ of a representation ρ of $Gal(L/K)$. The problem of describing the sets $Spl_S(L/\mathbb{Q})$ then becomes that of describing the set of analytic functions that arise in this fashion. Langlands[9] has constructed a class of L-series, called **automorphic L-series**, and conjectures that each $L_S(s,\rho)$ is automorphic, and specifies which automorphic L-series arise in this fashion. Thus, the conjecture answers the original question for all finite Galois extensions of $\mathbb{Q}$. For $n=1$ (so G is abelian) and all K, Artin proved all Artin L-series are automorphic. For $n=2$, Langlands (and Tunnell) have proved the conjecture in some cases.
In 1967 Langlands stated his conjectural functoriality principle, which includes a nonabelian class field theory as a special case. For a local field K this can be stated as follows..
The Weil group W_K of K is defined to be the subgroup of $Gal(K^{ab}/K)$ consisting of the elements that act on the residue field as an integer power of the Frobenius element. The local Artin map in abelian local class field theory can be regarded as an isomorphism ϕ_K from K^* onto the largest abelian quotient W_K^{ab} of W_K. Langlands conjectures that the homomorphisms from W_K into $GL_n(\mathbb{C})$ correspond to certain representations of $GL_n(K)$. For $n=1$, the representations of $GL_1(K)=K^*$ are just characters, and the correspondence is given by composition with ϕ_K. For $n>1$ the representations of $GL_n(K)$ are typically infinite dimensional.

On the automorphic side, let $\mathbb{A}_n(K)$ be the set of equivalence classes of irreducible representations of $GL_n(K)$ on complex vector spaces for which the stabilizer of each vector is open. On the Galois side, let $\mathbb{G}_n(K)$ be the set of equivalence classes of pairs (r,N) where r is a semisimple representation of W_K on an n-dimensional complex vector space V, trivial on an open subgroup, and N is a nilpotent endomorphism of V such that conjugating N by $r(\sigma)$ ($\sigma \in W_K$) multiplies it by the absolute value of $\phi_K^{-1}(\sigma)$. The local Langlands conjecture for K asserts that there is a family of bijections $(\sigma_n)_{n\geq 1}$.

$$\pi \mapsto \sigma_n(\pi) : \mathbb{A}_n(K) \to \mathbb{G}_n(K)$$

such that

- (a) the determinant of $\sigma_n(\pi)$, viewed as a character of W_K, corresponds under ϕ_K to the central character of π.

- (b) the map σ_n preserves L-factors and ε-factors of pairs of π's (as defined by Jacquet, Piatetskii-Shapiro, and Shalika on the automorphic side, and by Langlands and Deligne on the Galois side)

[8] **WEIL** (1906–1998). Defined the Weil group, which enabled him to give a common generalization of Artin L-series and Hecke L-series

[9] **LANGLANDS** (1936–). The Langlands program is a vast series of conjectures that, among other things, contains a nonabelian class field theory

- (c) for $\chi \in \mathbb{A}_1(K)$, $\sigma_n(\pi \otimes (\chi \circ det)) = \sigma_n(\pi) \otimes \sigma_1(\chi)$
- (d) σ_n commutes with passage to the contragredient, $\pi \mapsto \pi^\vee$

For each K, Henniart showed there exists at most one such family. The conjecture itself was proved by Harris and Taylor (2001). Several months later, Henniart(2000) found a simpler proof.

Chapter 3

The theory of valuations

3.1 Definition of p-adic numbers

We would like to introduce the p-adic numbers following the ideas of Neukirch [3], Milne [4] and Lang [6]. The valuation theory is our starting point to the development of our theory which started with the invention of the p-adic numbers at the beginning of the 20th century by the mathematician Kurt Hensel(1861-1941) with a view to introduce into number theory the powerful method of power series expansion, which plays in function theory a predominant role. We associate to the integer $f \in \mathbb{Z}$ its "value" at prime $p \in \mathbb{Z}$, ie

$$f(p) := f \, mod \, p \in \kappa(p), \quad \kappa(p) = \mathbb{Z}/p\mathbb{Z}$$

This suggests the further question, whether not only the value of $f \in \mathbb{Z}$ at p, but also the higher derivatives of f can be reasonably defined. This leads us to the definition of a p-adic integer.

Definition 3.1.1. *For a fixed prime p, a p-adic integer is a formal infinite series*

$$a_0 + a_1 \, p + a_2 \, p^2 + ... \qquad 0 \leq a_i < p, \quad \imath = 0, 1, 2...$$

The set of p-adic integers is denoted by $\mathbb{Z}_p$.

In the specific case of a positive integer $n \in \mathbb{N}$, we have

$$n = a_0 + a_1 \, p + ... + a_k \, p^k$$

Proposition 3.1.2. *The residue classes $a \, mod \, p^n \in \mathbb{Z}/p^n\mathbb{Z}$ can be uniquely represented in the form*

$$a \equiv a_0 + a_1 \, p + ... + a_{n-1} \, p^{n-1} \, mod \; p^n$$

where $0 \leq a_i < p$

Proof. we use induction on n... □

Every integer f and more generally every rational number

$$f \in \mathbb{Z}_{(p)} = \{g/h, \quad g,h \in \mathbb{Z}, \quad p \nmid h\}$$

defines a sequence of residue classes

$$\overline{s}_n = f mod\, p^n \in \mathbb{Z}/p^n\mathbb{Z}, \quad n = 1,2,...$$

and by the preceding proposition

$$\overline{s}_1 = a_0 \mod p$$

$$\overline{s}_2 = a_0 + a_1 p \mod p^2 \quad etc$$

where

$$a_0, a_1, ... \in \{0,1,...,p-1\}$$

are unique.

The sequence

$$s_n = a_0 + a_1 p + .. + a_{n-1}\, p^{n-1} \qquad n = 1,2...$$

defines a p-adic integer

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu \in \mathbb{Z}_p$$

we call it the p-adic expansion of f

Now if $f \in \mathbb{Q}$ we write $f = g/h\ p^{-m}$ sth $(gh,p) = 1$ and we have the analogy with the Laurent series ie we attach to f the p-adic number

$$a_0 p^{-m} + a_1 p^{-m+1} + .. + a_m + a_{m+1} p + .. \in \mathbb{Q}_p$$

so that we can define addition and multiplication of p-adic numbers, which turn $\mathbb{Z}_p$ into a ring and $\mathbb{Q}_p$ into its field of fractions, we have to view $f \in \mathbb{Z}_p$ not as sequences of s_n $n = 1,2,..$ as has been defined, but rather as sequences of residue classes:

$$\overline{s}_n = s_n\ mod\, p^n \in \mathbb{Z}/p^n\mathbb{Z}$$

we have the canonical projections between different rings $\mathbb{Z}/p^n\mathbb{Z}$

$$\mathbb{Z}/p\mathbb{Z} \xleftarrow{\lambda_1} \mathbb{Z}/p^2\mathbb{Z} \xleftarrow{\lambda_2} \mathbb{Z}/p^3\mathbb{Z} \xleftarrow{\lambda_3} ...$$

and

$$\lambda_n(\overline{s}_{n+1}) = \overline{s}_n$$

In the direct product

$$\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n\in N},\ x_n \in \mathbb{Z}/p^n\mathbb{Z}\}$$

we consider $(x_n)_{n\in N}$ sth $\lambda_n(x_{n+1}) = x_n \quad n = 1, 2, ..$ this set is called the **projective limit** of the rings $\mathbb{Z}/p^n\mathbb{Z}$ ie

$$\varprojlim_n \mathbb{Z}/p^n\mathbb{Z} = \{(x_n)_{n\in N} \in \prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \quad \lambda_n(x_{n+1}) = x_n\}$$

and we have our result:

Proposition 3.1.3. *There is a bijection*

$$\mathbb{Z}_p \xrightarrow{\sim} \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$$

The projective limit is a subring of the direct product $\prod_{n=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z}$ where we can add and multiply componentwise. We thus have the **ring of p-adic integers** $\mathbb{Z}_p$.

3.2 The p-adic absolute value

The representation of a p-adic integer

$$a_0 + a_1\, p + a_2\, p^2 + ... \qquad 0 \le a_i < p$$

resembles very much the decimal fraction representation

$$a_0 + a_1\,(\frac{1}{10}) + a_2\,(\frac{1}{10})^2 + ... \qquad 0 \le a_i < 10$$

of a real number. But it does not converge as the decimal fraction does. Nonetheless the field $\mathbb{Q}_p$ of p-adic numbers can be constructed from the field $\mathbb{Q}$ in the same fashion as the field of the real numbers $\mathbb{R}$. In that sense we have to replace the ordinary absolute value by a new p-adic absolute value $|\ |_p$ with respect to which the above series converge so that the p-adic numbers appear in the usual manner as limits of Cauchy sequences of rational numbers. This approach was proposed by *J Kurschak*. It is defined as follows

Let $a = \dfrac{b}{c} \quad b, c \in Z$ be a nonzero rational number, we extract from b, c as high a power of the prime number p as possible, ie $a = p^m \dfrac{b'}{c'} \quad (b'c', p) = 1$ and we set

$$|a|_p = \frac{1}{p^m}$$

we can see now that the summands of a p-adic series $a_0 + a_1\, p + a_2\, p^2 + ...$ form a sequence converging to 0 with respect to $|\ |_p$.

The exponent m in this representation is denoted by $\mathfrak{v}_p(a)$ and we put formally $\mathfrak{v}_p(0) = \infty$. This gives the function

$$\mathfrak{v}_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$$

which can be checked to satisfy the properties

- $\mathfrak{v}_p(a) = \infty \Leftrightarrow a = 0$
- $\mathfrak{v}_p(ab) = \mathfrak{v}_p(a) + \mathfrak{v}_p(b)$
- $\mathfrak{v}_p(a+b) \geq min\{\mathfrak{v}_p(a), \mathfrak{v}_p(b)\}$

where $x + \infty = \infty \quad , \quad \infty + \infty = \infty$ and $\infty > x, \forall x \in Z$

The function $\mathfrak{v}_p$ is called the **p-adic exponential valuation of** $\mathbb{Q}$. The **p-adic absolute value** is given by

$$|\ |_p : \mathbb{Q} \to \mathbb{R} \quad , \qquad a \mapsto |a|_p = p^{-\mathfrak{v}_p(a)}$$

In view of the 3 properties above it satisfies the conditions of a *norm* on $\mathbb{Q}$. One can show that the absolute values $|\ |_p$ and $|\ |$ essentially exhaust all norms on $\mathbb{Q}$, any further norm is a power $|\ |_p^s$ or $|\ |^s$ for some real $s > 0$. The usual absolute value $|\ |$ is denoted by $|\ |_\infty$, this gives the following **product formula**

Proposition 3.2.1. *For every rational number $a \neq 0$ we have*

$$\prod_p |a|_p = 1$$

where p varies over all prime numbers as well as the symbol ∞.

We want now to give an alternative definition for the field of p-adic numbers. For this we define:

A **Cauchy sequence** with respect to $|\ |_p$ is by definition a sequence $\{x_n\}$ of rational numbers such that for every $\varepsilon > 0$, there exists a positive integer n_0 satisfying

$$|x_n - x_m|_p < \varepsilon \quad for\ all \quad n, m \geq n_0$$

example: Every formal series

$$\sum_{\nu=0}^{\infty} a_\nu p^\nu \qquad 0 \leq a_\nu < p$$

provides a Cauchy sequence via its partial sums

$$x_n = \sum_{\nu=0}^{n-1} a_\nu p^\nu$$

because for $n > m$ one has

$$|x_n - x_m|_p = |\sum_{\nu=m}^{n-1} a_\nu p^\nu|_p \leq max_{m \leq \nu < n}\{|a_\nu p^\nu|_p\} \leq \frac{1}{p^m}$$

A sequence $\{x_n\}$ in $\mathbb{Q}$ is called a **nullsequence** with respect to $|\ \ |_p$ if $|x_n|_p$ is a sequence converging to 0 in the usual sense.

The Cauchy sequences form a ring $\mathbb{R}$, the nullsequences form a maximal ideal $\mathfrak{m}$, and we define the field of p-adic numbers to be the residue class field

$$\mathbb{Q}_p := \mathbb{R}/\mathfrak{m}$$

we embed $\mathbb{Q}$ in $\mathbb{Q}_p$ by associating to every element $a \in \mathbb{Q}$ the residue class of the constant sequence $(a, a, ...)$. The p-adic absolute value $|\ \ |_p$ on $\mathbb{Q}$ is extended to $\mathbb{Q}_p$ by giving the element $x = \{x_n\}\ mod\ \mathfrak{m} \in \mathbb{R}/\mathfrak{m}$ the absolute value

$$|x|_p := lim_{n\to\infty}|x_n|_p \in \mathbb{R}$$

This limit exists because $\{|x_n|_p\}$ is a Cauchy sequence in $\mathbb{R}$ and it is independent of the choice of the sequence $\{x_n\}$ within its class mod $\mathfrak{m}$ because any p-adic nullsequence $\{y_n\} \in \mathfrak{m}$ satisfies $lim_{n\to\infty}|y_n|_p = 0$.

3.3 Extensions of valuations

For every valuation v of K we consider the completion K_v and an algebraic closure $\overline{K}_v$ of K_v. The canonical extension of v to K_v is again denoted by v and the unique extension of this latter valuation to $\overline{K}_v$ by $\overline{v}$.

Let L/K be an algebraic extension. Choosing a K-embedding

$$\tau : L \to \overline{K}_v$$

we obtain by restriction of $\overline{v}$ to τL an extension

$$w = \overline{v} \circ \tau$$

of the valuation v to L. In other words, if v resp $\overline{v}$ are given by the absolute values $|\ \ |_v$ resp $|\ \ |_{\overline{v}}$ on K, K_v resp $\overline{K}_v$, where $|\ \ |_{\overline{v}}$ extends precisely the absolute value $|\ \ |_v$ of K_v, then we obtain on L the multiplication valuation

$$|x|_w = |\tau x|_{\overline{v}}$$

The mapping $\tau : L \to \overline{K}_v$ is obviously continuous with respect to this valuation. It extends in a unique way to a continuous K-embedding

$$\tau : L_w \to \overline{K}_v$$

where in the case of an infinite extension L/K, L_w does not mean the completion of L with respect to w, but the union $L_w = \bigcup_i L_{iw}$ of the completions L_{iw} of all finite subextensions L_i/K of L/K. This union will be henceforth called the **localization** of L with respect to w. When $[L : K] < \infty$, τ is given by the rule

$$x = w - lim_{n\to\infty}x_n \mapsto \tau\ x := \overline{v} - lim_{n\to\infty}\tau\ x_n$$

where $\{x_n\}_{n\in N}$ is a w-Cauchy sequence in L and hence $\{\tau\ x_n\}_{n\in N}$ a $\overline{v}$-Cauchy sequence in $\overline{K}_v$. We note here that the sequence $\tau\ x_n$ converges in the finite complete extension $\tau\ L \cdot K_v$ of K_v. We consider the diagram of fields

$$\begin{array}{ccc} L & \text{——} & L_w \\ | & & | \\ K & \text{——} & K_v \end{array}$$

The canonical extension of the valuation w from L to L_w is precisely the unique extension of the valuation v from K_v to the extension L_w/K_v, We have

$$L_w = L\ K_v$$

because if L/K is finite then the field $L\ K_v \subseteq L_w$ (is complete) contains the field L and therefore has to be its completion. If L_w/K_v has degree $n < \infty$, then the absolute values corresponding to v and w satisfy the relation

$$|x|_w = \sqrt[n]{|N_{L_w/K_v}(x)|_v}$$

The above field diagram is of central importance in algebraic number theory. It shows the passage from the global extension L/K to the local extension L_w/K_v and thus represents one of the most important methods of algebraic number theory, the **local-to-global principle**.

We saw that every K-embedding $\tau : L \to \overline{K}_v$ gave us an extension $w = \overline{v} \circ \tau$ of v. For every automorphism $\sigma \in Gal(\overline{K}_v/K_v)$ of $\overline{K}_v$ over K_v we obtain with the composite

$$L \xrightarrow{\tau} \overline{K}_v \xrightarrow{\sigma} \overline{K}_v$$

a new K-embedding $\tau' = \sigma \circ \tau$ of L. It will be said to be conjugate to τ over K_v. The following result gives us a complete description of the possibe extensions of v to L.

Theorem 3.3.1 (**Extension Theorem**). *Let L/K be an algebraic field extension and v a valuation of K. Then:*

(i) Every extension w of the valuation v arises as the composite $w = \overline{v} \circ \tau$ for some K-embedding $\tau : L \to \overline{K}_v$

(ii) Two extensions $\overline{v} \circ \tau$ and $\overline{v} \circ \tau'$ are equal if and only if τ and τ' are conjugate over K_v

Proof. we shall prove the second statement..

(ii) Let τ and $\sigma \circ \tau$ with $\sigma \in Gal(\overline{K}_v/K_v)$ be two embeddings of L conjugate over K_v. Since $\overline{v}$ is the only extension of the valuation v from K_v to $\overline{K}_v$, one has $\overline{v} = \overline{v} \circ \sigma$ and thus $\overline{v} \circ \tau = \overline{v} \circ (\sigma \circ \tau)$. The extensions induced to L by τ and by $\sigma \circ \tau$ are therefore the same.

Conversely: Let $\tau,\ \tau' : L \to \overline{K}_v$ be two embeddings such that $\overline{v} \circ \tau = \overline{v} \circ \tau'$ and let $\sigma : \tau L \to \tau' L$ be the K-isomorphism $\sigma = \tau' \circ \tau^{-1}$. We can extend σ to a K_v-isomorphism

$$\sigma : \tau L \cdot K_v \to \tau' L \cdot K_v$$

Indeed, τL is dense in $\tau L \cdot K_v$, so every element $x \in \tau L \cdot K_v$ can be written as a limit

$$x = lim_{n\to\infty} \tau x_n$$

for some sequence x_n which belongs to a finite subextension of L. As $\overline{v} \circ \tau = \overline{v} \circ \tau'$, the sequence $\tau' x_n = \sigma \tau x_n$ converges to an element

$$\sigma x = lim_{n\to\infty} \sigma \tau x_n$$

in $\tau' L \cdot K_v$. Clearly the correspondence $x \mapsto \sigma x$ does not depend on the choice of a sequence $\{x_n\}$ and yields an isomorphism $\tau L \cdot K_v \xrightarrow{\sigma} \tau' L \cdot K_v$ which leaves K_v fixed. Extending σ to a K_v-automorphism $\overline{\sigma} \in Gal(\overline{K}_v / K_v)$ gives $\tau' = \overline{\sigma} \circ \tau$ so that τ and τ' are indeed conjugate over K_v. □

Chapter 4

Abstract class field theory

4.1 Definition of class formation

The cohomological algebra behind the reciprocity law is common to both the local and global class field theory of number fields and function fields. Abstracting it led to the definition of a new algebraic structure, "**class formation**", which embodies the common features of our theories. The difference is in the proofs that the idele classes globally and the multiplicative groups locally, satisfy the axioms of a class formation. The relevant information can be found among others in Neukirch [1] and [2] (for a rigorous definition of profinite groups) and in Artin and Tate [5].
The mathematics we cover is the result of roughly a century of development, 1850-1950. The high point came in 1920's with Takagi's proof that the finite abelian extensions of a number field are in natural one to one correspondence with the quotients of the generalized ideal class groups of that field, and Artin's proof several years later that an abelian Galois group and the corresponding ideal class group are canonically isomorphic, by an isomorphism which implied all known reciprocity laws. Around 1950 the systematic use of the cohomology of groups by Hochschild, Nakayama, Artin and Tate shed new light. It enabled many theorems of the local class field theory of the 1930's to be transferred to the global theory, and led to the notion of class formation embodying the common features of both theories. At about the same time, Weil conceived the idea of Weil groups and proved their existence. With those two developments it is fair to say that the classical one-dimensional abelian class field theory had reached full maturity. There were still a few things to be worked out, such as the local and global duality theories, and the cohomology of algebraic tori, but it was time for new directions.
They soon came. For example:

Higher dimensional class field theory
Non-abelian reciprocity laws and the Langlands program
Iwasawa theory[1]
Leopold's conjecture

[1] **IWASAWA** (1917–1998). He introduced an important new approach into algebraic number theory which was suggested by the theory of curves over finite fields

Abelian (and non-abelian) l-adic representations

Lubin-Tate[2] local theory, Hayes explicit theory for function fields, Drinfeld modules

Stark conjectures

Serre conjectures (now theorems).

Local and global class field theory, as well as a series of further theories for which the name class field theory is similarly justified, have the following principle in common. All of these theories invole a canonical bijective correspondence between the abelian extensions of a field K and certain subgroups of a corresponding module A_K associated with the field K. This correspondence has the property that if the subgroup $I \subseteq A_K$ corresponds to an abelian field extension L/K (the "class field associated with I"), then there exists a canonical isomorphism between the Galois group $G_{L/K}$ and the factor group A_K/I. This so called reciprocity law is the main theorem of class field theory.

This main theorem can be tracked back to a common system of axioms for the concrete theories mentioned above which essentially consists of the assumptions in Tate's Theorem; in fact one can view Tate's Theorem itself as the abstract version of the main theorem of class field theory. The notion of a **class formation** is based on this idea. It separates the purely group theoretic machinery, which is characteristic of class field theory, from the specific considerations of field theory, and gives in an easily comprehensible and elegant way information about the goal and function of the theory.

First we will make a small parenthesis to introduce the decomposition group that we shall use later on, based on our theory of valuations.

If L/K is a finite extension of a number field K and $\mathfrak{F}$ a prime of L lying above the prime $\mathfrak{p}$ of K, then we write $\mathfrak{F}|\mathfrak{p}$. In this case the completion $L_{\mathfrak{F}}$ of L by $\mathfrak{F}$ contains $K_{\mathfrak{p}}$, since the restriction of the valuation associated with $\mathfrak{F}$ from L to K yields the valuation of the field K associated with $\mathfrak{p}$.

We illustrate this diagrammatically as follows..
the transition from the global extension L/K to the local extensions $L_{\mathfrak{F}}|K_{\mathfrak{p}}$ at the individual primes is the fundamental principle behind class field theory.

$$\begin{array}{ccc} L & \text{——} & L_{\mathfrak{F}} \\ | & & | \\ K & \text{——} & K_{\mathfrak{p}} \end{array}$$

Let's consider the prime decomposition

$$\mathfrak{p} = \mathfrak{F}^{e}..\mathfrak{F}'^{e'}$$

[2]**TATE** (1925–). He proved new results in group cohomology, which allowed him to give an elegant reformulation of class field theory. With Lubin he found an explicit way of generating abelian extensions of local fields

of $\mathfrak{p}$ in L, then $\hat{\mathfrak{p}} = \hat{\mathfrak{F}}^e$, where $\hat{\mathfrak{p}}$ (or $\hat{\mathfrak{F}}$) denotes the prime ideal of the field $K_{\mathfrak{p}}$ (resp $L_{\mathfrak{F}}$). If $\mathfrak{F}$ runs through all the primes of L over $\mathfrak{p}$, then we have

$$\sum_{\mathfrak{F}|\mathfrak{p}} [L_{\mathfrak{F}} : K_{\mathfrak{p}}] = [L : K]$$

Let L/K be finite normal field extension with $G = Gal(L/K)$ $(= G_{L/K})$, if $\sigma \in G$, then if $\mathfrak{F}|\mathfrak{p} \Rightarrow \sigma\mathfrak{F}|\mathfrak{p}$ and we say $\sigma\mathfrak{F}$ is conjugate to $\mathfrak{F}$ wrt σ.
We have that $K_{\mathfrak{p}}$ is contained in $L_{\mathfrak{F}}$ as well as $L_{\sigma\mathfrak{F}}$ since $\mathfrak{p}$ lies under $\mathfrak{F}$ and $\sigma\mathfrak{F}$.

There is a canonical $K_{\mathfrak{p}}$-isomorphism

$$L_{\mathfrak{F}} \xrightarrow{\sigma} L_{\sigma\mathfrak{F}}$$

In fact if $a \in L_{\mathfrak{F}}$, ie $a = \mathfrak{F} - lim a_i$ for some sequence $a_i \in L$, then the sequence $\sigma a_i \in L$ converges in $L_{\sigma\mathfrak{F}}$ wrt $\sigma\mathfrak{F}$, and the canonical isomorphism is obtained from

$$a = \mathfrak{F} - lim\ a_i \in L_{\mathfrak{F}} \mapsto \sigma a = \sigma\mathfrak{F} - lim\ \sigma a_i \in L_{\sigma\mathfrak{F}}$$

Under this isomorphism, $K_{\mathfrak{p}}$ is fixed elementwise.
In particular if $\sigma\mathfrak{F} = \mathfrak{F}$, then we have the $K_{\mathfrak{p}}$-automorphism

$$L_{\mathfrak{F}} \xrightarrow{\sigma} L_{\mathfrak{F}}$$

and therefore an element of the Galois group $G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}$, ie $G_{\mathfrak{F}} \subseteq G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}$. The above automorphism is the continuous extension of the automorphism σ of L to the completion $L_{\mathfrak{F}}$, $G_{\mathfrak{F}}$ is the decomposition group of $\mathfrak{F}$ over K.
Conversely every automorphism of $G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}$ yields an automorphism in $G_{\mathfrak{F}}$ by restriction to L, so we have a canonical isomorphism

$$G_{\mathfrak{F}} \cong G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}$$

and we can identify these two groups in the following text.

Our main reference towards the proof of reciprocity law is Tate's theorem [1], which is stated as:

Theorem 4.1.1 (Tate's Theorem). *Assume that A is G-module with the properties: For each subgroup $g \subseteq G$*

- $H^1(g, A) = 0$
- $H^2(g, A)$ *is cyclic of order* $|g|$

If a generates the group $H^2(G, A)$, then the map

$$a \cup : H^q(G, \mathbb{Z}) \to H^{q+2}(G, A)$$

is an isomorphism.

We shall make use of this theorem later on..

We shall now introduce a structure, ie the **profinite group**. In the course of the years since the 1950s, the point of view of class field theory has slightly changed. The classical approach describes the Galois groups of *finite* extensions using arithmetic invariants of the local or global ground field. An essential feature of the modern point of view is to consider infinite Galois groups instead, ie one investigates the set of all finite extensions of the field k at once, via the *absolute* Galois group G_K. These groups intrinsically come equipped with a topology, the Krull topology, under which they are Hausdorff, compact and locally disconnected topological groups. It proves to be useful to ignore, for the moment, their number theoretical motivation and to investigate topological groups of this type, the profinite groups, as objects of interest in their own right. For this reason an extensive "algebra of profinite groups" has been developed by number theorists, not as an end in itself but always with concrete number theoretical applications in mind. Nevertheless, many results can be formulated solely in terms of profinite groups and their modules, without reference to the number theoretical background.

Let G be a profinite group, ie a compact group with the normal-subgroup topology. We may think of G as the Galois group (endowed with the Krull topology) of an infinite Galois field extension, although the abstract notions in this section do not use this interpretation. The open subgroups of G are precisely the closed subgroups of finite index. In fact, the complement of an open subgroup is the union of (open) cosets, thus open, and since G is compact, finitely many of these cosets cover the group G, hence the index is finite. Conversely, a closed subgroup of finite index is open, because it is the union of finitely many cosets, hence its complement is closed.

Given a profinite group G, we consider the family $\{G_K : K \in X\}$ of all open subgroups of G ie the closed subgroups of finite index. We label each such subgroup with the index K, and call these indices "fields".

The "field" K_0 with $G_{K_0} = G$ is called the base field. If $G_L \subseteq G_K$, we write formally $K \subseteq L$ and define the degree of such an extension L/K as

$$[L : K] = (G_K : G_L)$$

The extension L/K is called normal if $G_L \subseteq G_K$ is a normal subgroup of G_K. If L/K is normal, then the Galois group of L/K is defined as the quotient group

$$G_{L/K} = G_K/G_L$$

An extension L/K is called cyclic, abelian, solvable etc, if its Galois group $G_{L/K} = G_K/G_L$ is cyclic, abelian, solvable etc. We define the intersection and the compositum of such fields K_i by setting

$$K = \bigcap_{i=1}^{n} K_i$$

if G_K is (topologically) generated by the G_{K_i} in G, and

$$K = \prod_{i=1}^{n} K_i$$

if $\quad G_K = \bigcap_{i=1}^{n} G_{K_i}$

If $G_{L'} = \sigma G_L \sigma^{-1}$ for $\sigma \in G$, then we write $L' = \sigma L$ and we call two extensions L/K and L'/K conjugate in case $L' = \sigma L$ for some $\sigma \in G_K$. With these notions, we obtain for each profinite group G a formal Galois theory.

In the following we consider modules A on which a profinite group G acts. In this context it is important to keep the topological structure on G in mind. The action of G on A should be in a certain sense continuous. More precisely, it should satisfy one of the following equivalent conditions:

- (i) The map $G \times A \to A$ with $(\sigma, a) \mapsto \sigma a$ is continuous (here A is interpreted as a discrete module)
- (ii) For each $a \in A$ the stabilizer $\{\sigma \in G : \sigma a = a\}$ is open in G
- (iii) $A = \bigcup_U A^U$ where U runs through all the open subgroups of G

Definition 4.1.2. *If G is a profinite group and A is a G-module satisfying the previous equivalent conditions, the pair (G, A) is called a* ***formation****.*

If G is the Galois group of a (infinite) Galois extension N/K then G acts on the multiplicative group N^* of the field N, and the pair (G, N^*) is a formation. It is precisely this example that comes into play in local class field theory, and one may use it as an orientation for what follows.

Let (G, A) be a formation. In the following we think of the module A as multiplicatively written. Let $\{G_K : K \in X\}$ be the family of open subgroups of G, indexed by the set of fields X. For each field $K \in X$ we consider the fixed module associated with K ie

$$A_K = A^{G_K} = \{a \in A : \sigma a = a \quad for\ all \quad \sigma \in G_K\}$$

In the class field theory example mentioned above, we obviously have $A_K = K^*$. If $K \subseteq L$, then $A_K \subseteq A_L$.

If L/K is a normal extension, then A_L is a $G_{L/K}$-module. When we call the pair (G, A) a formation, we basically mean by this the formation of these normal extensions L/K together with the $G_{L/K}$-modules A_L.

We consider now for each normal extension L/K the cohomology groups of the $G_{L/K}$-module A_L. For simplicity of notation, we set

$$H^q(L/K) = H^q(G_{L/K}, A_L)$$

If $K \subseteq L \subseteq N$ is a tower of normal extensions of K we have inclusions $G_N \subseteq G_L \subseteq G_K$ with G_N and G_L normal in G_K and the cohomology theory yields the homomorphism

$$H^q(G_{L/K}, A_L) = H^q(G_{L/K}, A_N^{G_{N/L}}) \xrightarrow{\inf} H^q(G_{N/K}, A_N)$$

in other words

$$H^q(L/K) \xrightarrow{\inf_N} H^q(N/K) \quad for \;\; q \geq 1$$

In addition we also have the restriction and corestriction maps

$$H^q(G_{N/K}, A_N) \xrightarrow{\text{res}} H^q(G_{N/L}, A_N) \quad and$$

$$H^q(G_{N/L}, A_N) \xrightarrow{\text{cor}} H^q(G_{N/K}, A_N)$$

that is, for every integer q homomorphisms

$$H^q(N/K) \xrightarrow{\text{res}_L} H^q(N/L) \;\; and \;\; H^q(N/L) \xrightarrow{\text{cor}_K} H^q(N/K)$$

here we only need to assume that N/K is normal. If both N and L are normal, then the sequence

$$1 \to H^q(L/K) \xrightarrow{\inf_N} H^q(N/K) \xrightarrow{\text{res}_L} H^q(N/L)$$

is exact for $q = 1$ and exact for $q > 1$ if $H^i(N/L) = 1$ for $i = 1, .., q-1$.

If L/K is normal and $\sigma \in G$ then

$$\tau G_L \mapsto \sigma\tau\sigma^{-1} G_{\sigma L}$$

defines an isomorphism between $G_{L/K}$ and $G_{\sigma L/\sigma K}$ and

$$a \mapsto \sigma a$$

an isomorphism between A_L and $A_{\sigma L}$. Since $(\sigma\tau\sigma^{-1}G_{\sigma L})\sigma a = \sigma(\tau G_L)a$, these isomorphisms are compatible and we obtain an equivalence between the $G_{L/K}$-module A_L and the $G_{\sigma L/\sigma K}$-module $A_{\sigma L}$. Thus every $\sigma \in G$ yields an isomorphism

$$H^q(L/K) \xrightarrow{\sigma^*} H^q(\sigma L/\sigma K)$$

using the equivalence of the modules A_L and $A_{\sigma L}$ it is easy to see that the isomorphism σ^* commutes with inflation, restriction and corestriction.

We call a formation (G, A) a **field formation** when for each normal extension the first cohomology group vanishes:

$$H^1(L/K) = 1$$

In a field formation we have that

$$1 \to H^2(L/K) \xrightarrow{\inf_N} H^2(N/K) \xrightarrow{\text{res}_L} H^2(N/L)$$

is always exact.

We shall see soon that when G is the Galois group of a Galois field extension and A the multiplicative group of the extension field, then we have a field formation.

If $K \subseteq L \subseteq N$ are normal extensions, then we can always think of the group $H^2(L/K)$ as embedded in the group $H^2(N/K)$, since the inflation map

$$H^2(L/K) \xrightarrow{\inf_N} H^2(N/K)$$

is injective. The presentation of our ideas will become formally especially simple if we take this identification one step further. If L ranges over the normal extensions of K, then the groups $H^2(L/K)$ form a direct system of groups with respect to the inflation maps. We thus take the direct limit

$$H^2(\ \ /K) = \varinjlim_L H^2(L/K)$$

and we obtain a group $H^2(\ \ /K)$ in which all the groups $H^2(L/K)$ are embedded via the injective inflation maps. If we identify these groups with their images under this embedding, then $H^2(L/K)$ become subgroups of $H^2(\ \ /K)$, and

$$H^2(\ \ /K) = \bigcup_L H^2(L/K)$$

In particular, if $K \subseteq L \subseteq N$ is a tower of normal extensions of K, we have

$$H^2(L/K) \subseteq H^2(N/K) \subseteq H^2(\ \ /K)$$

we emphasize that the inflation maps are to be interpreted as inclusions here.

Remark 4.1.3. *Let G_K be a profinite group and let A be a G_K-module. Exactly as for finite groups, we can define cohomology groups $H^q(G_K, A)$ for $q \geq 0$ by taking as cochains the* ***continuous*** *maps $G_K \times ... \times G_K \to A$. Then*

$$H^q(G_K, A) \cong H^q(\ \ /K) = \varinjlim_L H^q(L/K)$$

Given any extension K'/K of K, we obtain a canonical homomorphism

$$H^2(\ \ /K) \xrightarrow{res_{K'}} H^2(\ \ /K')$$

In fact if $c \in H^2(\ \ /K)$, then there is an extension $K \subseteq K' \subseteq L$, so that c is contained in the group $H^2(L/K)$, hence the restriction map

$$H^2(L/K) \xrightarrow{res_{K'}} H^2(L/K')$$

defines an element

$$res_{K'} c \in H^2(L/K') \subseteq H^2(\ \ /K')$$

The fundamental assertion in both local and global class field theory is the existence of a canonical isomorphism, the so called "reciprocity map"

$$G_{L/K}^{ab} \cong A_K/N_{L/K}A_L$$

for every normal extension L/K where $G_{L/K}^{ab}$ is the abelianization of $G_{L/K}$ and $N_{L/K}A_L = N_{G_{L/K}}A_L$ is the norm group of A_L. Because of Tate's Theorem, we can force the existence of such an isomorphism *in abstracto* , by imposing the following conditions on our formation (G, A): If L/K is any extension, then

$$I.\ \ H^1(L/K) = 1$$
$$II.\ \ H^2(L/K) \textit{ is cyclic of order } [L:K]$$

If this holds, then the cup product with a generator of $H^2(L/K)$ gives an isomorphism

$$G_{L/K}^{ab} \cong A_K/N_{L/K}A_L$$

However there is a certain arbitrariness to this isomorphism, since it depends on the choice of the generator of $H^2(L/K)$. Therefore and in order to get a "canonical" reciprocity law, we replace $II.$ by the condition that there is an isomorphism between $H^2(L/K)$ and the cyclic group $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, the so-called **invariant map**, which uniquely determines the element $u_{L/K} \in H^2(L/K)$ with image $\frac{1}{[L:K]} + \mathbb{Z}$. The crucial point here is that this element $u_{L/K}$ remains "correct" when passing to extension fields and subfields, which we ensure by imposing certain compatibility conditions on the invariant map.

These considerations lead us to the:

Definition 4.1.4. *A formation (G, A) is be called a **class formation** if it satisfies the following axioms:*

- ***Axiom I*** $H^1(L/K) = 1$ *for every normal extension L/K (field formation)*
- ***Axiom II*** *For every normal extension L/K there exists an isomorphism:*

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

*the **invariant map** with the following properties:*

- *(a) If $K \subseteq L \subseteq N$ is a tower of normal extensions, then*

$$inv_{L/K} = inv_{N/K}|_{H^2(L/K)}$$

- *(b) If $K \subseteq L \subseteq N$ is a tower of extensions with N/K normal, then*

$$inv_{N/L} \circ res_L = [L:K] \cdot inv_{N/K}$$

In order to make the property (b) obvious, we visualize with the commutative diagram

$$\begin{array}{ccc} H^2(N/K) & \xrightarrow{inv_{N/K}} & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \\ \Big\downarrow{\scriptstyle res_L} & & \Big\downarrow{\scriptstyle \cdot[L:K]} \\ H^2(N/L) & \xrightarrow{inv_{N/L}} & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z} \end{array}$$

The extension property $(II\ a)$ of the invariant map implies that if

$$H^2(\ \ /K) = \bigcup_L H^2(L/K)$$

then there is an injective homomorphism

$$inv_K : H^2(\ \ /K) \to \mathbb{Q}/\mathbb{Z}$$

we have additional formulas for the corestriction map *cor* and the conjugate map σ^*.

Proposition 4.1.5. *Let $K \subseteq L \subseteq N$ be extensions with N/K normal, then*

- *(a)* $inv_{N/K}(cor_K c) = inv_{N/L} c$ *for* $c \in H^2(N/L)$
- *(b)* $inv_{\sigma N/\sigma K}(\sigma^* c) = inv_{N/K} c$ *for* $c \in H^2(N/K)$ *and* $\sigma \in G$

Now we can distinguish a "canonical" generator in each group $H^2(L/K)$

Definition 4.1.6. *Let L/K be a normal extension. The uniquely determined element $u_{L/K} \in H^2(L/K)$ such that*

$$inv_{L/K}(u_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z}$$

is called the ***fundamental class*** *of L/K.*

From the behaviour of the invariant map described in 4.1.5, we see how the fundamental classes of different field extensions are related, ie

Proposition 4.1.7. *Let $K \subseteq L \subseteq N$ be extensions with N/K normal, then*

- *(a)* $u_{L/K} = (u_{N/K})^{[N:L]}$ *if L/K is normal*
- *(b)* $res_L(u_{N/K}) = u_{N/L}$
- *(c)* $cor_K(u_{N/L}) = (u_{N/K})^{[L:K]}$
- *(d)* $\sigma^*(u_{N/K}) = u_{\sigma N/\sigma K}$ *for* $\sigma \in G$

Now we can apply Tate's Theorem, to obtain the main theorem of class formations

Theorem 4.1.8 (**Main Theorem**). *Let L/K be a normal extension, then the map*

$$u_{L/K}\cup : H^q(G_{L/K}, \mathbb{Z}) \to H^{q+2}(L/K)$$

given by the cup product with the fundamental class $u_{L/K} \in H^2(L/K)$ is an isomorphism in all dimensions q.

For $q = 1, 2$ we immediately obtain

Corollary 4.1.9.

$$H^3(L/K) = 1 \quad \textit{and} \quad H^4(L/K) \cong \chi(G_{L/K})$$

Since we do not have a concrete interpretation of the groups $H^q(L/K)$ in case $q = 3, 4$, or generally for all cohomology groups of higher dimensions, 4.1.9 has no immediate concrete application, however for $q = -2$ we have such an interpretation, because of the canonical isomorphisms

$$G_{L/K}^{ab} \cong H^{-2}(G_{L/K}, \mathbb{Z})$$

and

$$H^0(L/K) = A_K/N_{L/K}A_L$$

and so we obtain the following **general reciprocity law:**

Theorem 4.1.10. *Let L/K be a normal extension. Then the cup product map*

$$u_{L/K}\cup : H^{-2}(G_{L/K}, \mathbb{Z}) \to H^0(L/K)$$

yields a canonical isomorphism

$$\theta_{L/K} : G_{L/K}^{ab} \to A_K/N_{L/K}A_L$$

between the abelianization of the Galois group and the norm residue group of the module.

The isomorphism $\theta_{L/K}$ in the Theorem is called **Nakayama map**.

Chapter 5

Main Theorems in terms of ideals

5.1 Definition of Artin or reciprocity map

At this point we can make a small parenthesis to see how our main theorems can be stated in terms of ideals, instead of ideles, stating Artin reciprocity law in that case and can shortly after return to our beautiful and intuitive cohomology formalism which is the basis of our theory. For the ideas of this chapter we follow mainly Milne [4]. We can begin with the following definitions:

Definition 5.1.1. *A **modulus** for K is a function*

$$\mathfrak{m} : \{primes \ \ of \ \ K\} \to \mathbb{Z}$$

sth:

- *a)* $\mathfrak{m}(\mathfrak{p}) \geq 0$ *for all primes* $\mathfrak{p}$ *and* $\mathfrak{m}(\mathfrak{p}) = 0$ *for almost all* $\mathfrak{p}$
- *b) if* $\mathfrak{p}$ *is real, then* $\mathfrak{m}(\mathfrak{p}) = 0 \ \ or \ \ 1$
- *c) if* $\mathfrak{p}$ *is complex, then* $\mathfrak{m}(\mathfrak{p}) = 0$

one writes:

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$$

A modulus $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{m}(\mathfrak{p})}$ is said to divide a modulus $\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathfrak{n}(\mathfrak{p})}$ if

$\mathfrak{m}(\mathfrak{p}) \leq \mathfrak{n}(\mathfrak{p}) \ \forall \mathfrak{p}$.

A modulus $\mathfrak{m}$ can be written $\mathfrak{m} = \mathfrak{m}_\infty \mathfrak{m}_0$, where $\mathfrak{m}_\infty$ is a product of real primes and $\mathfrak{m}_0$ is a product of positive powers of prime ideals, ie can be identified with an ideal in O_K.

For a modulus $\mathfrak{m}$, define $K_{\mathfrak{m},1}$ to be the set of $a \in K^*$, sth

$$\begin{cases} ord_{\mathfrak{p}}(a-1) \geq \mathfrak{m}(\mathfrak{p}) & all \;\; finite \;\; \mathfrak{p}|\mathfrak{m} \\ a_{\mathfrak{p}} > 0 & all \;\; real \;\; \mathfrak{p}|\mathfrak{m} \end{cases}$$

we note that

$$ord_{\mathfrak{p}}(a-1) \geq \mathfrak{m}(\mathfrak{p}) \Leftrightarrow \pi^{\mathfrak{m}(\mathfrak{p})} | (a_{\mathfrak{p}} - 1) \Leftrightarrow$$

$$a \mapsto 1 \;\; in \;\; (O_{\mathfrak{p}}/\mathfrak{p}^{\mathfrak{m}(\mathfrak{p})})^* \cong (\hat{O}_{\mathfrak{p}}/\hat{\mathfrak{p}}^{\mathfrak{m}(\mathfrak{p})})^*$$

where π is a prime element in the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$.

Let $S(\mathfrak{m}) = \{primes \;\; dividing \;\; \mathfrak{m}\}$

For any $a \in K_{m,1}$ and prime ideal $\mathfrak{p}|\mathfrak{m}$ $ord_{\mathfrak{p}}(a-1) > 0 = ord_{\mathfrak{p}}(1)$ and so

$$ord_{\mathfrak{p}}(a) = ord_{\mathfrak{p}}((a-1)+1) = 0$$

therefore for any $a \in K_{m,1}$, the ideal $(a) \in J^{S(\mathfrak{m})}$.

..where we define J^S to be the subgroup of $J(= J_K)$ (group of fractional ideals of K), generated by prime ideals not in S , where S is any fixed finite set of primes in K

if we set

$$i : K_{\mathfrak{m},1} \to J^{S(\mathfrak{m})}$$

with

$$a \mapsto (a)$$

The quotient $C_{\mathfrak{m}} := J^{S(\mathfrak{m})}/i(K_{\mathfrak{m},1})$ is called the **(ray) class group modulo** $\mathfrak{m}$.

Let L/K be a finite abelian extension with Galois group G. Recall that, for a prime ideal $\mathfrak{p}$ of K that is unramified in L, there is a Frobenius automorphism $\sigma = (\mathfrak{p}, L/K)$ of L uniquely determined by the following condition: for every prime ideal $\mathfrak{F}$ of L lying over $\mathfrak{p}$, $\sigma\mathfrak{F} = \mathfrak{F}$ and $\sigma a \equiv a^{\mathbb{N}\mathfrak{p}} \; mod \; \mathfrak{F}$.
For any finite set S of primes in K containing all primes that ramify in L, we have the homomorphism:

$$\psi_{L/K} : J^S \to Gal(L/K)$$

with

$$\mathfrak{p}_1^{n_1} .. \mathfrak{p}_1^{n_s} \mapsto \prod_i (\mathfrak{p}_i, L/K)^{n_i}$$

the **global Artin map (or reciprocity map)**.

Proposition 5.1.2. *Let L be an abelian extension of K and K', sth $K \subseteq K' \subseteq L$, then the diagram commutes (S is defined below)*

$$\begin{array}{ccc} J_{K'}^S & \xrightarrow{\psi_{L/K'}} & Gal(L/K') \\ \downarrow{\scriptstyle Nm} & & \downarrow{\scriptstyle inclusion} \\ J_K^S & \xrightarrow{\psi_{L/K}} & Gal(L/K) \end{array}$$

Proof. Let $\mathfrak{p}' \in \{prime\ ideals\ of\ K'\}$, lying over a prime ideal $\mathfrak{p}$ of K not in S, where S is any finite set of prime ideals of K containing all those that ramify in L and also the set of primes of K' lying over a prime in S. Then $Nm_{K'/K}(\mathfrak{p}') = \mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}$ and we have to show that

$$\psi_{L/K}(\mathfrak{p}^{f(\mathfrak{p}'/\mathfrak{p})}) = \psi_{L/K'}(\mathfrak{p}') \Leftrightarrow$$

$$(\mathfrak{F}, L/K)^{f(\mathfrak{p}'/\mathfrak{p})} = (\mathfrak{F}, L/K')$$

for every $\mathfrak{F}$ lying over $\mathfrak{p}$, but this is a property of the Frobenius element for $\mathfrak{F}$ unramified over $\mathfrak{p}$ as it is accepted to be. □

Corollary 5.1.3. *For every finite abelian extension L/K, $Nm_{L/K}(J_L^S)$ is contained in the kernel of*

$$\psi_{L/K} : J^S \to Gal(L/K)$$

Proof. we can take in the previous diagram $K' = L$ □

Thus the Artin map induces a homomorphism

$$\psi_{L/K} : J_K^S / Nm(J_L^S) \to Gal(L/K)$$

The group $J_K^S/Nm(J_L^S)$ is infinite (because infinitely many primes do not split), so $\psi_{L/K}$ can not be injective, to do so, we get an isomorphism as follows:

Let S be a finite set of primes in K. We shall say that the homomorphism

$$\psi : J^S \to G$$

admits a modulus, if there exists a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) \supseteq S$, sth $\psi(i(K_{\mathfrak{m},1})) = 0$. Thus ψ admits a modulus if and only if it factors through $C_{\mathfrak{m}}$ for some $\mathfrak{m}$ with $S(\mathfrak{m}) \supseteq S$. This leads to

Theorem 5.1.4 (Reciprocity law). *Let L/K be a finite, abelian extension, S be the set of primes of K ramifying in L. Then the Artin map $\psi : J^S \to Gal(L/K)$ admits a modulus $\mathfrak{m}$ with $S(\mathfrak{m}) = S$ and it defines an isomorphism*

$$J_K^{S(\mathfrak{m})} / i(K_{\mathfrak{m},1}) \cdot Nm(J_L^{S(\mathfrak{m})}) \xrightarrow{\sim} Gal(L/K)$$

*in that case, $\mathfrak{m}$ is a **defining modulus** for L.*

Note that the Theorem does not imply that K has even a single nontrivial abelian extension. This is guaranteed by the existence theorem.

Call a subgroup H of $J_K^{\mathfrak{m}}$ a **congruence subgroup modulo** $\mathfrak{m}$, if

$$J_K^{\mathfrak{m}} \supseteq H \supseteq i(K_{\mathfrak{m},1})$$

$I_K^{\mathfrak{m}}$ denotes the group of $S(\mathfrak{m})$-ideals in K and $J_L^{\mathfrak{m}}$ the group of $S(\mathfrak{m})'$-ideals in L, where $S(\mathfrak{m})'$ contains the primes of L lying over a prime in $S(\mathfrak{m})$.

Then we state the following:

Theorem 5.1.5 (**Existence**). *For every congruence subgroup H modulo $\mathfrak{m}$, there exists a finite abelian extension L/K, such that*

$$H = i(K_{\mathfrak{m},1}) \cdot Nm_{L/K}(J_L^{\mathfrak{m}})$$

The field L corresponding to a congruence subgroup H is called the **class field** of H, whence the name of the subject.

Theorems 5.1.4 and 5.1.5 show that, for any number field K, there is a canonical isomorphism $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}} \to Gal(K^{ab}/K)$. Rather than studying $\varprojlim_{\mathfrak{m}} C_{\mathfrak{m}}$ directly, it turns out to be more natural to introduce another group that has it as a quotient; this is the idele class group, which is the main object of our cohomology theory.

I will tell you a story about the Reciprocity Law. After my thesis, I had the idea to define L-series for non-abelian extensions. But for them to agree with the L-series for abelian extensions, a certain isomorphism had to be true. I could show it implied all the standard reciprocity laws. So I called it the General Reciprocity Law and tried to prove it but couldn't, even after many tries. Then I showed it to the other number theorists, but they all laughed at it, and I remember Hasse in particular telling me it couldn't possibly be true. Still, I kept at it, but nothing I tried worked. Not a week went by — for three years ! — that I did not try to prove the Reciprocity Law. It was discouraging, and meanwhile I turned to other things. Then one afternoon I had nothing special to do, so I said, "Well, I try to prove the Reciprocity Law again." So I went out and sat down in the garden. You see, from the very beginning I had the idea to use the cyclotomic fields, but they never worked, and now I suddenly saw that all this time I had been using them in the wrong way — and in half an hour I had it.

Emil Artin, as recalled by Mattuck (in Recountings: Conversations with MIT Mathematicians 2009).

Chapter 6

Global class field theory

6.1 Ideles and Idele classes

In the following we will consider **ideles** as in Neukirch [1], [3], Milne [4] and Lang [6] which were first intoduced by Chevalley, in the first two sections we use extensively [6],[8]. The notion of ideles is a slight modigication of the notion of ideals, or more precisely of divisors and its significance lies in the fact that it permits a transition between global and local number theory, and therefore represents a suitable mean for applying the local-global principle, which is a method to obtain theorems and definitions in global class field theory from local class field theory[1]. The development of the global theory using ideles with cohomological methods is particularly transparent and has led to a plethora of far reaching results. The analytic methods, ie Dirichlet series and their generalizations which were necessary in the classical ideal theoretic treatment have subsequently disappeared.

Let K be an algebraic number field. An **idele** a of K is a family $a = (a_\mathfrak{p})$ of elements $a_\mathfrak{p} \in K_\mathfrak{p}^*$ such that $\mathfrak{p}$ ranges over all primes of K, but $a_\mathfrak{p}$ is a unit in $K_\mathfrak{p}$ for almost all primes $\mathfrak{p}$.

Definition 6.1.1. *Let S be a finite set of primes of K. The group*

$$I_K^S = \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^* \times \prod_{\mathfrak{p}\notin S} U_\mathfrak{p} \subseteq \prod_{\mathfrak{p}} K_\mathfrak{p}^*$$

*is called the **group of S-ideles**. The union*

$$I_K = \bigcup_S I_K^S \subseteq \prod_{\mathfrak{p}} K_\mathfrak{p}^*$$

*where S runs through all finite sets of primes of K, is the **idele group** of K. If $a = (a_\mathfrak{p}) \in I_K$, $a_\mathfrak{p} \in K_\mathfrak{p}^*$, then the $a_\mathfrak{p}$ are the **local components** of the idele a, an $a_\mathfrak{p} \in K_\mathfrak{p}^*$ is an **essential component** of a if $a_\mathfrak{p}$ is not a unit.*

[1] Class field theory has a reputation for being difficult, which is partly justified. But it is necessary to make a distinction: there is perhaps nowhere in science a theory in which the proofs are so difficult but at the same time the results are of such perfect simplicity and of such great power.
J. Herbrand 1936

We now want to define the idele class group of K as the factor group $C_K = I_K/K^*$. To do so we use the following definition

Definition 6.1.2. *Let L/K be Galois with $G = Gal(L/K)$, we define a norm map*

$$N = N_K^L : I_L \to I_K$$
$$x = (x_w) \mapsto y = (y_v)$$

by $y_v := \prod_{w|v} N_{K_v}^{L_w}(x_w)$ (where v, w are primes.. we use these symbols instead of the usual $\mathfrak{p}$, $\mathfrak{F}$ interchangeably)

$$\begin{array}{ccc} (..., x_{w_1}, ... & & ..., x_{w_n}, ...) = x \\ & \searrow^{N_{K_v}^{L_{w_1}}} & \downarrow N_{K_v}^{L_{w_n}} \\ & & (..., y_v, ...) = y \end{array}$$

Lemma 6.1.3. *(**Properties of the norm map**)*

1 If $K \leq L \leq M$, then $N_K^M = N_L^M \cdot N_K^L$

2 If L/K is Galois, then $N_K^L(x) = \prod_{\sigma \in Gal(L/K)} \sigma x$

3 $N_K^L(x) = x^{[L:K]} \quad \forall x \in I_K$

4 The diagram

$$\begin{array}{ccc} L^* & \xrightarrow{N_K^L} & K^* \\ \downarrow \iota & & \downarrow \iota \\ I_L & \xrightarrow{N_K^L} & I_K \end{array}$$

commutes.

Proof. we prove the $4th$ property, assuming more specifically that L/K is Galois. Let $x \in L^*$, we choose a place (ie prime) v and fix a place $w_0|v$, we obtain

$$\{w : w|v\} = \{\sigma w_0, \sigma \in G\} = \{\sigma w_0, \sigma \in G/G_{w_0}\}$$

where

$$G_{w_0} = \{\sigma \in G : \sigma w_0 = w_0\}$$

the decomposition group of w_0. For any $x \in L^*$ we obtain the v-component of $N_K^L(\underbrace{(x, .., x)}_{\iota(x)})$ as

$$\prod_{w|v} N_{K_v}^{L_w}(x) = \prod_{\sigma \in G/G_{w_0}} N_{K_v}^{L_{\sigma w_0}}(x) = \prod_{\sigma \in G/G_{w_0}} \prod_{\tau \in Gal(L_{\sigma w_0}/K_v)} \tau x =$$

$$\prod_{\sigma\in G/G_{w_0}}\prod_{\tau\in\sigma Gal(L_{\sigma w_0}/K_v)\sigma^{-1}}\tau x=\prod_{\sigma\in G/G_{w_0}}\prod_{\tau\in Gal(L_{\sigma w_0}/K_v)}\sigma\tau\sigma^{-1}x$$

$$\prod_{\sigma\in G/G_{w_0}}\sigma\underbrace{\prod_{\tau\in Gal(L_{w_0}/K_v)}\tau\sigma^{-1}x}_{N_{K_v}^{L_{w_0}}(\sigma^{-1}x)\,\in\,\prod K_v^*}$$

(the field in the last bracket is a base field, hence invariant under σ, and therefore can be omitted)

$$=\prod_{\sigma\in G/G_{w_0}}\prod_{\tau\in G_{w_0}(L/K)}\tau\sigma^{-1}x=\prod_{\sigma\in G}\sigma x=N_K^L(x)$$

which implies that

$$N_K^L((x,..,x))=(N_K^L(x),..,N_K^L(x))$$

or

$$N_K^L\circ\iota(x)=\iota\circ N_K^L(x)$$

□

Lemma 6.1.4. *The following diagram commutes*

$$\begin{array}{ccc} I_L & \xrightarrow{N_K^L} & I_K \\ \downarrow{\scriptstyle \psi_L} & & \downarrow{\scriptstyle \psi_K} \\ J_L & \xrightarrow{N_K^L} & J_K \end{array}$$

Reminder:

$x=(x_v)_v\mapsto_\psi \prod_{\mathfrak{p}\leq O_K}\mathfrak{p}^{v_\mathfrak{p}(x_\mathfrak{p})}$ (in this way we get from an Idele to an ideal).

Proof. Let $x=(x_w)_w\in I_L$. Since

$$v_\mathfrak{p}(N_{K_\mathfrak{p}}^{L_\mathfrak{k}}(x_\mathfrak{k}))=f_{\mathfrak{k}|\mathfrak{p}}v_\mathfrak{k}(x_\mathfrak{k})$$

(because $N(\mathfrak{k})=\mathfrak{p}^{f_{\mathfrak{k}|\mathfrak{p}}}\Rightarrow v_\mathfrak{p}(N(\mathfrak{k}))=f_{\mathfrak{k}|\mathfrak{p}}v_\mathfrak{k}(\mathfrak{k})$)

$$\psi_K(N_K^L(x))=\psi_K((\prod_{\mathfrak{k}|\mathfrak{p}}N_{K_\mathfrak{p}}^{L_\mathfrak{k}}(x_\mathfrak{k}))_\mathfrak{p},\underbrace{\cdots}_{archimedean-places})=$$

$$\prod_{\mathfrak{p}\leq O_K}\prod_{\mathfrak{k}|\mathfrak{p}}\mathfrak{p}^{f_{\mathfrak{k}|\mathfrak{p}}v_\mathfrak{k}(x_\mathfrak{k})}=\prod_{\mathfrak{k}\leq O_L}N_K^L(\mathfrak{k})^{v_\mathfrak{k}(x_\mathfrak{k})}=N_K^L(\prod_{\mathfrak{k}\leq O_L}(\mathfrak{k})^{v_\mathfrak{k}(x_\mathfrak{k})})=$$

$$N_K^L(\psi_L(\underbrace{x}_{(x_\mathfrak{k})_\mathfrak{k}}))$$

□

Corollary 6.1.5. *The norm induces a mapping*

$$N_K^L : \underbrace{I_L/L^*}_{C_L} \to \underbrace{I_K/K^*}_{C_K}$$

an idele class group.

6.2 Generalized idele class group

In this section we deduce from the norm index inequalities based on ideals (we proved the second norm index inequality with analytic methods), the ones based on idele class groups and see that the indices are equal. Let $K/\mathbb{Q}$ be a number field, for any valuation v (of the field K) and any integer $m \in \mathbb{N}_0$ we define a subgroup $U_v(m) \leq K_v^*$ as follows:

$$U_v(m) := \begin{cases} 1 + \mathfrak{m}_v^m & m \geq 1 \\ U_v = O_v^* & m = 0 \end{cases} \quad for \;\; v = \mathfrak{p} \;\; nonarchimedean$$

Let A be the integral closure of $\mathbb{Z}$ in K, ie the ring of algebraic integers of K. Denote by A_v the closure of A in K_v, and let $o = A_{\mathfrak{p}}$ be the local ring at $\mathfrak{p}$. All the elements of o have a $\mathfrak{p}$-adic absolute value ≤ 1 because their orders at $\mathfrak{p}$ are ≥ 0. Hence o lies in the closure of A, and hence the closure of o in K_v is the same as the closure of A. It is called the ring of $\mathfrak{p}$-adic integers in K_v and $\mathfrak{m}_v$ is the maximal ideal in the complete local ring o_v. We may say that $W_{\mathfrak{m}}(v)$ (see below) is a disc of center 1 in the $\mathfrak{p}$-adic field.

$$U_v(m) := \begin{cases} \mathbb{R}_{>0}^* & m \geq 1 \\ \mathbb{R}^* & m = 0 \end{cases} \quad for \;\; v \;\; archimedean \;\; and \;\; real$$

$$U_v(m) := \mathbb{C}^* \;\; for \;\; all \;\; m \quad for \;\; v \;\; archimedean \;\; and \;\; complex$$

For all v we set

$$O_v^* := U_v(0) = \begin{cases} O_v^* & v \;\; nonarchimedean \\ \mathbb{R}^* & v \;\; real \\ \mathbb{C}^* & v \;\; complex \end{cases}$$

Notation 6.2.1. *An index "$J(\mathfrak{m})$" is the "group of fractional ideals" "prime to $\mathfrak{m}$; an index $P_{\mathfrak{m}}$, $W_{\mathfrak{m}}$, $I_{\mathfrak{m}}$ means "prime to $\mathfrak{m}$ and $\equiv 1 \; (mod \; \mathfrak{m})$" (ie locally the elements are units at all places v dividing $\mathfrak{m}$ and are even $\equiv 1 \; (mod \; v^{\mathfrak{m}_v})$, where P is the group of principal ideals, the rest are defined below..*

we can use "c" instead of "$\mathfrak{m}$" as a cycle, and also refer to [6] for more details.

Notation 6.2.2. *$U_v(m) \leq K_v^*$ is called the subgroup of m-units in K_v^**

Let now $\mathfrak{m} = \prod_v v^{m_v}$ be a cycle in K, we define the following subgroups:

- $W_{\mathfrak{m}}(v) := U_v(m_v) \leq K_v^*$
- $W_{\mathfrak{m}} := \prod_{v|\mathfrak{m}} W_{\mathfrak{m}}(v) \times \prod_{v\nmid\mathfrak{m}} \underbrace{O_v^*}_{W_{\mathfrak{m}}(v)\ (=U_v(m_v))} \leq I_K$

$$because\ m_v = 0 \quad for\ v \nmid \mathfrak{m}$$

- $I_{\mathfrak{m}} := \{x = (x_v)_v \in I_K : x_v \in W_{\mathfrak{m}}(v)\ for\ all\ v \mid \mathfrak{m}\} \leq I_K =$

$$\prod_{v|\mathfrak{m}} W_{\mathfrak{m}}(v) \times \prod_{v\nmid\mathfrak{m}} K_v^*$$

Remark 6.2.3. *1) $I_{\mathfrak{m}} \leq I$ is the subgroup consisting of all ideles $x = (x_v)_v$ whose components at all $v \mid \mathfrak{m}$ are m_v-units.*

2) $W_{\mathfrak{m}} \leq I_{\mathfrak{m}}$ consists of all ideles $x = (x_v)_v$ whose components are m_v-units ***at all*** *places v.*

3) we have

$$K_{\mathfrak{m}} = K^* \cap I_{\mathfrak{m}} \quad (K^* \hookrightarrow I)$$

Lemma 6.2.4. *We have*

$$I_{\mathfrak{m}}/K_{\mathfrak{m}} \cong I/K^* \quad (idele\ class\ group)$$

Proof. we define the mapping

$$\phi : I_{\mathfrak{m}}/K_{\mathfrak{m}} \to I/K^*$$
$$xK_{\mathfrak{m}} \mapsto xK^*$$

since $K_{\mathfrak{m}} = K^* \cap I_{\mathfrak{m}}$ the map ϕ is injective.. and we prove surjectivity.

Let $x = (x_v)_v \in I$ be arbitrary. By the approximation theorem there is an element $\alpha \in K^*$ such that $v(\alpha - x_v) < \epsilon$ for all $v \mid \mathfrak{m}$

$\Rightarrow v(1 - \alpha^{-1}x_v) < \dfrac{\epsilon}{v(\alpha)}$ for all $v \mid \mathfrak{m}$

$\Rightarrow \alpha^{-1}x_v \in U_v(\mathfrak{m}_v)$ for all $v \mid \mathfrak{m}$ if ϵ is chosen sufficiently small

$\Rightarrow \alpha^{-1}x \in I_{\mathfrak{m}}$

since $\phi(\underbrace{\alpha^{-1}x}_{I_{\mathfrak{m}}}) = \alpha^{-1}x\ K^* = xK^*$

we find that ϕ is surjective. □

Definition 6.2.5. *The quotient*

$$C_{\mathfrak{m}} := I_{\mathfrak{m}}/K_{\mathfrak{m}}W_{\mathfrak{m}}$$

is called the (generalized) idele class group attached to the cycle $\mathfrak{m}$ *in* K*.*

Proposition 6.2.6. ***(idele theoretic interpretation of generalized ideal class group)***

For any cycle $\mathfrak{m}$ *there is an isomorphism*

$$I_{\mathfrak{m}}/K_{\mathfrak{m}}W_{\mathfrak{m}} \cong J(\mathfrak{m})/P_{\mathfrak{m}}$$

Proof. consider the mapping

$$\psi : I_{\mathfrak{m}} \to J(\mathfrak{m})$$

$$x \mapsto (x)$$

since ψ vanishes on $W_{\mathfrak{m}}$ (elements in $W_{\mathfrak{m}}$ are units at all places), we obtain

$\psi(K_{\mathfrak{m}}W_{\mathfrak{m}}) = \psi(K_{\mathfrak{m}}) \subseteq P_{\mathfrak{m}}$ (by definition of $P_{\mathfrak{m}}$)

Thus we obtain a mapping

$$\overline{\psi} : I_{\mathfrak{m}}/K_{\mathfrak{m}}W_{\mathfrak{m}} \to J(\mathfrak{m})/P_{\mathfrak{m}}$$

surjectivity of $\overline{\psi}$ is immediate because ψ is obviously surjective.. we prove therefore injectivity.

Let $x \in I_{\mathfrak{m}}$ and assume that $\psi(x) \in P_{\mathfrak{m}}$

(ie $xK_{\mathfrak{m}}W_{\mathfrak{m}} \in ker\ \overline{\psi}$)

$\Rightarrow (x) = \psi(x) = (\underbrace{\alpha}_{\in P_{\mathfrak{m}}})$ for some $\alpha \in K_{\mathfrak{m}}$

$\Rightarrow (\alpha^{-1}x) = (1)$

$\Rightarrow \alpha^{-1}x = b$ for some(any) $b \in I^{S_\infty}$ $(\Rightarrow (b) = (1)\ )$

since $\underbrace{\alpha^{-1}}_{\in K_{\mathfrak{m}}}$, $\underbrace{x_v}_{\in I_{\mathfrak{m}}} \in U_v(\mathfrak{m}_v)$ for all $v|\mathfrak{m}$

we obtain b even is contained in $W_{\mathfrak{m}}$. This implies

$$x = ab \in K_{\mathfrak{m}}W_{\mathfrak{m}}$$

since x was arbitrary this shows that

$$\psi^{-1}(P_{\mathfrak{m}}) = K_{\mathfrak{m}}W_{\mathfrak{m}}$$

$\Rightarrow \overline{\psi}$ is injective. □

6.2.1 The norm residue group

Let L/K be an extension of number fields.

Definition 6.2.7. *A cycle $\mathfrak{m} = \prod_v v^{m_v}$ in K is called admissible for the extension L/K iff*

$$\underbrace{W_{\mathfrak{m}}(v)}_{\leq K_v^*} \subseteq N_{K_v}^{L_w} L_w^*$$

for all places $v|\mathfrak{m}$ and all places $w|v$.

Aim: Idele theoretic interpretation of the norm residue group

$$J_K(\mathfrak{m})/P_{\mathfrak{m}} N_K^L J_L(\mathfrak{m})$$

Proposition 6.2.8. *Let $\mathfrak{m}$ be an admissible cycle in K for the extension L/K. Then*

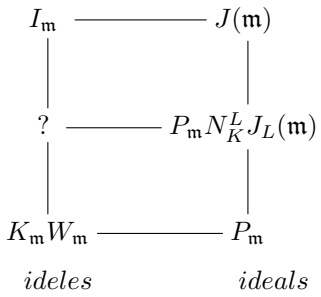
$$\underbrace{I_K/K^* N_K^L I_L}_{\text{I consider things locally(without } K^*) \text{ and then insert } K^*} \cong \underbrace{J_K(\mathfrak{m})/P_{\mathfrak{m}} N_K^L J_L(\mathfrak{m})}_{\text{here things are hopelessly mixed}}$$

Proof. we consider the mapping

$$\psi : I_{\mathfrak{m}} \to J(\mathfrak{m})$$

$$x \mapsto (x)$$

By Proposition in the previous subsection we already know that $\psi^{-1}(P_{\mathfrak{m}}) = K_{\mathfrak{m}} W_{\mathfrak{m}}$ and $I_{\mathfrak{m}}/K_{\mathfrak{m}} W_{\mathfrak{m}} \cong J(\mathfrak{m})/P_{\mathfrak{m}}$.



we claim

$$\psi^{-1}(P_{\mathfrak{m}} N_K^L J_L(\mathfrak{m})) = K^* N_K^L I_L \cap I_{\mathfrak{m}}$$

this implies the assertion of the Proposition. To prove this equation we verify **both implications**.

" $\supseteq$ "

Let $\alpha\ N_K^L y \subseteq I_{\mathfrak{m}}$ where $\alpha \in K^*$ and $y = (y_w)_w \in I_L$ ie $\alpha\ N_K^L y$ is contained in the rHS of our eq.

By approximation Theorem there is $\beta \in L$ sth βy_w is sufficiently close to $1 \in O_w^*$ for all $w|\mathfrak{m}$

$\Rightarrow N_K^L \beta y_w$ is sufficiently close to $1 \in O_v^*$ $(\leq K_v^*)$

$\Rightarrow N_K^L(\ \underbrace{\beta y}_{full\ idele}\ ) \in I_{\mathfrak{m}}$

we obtain $\underbrace{\alpha N y}_{\in I_{\mathfrak{m}}} = \alpha N \beta^{-1}\ \ \underbrace{N\ (\beta y)}_{\in I_{\mathfrak{m}}}$

which implies $\alpha N(\beta^{-1}) \in I_{\mathfrak{m}}$

$\Rightarrow \alpha N(\beta^{-1}) \in \underbrace{I_{\mathfrak{m}} \cap K^*}_{K_{\mathfrak{m}}}$ $\quad (\alpha \in K^*\ \ and\ \ \beta \in L^*)$

we therefore obtain

$\psi(\alpha N(y)) = \psi(\alpha N(\beta)^{-1})\psi(N(\beta y)) =$

$\psi(\underbrace{\alpha N(\beta^{-1})}_{K_{\mathfrak{m}}})\ \ \underbrace{N\,\psi(\underbrace{\beta y}_{\in I_{\mathfrak{m}}})}_{J_L(\mathfrak{m})}\ \ \subseteq$

$\subseteq\ P_{\mathfrak{m}}\ N_K^L J_L(\mathfrak{m})$

in other words

$\alpha N(y) \in \psi^{-1}(P_{\mathfrak{m}}\ N_K^L J_L(\mathfrak{m}))$

we now want to prove the **opposite direction..**

" $\subseteq$ "

Let $x \in I_{\mathfrak{m}}$ and assume that $x \in \psi^{-1}(P_{\mathfrak{m}}\ N_K^L J_L(\mathfrak{m}))$, then

$$\psi(x) = (\alpha) N_K^L \mathfrak{u}$$

where $\alpha \in K_{\mathfrak{m}}$ and $\mathfrak{u} \in J_L(\mathfrak{m})$, we select an idele $A = (A_w)_w \in I_L$ sth

$v_{\mathfrak{k}}(\underbrace{A_{\mathfrak{k}}}_{\in L_{\mathfrak{k}}}) = v_{\mathfrak{k}}(\mathfrak{u})$ for all $\mathfrak{k} \nmid \mathfrak{m}$ $\quad (\mathfrak{k} \leq O_L)$ and

$A_{\mathfrak{k}} = 1$ for all $\mathfrak{k}|\mathfrak{m}$

then we obtain that $\psi_L(A) = \mathfrak{u}$

which implies that

$$(x) = \psi(x) = (\alpha)N_K^L\mathfrak{u} = (\alpha)\ (N_K^L A) = (\alpha N_K^L A)$$

This shows that

$$x = \alpha N_K^L A \cdot w$$

by an element $w \in I^{S_\infty}$. Since furthermore $x \in I_\mathfrak{m}$ and

$$\underbrace{\alpha}_{\in K_\mathfrak{m}\ I_\mathfrak{m}} \quad \underbrace{N_K^L(A)}_{because\ A_\mathfrak{t}=1\ for\ all\ \mathfrak{t}|\mathfrak{m}} \quad \in I_\mathfrak{m}$$

we see that $w \in I_\mathfrak{m}$ hence $w \in I_\mathfrak{m} \cap I^{S_\infty} = W_\mathfrak{m}$

Since $\mathfrak{m}$ is admissible for L/K we know that all elements in $W_\mathfrak{m}$ are norms of elements, thus there is an idele $B \in I_L$ sth $N_K^L(B) = w$

Altogether we obtain

$$x = \alpha N_K^L(A) \cdot w = \alpha N_K^L(A)\ N_K^L(B) = \alpha N_K^L(\underbrace{AB}_{\in I_L}) \in K^*\ N_K^L I_L$$

Therefore our equation is proven. □

Corollary 6.2.9. *Let $\mathfrak{m}$ be admissible for L/K. Then we have*

$$[I_K : K^* N_K^L I_L] \leq [L : K]$$

Proof. $I_K/K^*N_K^L I_L \cong J(\mathfrak{m})/P_\mathfrak{m} N_K^L J_L(\mathfrak{m})$ and the claim is shown above. □

Remark 6.2.10. *For any extention L/K it holds that*

$$I_K/K^*N_K^L I_L \cong C_K/N_K^L C_L$$

Proof. $C_K/N_K^L C_L \cong (I_K/K^*)/(N_K^L I_L\ K^*/K^*) \cong I_K/K^*N_K^L I_L$ □

Altogether we obtain:

Corollary 6.2.11.

$$[C_K : N_K^L C_L] = [I_K : K^* N_K^L I_L] = [J(\mathfrak{m}) : P_\mathfrak{m} N_K^L J_L(\mathfrak{m})] \leq [L : K]$$

Note: we can use the idele theoretic formulation of the norm residue group to prove the remaining 1^{st} norm index inequality, we will save the time of doing so, by following the guidelines of abstract class field theory instead which we developed earlier.

both inequalities will supply us with the isomorphism

$$J(\mathfrak{m})/P_\mathfrak{m} N_K^L J_L(\mathfrak{m}) \xrightarrow{\sim} Gal(L/K)$$

After this small parenthesis we continue our formulation:

6.3 Continuation of the formulation based on ideles and idele classes

Proposition 6.3.1. *Let S_∞ be the set of infinite primes of K and $I_K^{S_\infty}$ the group of ideles which have units as components at all finite primes, then*

$$I_K/I_K^{S_\infty} \cong J_K$$
$$I_K/(I_K^{S_\infty} \cdot K^*) \cong J_K/P_K$$

J_K,P_K are the group of ideals and principal ideals respectively.

Proof. Let $\mathfrak{p}$ be a finite prime of the field K and $v_\mathfrak{p}$ be the valuation of $K_\mathfrak{p}$ normalized with minimal positive value 1. If $a \in I_K \Rightarrow a_\mathfrak{p} \in U_\mathfrak{p}$ for almost all finite primes, thus $v_\mathfrak{p} a_\mathfrak{p} = 0$, so we have the well defined map

$$\phi : a \mapsto \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_\mathfrak{p} a_\mathfrak{p}}$$

as a canonical homomorphism from I_K to J_K, obviously $ker\phi = I_K^{S_\infty}$, which proves the first assertion. The second is analogous. □

Remark 6.3.2. *$I_K/I_K^{S_\infty}$ is the well known group of fractional ideals of K.*

Proposition 6.3.3. *Let S be a sufficiently large finite set of primes. Then*

$$I_K = I_K^S \cdot K^*$$

, and therefore

$$C_K = I_K^S \cdot K^*/K^*$$

Remark 6.3.4. *The embedding (ie injective homomorphism) of $a \in I_K$ in $a' \in I_L$ is as follows*

$$a'_\mathfrak{F} = a_\mathfrak{p} \in K_\mathfrak{p} \subseteq L_\mathfrak{F}$$

for $\mathfrak{F}|\mathfrak{p}$.

where we mention again that $\mathfrak{p}$,$\mathfrak{F}$ are primes denoted also by v,w without distinction. This allows us to think of I_K as a subgroup of I_L.

If L/K is normal and $G = G_{L/K}$ denotes its Galois group, I_L is canonically a G-module: An element $\sigma \in G$ defines a canonical isomorphism from $L_{\sigma^{-1}\mathfrak{F}}$ onto $L_\mathfrak{F}$, which we also denote by σ. Here we associate with an idele $a \in I_L$ with components $a_\mathfrak{F} \in L_\mathfrak{F}^*$ the idele $\sigma a \in I_L$ with components

$$(\sigma a)_\mathfrak{F} = \sigma a_{\sigma^{-1}\mathfrak{F}} \in L_\mathfrak{F}$$

Proposition 6.3.5. *Let L/K be normal and $G = G_{L/K}$ its galois group. Then*

$$I_L^G = I_K$$

It is well known that an ideal of a field K can very well become a principal ideal in an extension field L without being a principal ideal in the base field K. Ideles behave differently.[2] In particular, if $a \in I_K$ is an idele of K that becomes principal idele in the extension L, ie, $a \in L^*$, then a is already principal in K. We prove it with the following:

Proposition 6.3.6. *If L/K is an arbitrary finite extension, then*

$$L^* \cap I_K = K^*$$

Proof. The inclusion $K^* \subseteq L^* \cap I_K$ is trivial. Let $\overline{L}$ be a finite normal extension of K containing L and let $\overline{G} = G_{\overline{L}/K}$ be its Galois group. Then I_K and I_L are subgroups of $I_{\overline{L}}$. If $a \in \overline{L}^* \cap I_K$, then the last proposition shows that $a \in I_{\overline{L}}^{\overline{G}}$, ie, $\sigma a = a$, for all $\sigma \in \overline{G}$ and because $a \in \overline{L}^*$ we even have $a \in (\overline{L}^*)^{\overline{G}} = K^*$. Therefore $\overline{L}^* \cap I_K = K^*$, which implies $L^* \cap I_K \subseteq \overline{L}^* \cap I_K = K^*$. □

6.4 Cohomology of the idele group

Let L/K be a finite normal extension with Galois group $G = G_{L/K}$. While working with groups $H^q(G, I_L)$ we can see that these can be localized ,ie, decomposed into a direct product of cohomology groups over the local fields $K_\mathfrak{p}$.

Initially we can write

$$I_L^S = \prod_{\mathfrak{p} \in S} I_L^P \times \prod_{\mathfrak{p} \notin S} U_L^P$$

where

$$I_L^\mathfrak{p} = \prod_{\mathfrak{F}|\mathfrak{p}} L_\mathfrak{F}^*$$

$$U_L^\mathfrak{p} = \prod_{\mathfrak{F}|\mathfrak{p}} U_\mathfrak{F}$$

which are also G-modules since the automorphisms $\sigma \in G$ only permute the primes $\mathfrak{F}$ above $\mathfrak{p}$.

We have the following:

Proposition 6.4.1. *Let $\mathfrak{F}$ be a prime of L above $\mathfrak{p}$, then*

$$H^q(G, I_L^\mathfrak{p}) \cong H^q(G_\mathfrak{F}, L_\mathfrak{F}^*)$$

[2] ...to my shame, I have been unable to find the "corollary" stating that all ideals of K become principal in the largest abelian extension unramified at the finite primes. If it can be explained in two words, I would be very grateful to you.

Serre responded:
Enclosed is a little paper on the "Hauptidealsatz" explaining how the theorem can be reduced to an (actually very mysterious) theorem in group theory. This in fact is the reduction given by Artin himself in his paper on the subject; if you could find a beautiful cohomological proof on the theorem, it would be so much better, but everyone has got stuck on it up to now.

"Grothendieck letter to Serre, 19.9.1956"

$G_{\mathfrak{F}}$ is the decomposition group of $\mathfrak{F}$ over K. If $\mathfrak{p}$ is a finite, unramified prime in L, then

$$H^q(G, U_L^{\mathfrak{p}}) = 1$$

for all q.

Proof. $I_L^{\mathfrak{p}} = \prod_{\sigma \in G/G_{\mathfrak{F}}} L^*_{\sigma\mathfrak{F}} = \prod_{\sigma \in G/G_{\mathfrak{F}}} \sigma L^*_{\mathfrak{F}}$

$U_L^{\mathfrak{p}} = \prod_{\sigma \in G/G_{\mathfrak{F}}} \sigma U_{\mathfrak{F}}$

which shows that $I_L^{\mathfrak{p}}$, $U_L^{\mathfrak{p}}$ are $G/G_{\mathfrak{F}}$ induced G-modules, thus applying Shapiro's Lemma

$$H^q(G, I_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{F}}, L^*_{\mathfrak{F}})$$
$$H^q(G, U_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{F}}, U_{\mathfrak{F}})$$

this isomorphism is given by the composition

$$H^q(G, I_L^{\mathfrak{p}}) \xrightarrow{res} H^q(G_{\mathfrak{F}}, I_L^{\mathfrak{p}}) \xrightarrow{\overline{\pi}} H^q(G_{\mathfrak{F}}, L^*_{\mathfrak{F}})$$

$\overline{\pi}$ is induced by the canonical projection $I_L^{\mathfrak{p}} \xrightarrow{\pi} L^*_{\mathfrak{F}}$ that takes each idele in $I_L^{\mathfrak{p}}$ to its $\mathfrak{F}$-component. If $\mathfrak{p}$ is unramified in L then the extension $L_{\mathfrak{F}}/K_{\mathfrak{p}}$ is unramified and we can refer to local class field theory to obtain the result

$$H^q(G, U_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{F}}, U_{\mathfrak{F}}) = 1$$

□

Theorem 6.4.2. *If S is a finite set containing all finite primes of K which are ramified in L, then*

$$\forall \mathfrak{p} \notin S, \quad H^q(G, U_L^{\mathfrak{p}}) = 1$$

and

$$H^q(G, I_L^S) \cong \prod_{\mathfrak{p} \in S} H^q(G_{\mathfrak{F}}, L^*_{\mathfrak{F}})$$

for $\mathfrak{F}|\mathfrak{p}$

Then $I_L = \bigcup_S I_L^S$ gives us

$$H^q(G, I_L) \cong \varinjlim_S H^q(G, I_L^S) \cong \bigoplus_{\mathfrak{p}} H^q(G_{\mathfrak{F}}, L^*_{\mathfrak{F}})$$

this isomorphism is given by the composition of maps

$$H^q(G, I_L) \xrightarrow{res} H^q(G_{\mathfrak{F}}, I_L) \xrightarrow{\overline{\pi}} H^q(G_{\mathfrak{F}}, L^*_{\mathfrak{F}})$$

and $\overline{\pi}$ is induced by the canonical projection $I_L \xrightarrow{\pi} L^*_{\mathfrak{F}}$ which takes each idele a to its $\mathfrak{F}$-component $a_{\mathfrak{F}}$, ie

$$I_L \xrightarrow{\pi} L^*_{\mathfrak{F}}$$
$$a \mapsto a_{\mathfrak{F}}$$

The above projections map each element $c \in H^q(G, I_L)$ to its $\mathfrak{p}$-components $c_\mathfrak{p} \in H^q(G_\mathfrak{F}, L_\mathfrak{F}^*)$. We can see above that each c is uniquely determined by its **local components** $c_\mathfrak{p}$, which because of the direct sum are almost all equal to 1. In dimensions $q > 0$ the map $c \mapsto c_\mathfrak{p}$ can be described in the following simple way. Given a cohomology class $c \in H^q(G, I_L)$ choose a cocycle $a(\sigma_1, ..., \sigma_q)$ representing c. This is a function on the group G which takes values in the idele group I_L. Restrict this function to the group $G_\mathfrak{F}$ and take the $\mathfrak{F}$-components $a_\mathfrak{F}(\sigma_1, ..., \sigma_q)$ of the idele $a(\sigma_1, ..., \sigma_q)$. The resulting function from $G_\mathfrak{F}$ to $L_\mathfrak{F}^*$ is a cocycle, and its cohomology class $c_\mathfrak{p} \in H^q(G_\mathfrak{F}, L_\mathfrak{F}^*)$ is the $\mathfrak{p}$-component of c.

When we change the field, taking local components is affected according to

Proposition 6.4.3. *Let $K \subseteq L \subseteq N$ be normal extensions of K and $\mathfrak{F}'|\mathfrak{F}|\mathfrak{p}$ primes of N, L, K, then*

$$(inf_N c)_\mathfrak{p} = inf_{N_{\mathfrak{F}'}}(c_\mathfrak{p})$$

for $c \in H^q(G_{L/K}, I_L)$, $q \geq 1$

$$(res_L c)_\mathfrak{F} = res_{L_\mathfrak{F}}(c_\mathfrak{p})$$

for $c \in H^q(G_{N/K}, I_N)$

$$(cor_K c)_\mathfrak{p} = \sum_{\mathfrak{F}|\mathfrak{p}} cor_{K_\mathfrak{p}}(c_\mathfrak{F})$$

for $c \in H^q(G_{N/L}, I_N)$

for the last two properties it is sufficient to assume $N|K$ normal.

In particular the isomorphism

$$H^q(G, I_L) \cong \bigoplus_\mathfrak{p} H^q(G_\mathfrak{F}, L_\mathfrak{F}^*)$$

yields the following corollary **Norm Theorem for ideles**

Corollary 6.4.4. *An idele $a \in I_K$ is the norm of an idele $b \in I_L$ iff each component $a_\mathfrak{p} \in K_\mathfrak{p}^*$ is the norm of an $b_\mathfrak{F} \in L_\mathfrak{F}^*$ $(\mathfrak{F}|\mathfrak{p})$,ie iff it is a local norm everywhere.*

Proof. $H^0(G, I_L) = I_L^G / N_G I_L = I_K / N_G I_L$

also $H^0(G_\mathfrak{F}, L_\mathfrak{F}^*) = K_\mathfrak{p}^* / N_{G_\mathfrak{F}} L_\mathfrak{F}^*$, thus we have

$$I_K / N_G I_L \cong \bigoplus_\mathfrak{p} K_\mathfrak{p}^* / N_{G_\mathfrak{F}} L_\mathfrak{F}^*$$

If $a \in I_K$ then this isomorphism takes the 0-cohomology class $a \cdot N_G I_L = \overline{a}$ to its components $\overline{a}_\mathfrak{p}$, which can be computed as $\overline{a}_\mathfrak{p} = a_\mathfrak{p} \cdot N_{G_\mathfrak{F}} L_\mathfrak{F}^*$
Now since we have an isomorphism. $\overline{a} = 1$ if and only if $\overline{a}_\mathfrak{p} = 1$, ie $a \in N_G I_L$ if and only if for every component $a_\mathfrak{p} \in N_{G_\mathfrak{F}} L_\mathfrak{F}^*$. □

We shall use the following results from local class field theory..

Theorem 6.4.5 (**Hilbert-Noether**).

$$H^1(G, L^*) = 1$$

Thus from $H^1(G_{\mathfrak{F}}, L^*_{\mathfrak{F}}) = H^1(G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}, L^*_{\mathfrak{F}}) = 1, \quad \forall \mathfrak{F}$, we deduce the

Corollary 6.4.6.

$$H^1(G, I_L) = 1$$

This implies that the extensions L/K wrt I_L form a field formation. This allows us to think the groups $H^2(G_{L/K}, I_L)$ as the elements of

$$H^2(G_{\Omega/K}, I_\Omega) = \bigcup_L H^2(G_{L/K}, I_L)$$

where the inclusions are given by the injective (because $H^1(G_{L/K}, I_L) = 1$) inflation maps.

Theorem 6.4.7. *Let K be a finite algebraic number field. Then*

$$Br(K) = \bigcup_{L/K \text{ cyclic}} H^2(G_{L/K}, L^*)$$

$$H^2(G_{\Omega/K}, I_\Omega) = \bigcup_{L/K \text{ cyclic}} H^2(G_{L/K}, I_L)$$

where L/K ranges over all cyclic cyclotomic extensions.

Remark 6.4.8. *In local class field theory we have seen that the Brauer group $Br(K) = \bigcup_{L/K} H^2(G_{L/K}, L^*)$ of a $\mathfrak{p}$-adic number field K is the union of the cohomology groups $H^2(G_{L/K}, L^*)$ of the unramified extensions L/K, for which it is relatively easy to prove the reciprocity law. The role of the unramified extensions in the local theory is played in the global case by the cyclic **cyclotomic field extensions**, ie, cyclic extensions which are contained in a field which is formed by adjoining roots of unity.*

But before that we state the:

Lemma 6.4.9. *Let K be a finite algebraic number field, S a finite set of primes of K, and m a natural number. Then there exists a cyclic cyclotomic field L/K with the property that:*

- $m | [L_{\mathfrak{F}} : K_{\mathfrak{p}}]$, *for all finite* $\mathfrak{p} \in S$
- $[L_{\mathfrak{F}} : K_{\mathfrak{p}}] = 2$, *for all real-infinite* $\mathfrak{p} \in S$.

Let's now **prove** 6.4.7

Proof. we only give the proof for $H^2(G_{\Omega/K}, I_\Omega)$, the proof for $Br(K)$ is exactly the same if one replaces for the occuring fields L the idele group I_L by the multiplicative group L^*.

Let $c \in H^2(G_{\Omega/K}, I_\Omega)$ say $c \in H^2(G_{L'/K}, I_{L'})$, let m be the order of c and let S be the (finite) set of primes $\mathfrak{p}$ of K for which the local components $c_\mathfrak{p}$ of c are not equal to 1. By the previous Lemma there is a cyclic cyclotomic field L/K with $m|[L_\mathfrak{F} : K_\mathfrak{p}]$ for the finite $\mathfrak{p} \in S$ and $[L_\mathfrak{F} : K_\mathfrak{p}] = 2$ for the real infinite $\mathfrak{p} \in S$. If we form the compositum $N = L^{'} \cdot L$, then we have

$$H^2(G_{L'/K}, I_{L'}) \ \ and \ \ H^2(G_{L/K}, I_L) \subseteq H^2(G_{N/K}, I_N)$$

and we will show that c lies in the group $H^2(G_{L/K}, I_L)$. Since the sequence

$$1 \to H^2(G_{L/K}, I_L) \to H^2(G_{N/K}, I_N) \xrightarrow{res_L} H^2(G_{N/L}, I_N)$$

is exact, it suffices to show that $res_L c = 1$. But by local class field theory and our equations in 6.4.2, 6.4.3, we have $res_L c = 1 \Leftrightarrow (res_L c)_\mathfrak{F} = res_{L_\mathfrak{F}} c_\mathfrak{p} = 1$ for all primes $\mathfrak{F}$ of $L \Leftrightarrow inv_{N_{\mathfrak{F}'|L_\mathfrak{F}}}(res_{L_\mathfrak{F}} c_\mathfrak{p}) = [L_\mathfrak{F} : K_\mathfrak{p}] \cdot inv_{N_{\mathfrak{F}'|K_\mathfrak{p}}} c_\mathfrak{p} = inv_{N_{\mathfrak{F}'|K_\mathfrak{p}}} c_\mathfrak{p}^{[L_\mathfrak{F}:K_\mathfrak{p}]} = 0$ for all primes $\mathfrak{p}$ of $K \Leftrightarrow c_\mathfrak{p}^{[L_\mathfrak{F}:K_\mathfrak{p}]} = 1$ for all $\mathfrak{p} \in S$.

Now the last equality holds, because $c_\mathfrak{p}^m = 1$ and $m|[L_\mathfrak{F} : K_\mathfrak{p}]$ for the finite primes, and $[L_\mathfrak{F} : K_\mathfrak{p}] = 2$ for the real-infinite $\mathfrak{p} \in S$. □

6.5 Cohomology of the Idele Class group

The role of the multiplicative group of a field in the local theory is taken by the idele class group in the global class field theory [3]. Thus our aim is to show that there is a canonical reciprocity isomorphism between the abelianization of the Galois group $G = G_{L/K}$ of a normal extension L/K of finite algebraic number fields and the norm residue group $C_K/N_G C_L$, in other words, that the finite normal extensions L/K of an algebraic number field K constitute a class formation with respect to the idele class group C_L.

In particular we will have to prove that $H^1(G, C_L) = 1$ and that $H^2(G, C_L)$ is cyclic of order $[L : K]$.

In what follows we fix a normal extension L/K with a cyclic Galois group $G = G_{L/K}$ of prime order p. The **first fundamental inequality** is the relation $[C_K : N_G C_L] \geqslant p$.

This follows immediately from the following

Theorem 6.5.1. *The idele class group C_L is a Herbrand module with Herbrand quotient*

$$h(C_L) = \frac{|H^0(G, C_L)|}{|H^1(G, C_L)|} = p$$

From this we obtain as a

Corollary 6.5.2.

$$|H^0(G, C_L)| = [C_K : N_G C_L] = |H^2(G, C_L)| = p \cdot |H^1(G, C_L)| \geqslant p$$

[3] I have been reviewing a little class field theory, of which I finally have the impression that I understand the main results(but not the proofs of course!) - Grothendieck, letter to Serre

Let's now prove Theorem 6.5.1,

Proof. Let S be a finite set of primes of K such that

- 1) S contains all infinite primes and all primes ramified in L
- 2) $I_L = I_L^S \cdot L^*$
- 3) $I_K = I_K^S \cdot K^*$

Note that by Proposition 6.3.3 such a set S certainly exists. Then we have

$$C_L = I_L^S \cdot L^*/L^* \cong I_L^S/L^S$$

where $L^S = L^* \cap I_L^S$ is the group of S-units, ie the group of all those elements in L^* which are units for all the primes $\mathfrak{F}$ of L which do not lie above the primes in S. We then obtain

$$h(C_L) = h(I_L^S) \cdot h(L^S)^{-1}$$

in the sense that when two of these Herbrand quotients are defined, then so is the third and equality holds.

we compute the two terms..

because of 6.4.2 the computation of $h(I_L^S)$ is a local question. Let

- n the number of primes in S
- N the number of primes of L, which lie above S
- n_1 the number of primes in S, which are inert in L

Since $[L : K]$ has prime degree, a prime of K that is not inert splits completely, ie decomposes into exactly p primes of L, thus $N = n_1 + p \cdot (n - n_1)$.

To compute the quotient

$h(I_L^S) = \dfrac{|H^0(G, I_L^S)|}{|H^1(G, I_L^S)|}$, we have to determine the factors. We do this by making use of the isomorphism

$$H^q(G, I_L^S) \cong \prod_{\mathfrak{p} \in S} H^q(G_{\mathfrak{F}}, L_{\mathfrak{F}}^*)$$

If $q = 1$ the above isomorphism immediately yields $H^1(G, I_L^S) = 1$ because $H^1(G_{\mathfrak{F}}, L_{\mathfrak{F}}^*) = 1$. If $q = 0$ we have $H^0(G, I_L^S) \cong \prod_{\mathfrak{p} \in S} H^0(G_{\mathfrak{F}}, L_{\mathfrak{F}}^*)$ and use again local class field theory to determine the order $|H^0(G_{\mathfrak{F}}, L_{\mathfrak{F}}^*)|$.

In fact we have $H^0(G_{\mathfrak{F}}, L_{\mathfrak{F}}^*) = G_{\mathfrak{F}}$, so that

$$|H^0(G_{\mathfrak{F}}, L_{\mathfrak{F}}^*)| = \begin{cases} 1 & \textit{the prime } \mathfrak{p} \textit{ lying under } \mathfrak{F} \textit{ splits } (\textit{because} G_{\mathfrak{F}} = 1) \\ p & \textit{if } \mathfrak{p} \textit{ is inert } (\textit{because } G_{\mathfrak{F}} = G) \end{cases}$$

Hence $|H^0(G, I_L^S)| = p^{n_1}$, and since $H^1(G, I_L^S) = 1$ we have

$h(I_L^S) = p^{n_1}$.

For the computation $h(L^S)$ we know that the group $L^S = L^* \cap I_L^S$ of S-units of L is finitely generated of rank $N-1$ and its fixed group $(L^S)^G = K^S = K^* \cap L^S$ is the group of S-units of K and finitely generated of rank $n-1$.

We shall use without proof a Theorem from Cohomology of cyclic groups to obtain

$$h(L^S) = p^{(p(n-1)-N+1)/(p-1)} = p^{n_1-1}$$

and then $h(C_L) = p$. □

This has the following:

Corollary 6.5.3. *Let L/K be a cyclic extension of prime power degree. Then K has infinitely many primes which are inert in L.*

We now prove **the second fundamental inequality** $[C_K : N_G C_L] \leqslant p$ for cyclic extensions L/K of prime degree, making the additional assumption that K contains the p-th roots of unity. In this case L is a Kummer extension: $L = K(\sqrt[p]{x_0})$, $x_0 \in K^*$. We start with the following:

Lemma 6.5.4. *Let $N = K(\sqrt[p]{x})$, $x \in K^*$ be any Kummer extension over K and let $\mathfrak{p}$ be a finite prime of K not lying over the prime number p. Then $\mathfrak{p}$ is unramified in N if and only if $x \in U_\mathfrak{p} \cdot (K_\mathfrak{p}^*)^p$ and $\mathfrak{p}$ splits completely in N if and only if $x \in (K_\mathfrak{p}^*)^p$.*

Theorem 6.5.5. *Let L/K be a cyclic extension of prime degree p. Assume the field K contains the p-th roots of unity, Then*

$$|H^0(G, C_L)| = [C_K : N_G C_L] \leqslant p$$

The difficulty here is that we cannot a priori decide which idele classes in C_K are represented by a norm idele, and therefore lie in $N_G C_L$. This is completely different from the case of idele groups, where by the Norm Theorem for idele groups $a \in I_K$ is a norm if and only if it is a local norm everywhere. We work around this by considering instead of $N_G C_L$ an auxiliary group $\overline{F}$ which is constructed such that its elements are represented by norm idele, hence $\overline{F} \subseteq N_G C_L$, and which has the property that its index $(C_K : \overline{F})$ can actually be shown to be equal to p. Using this $\overline{F}$, we obtain the inequality

$$[C_K : N_G C_L] \leqslant [C_K : \overline{F}] = p$$

Let $L = K(\sqrt[p]{x_0})$, $x_0 \in K^*$. Let S be a finite set of primes of K such that

- 1 S contains all the primes above p and all infinite primes of K
- 2 $I_K = I_K^S \cdot K^*$
- 3 $x_0 \in K^S = I_K^S \cap K^*$ (ie, x_0 is an S-unit)

Here 2. can be satisfied by 6.3.3 and 3 because x_0 is a unit for almost all primes.

Together with S we choose m additional primes $q_1, ..q_m \notin S$ that split completely in L; set $S^* = S \cup \{q_1, .., q_m\}$. To construct $\overline{F}$ we have to specify an idele group $F \subseteq I_K$ whose elements represent the idele classes of $\overline{F}$. It must consist of nothing but norm ideles so that $\overline{F} \subseteq N_G C_L$, it must be sufficiently large to ensure that the index $[C_K : \overline{F}]$ is finite, and it must be simple enough so that it is possible to compute this index. These properties are satisfied by the idele group

$$F = \prod_{\mathfrak{p} \in S} (K_\mathfrak{p}^*)^p \times \prod_{i=1}^{m} K_{q_i}^* \times \prod_{\mathfrak{p} \notin S^*} U_\mathfrak{p}$$

To see that $F \subseteq N_G I_L$, it suffices by the Norm Theorem for ideles to convince ourselves that the components $a_\mathfrak{p}$ of each idele $a \in F$ are norms from the extension $L_\mathfrak{F}/K_\mathfrak{p}$, where $(\mathfrak{F}|\mathfrak{p})$.

This is true for $\mathfrak{p} \in S$ because $a_\mathfrak{p} \in (K_\mathfrak{p}^*)^p \subseteq N_{L_\mathfrak{F}/K_\mathfrak{p}} L_\mathfrak{F}^*$ (regardless of $[L_\mathfrak{F} : K_\mathfrak{p}] = p$ or $= 1$); this is trivially true for $\mathfrak{p} = q_i$, because q_i splits completely so that $L_\mathfrak{F} = K_\mathfrak{p}$ and it is true for $\mathfrak{p} \notin S^*$ because $x_0 \in U_\mathfrak{p}$ by 3, and therefore by 6.5.4 each $\mathfrak{p} \notin S^*$ is unramified in $L = K(\sqrt[p]{x_0})$, so that $a_\mathfrak{p} \in U_\mathfrak{p} \subseteq N_{L_\mathfrak{F}/K_\mathfrak{p}} L_\mathfrak{F}^*$. If we now set $\overline{F} = F \cdot K^*/K^*$, then $\overline{F} \subseteq N_G C_L$, since each idele class $\overline{a}$ is represented by a norm idele $a \in F$. To compute the index $[C_K : \overline{F}]$, we consider the following decomposition:

$$[C_K : \overline{F}] = [I_K^{S^*} \cdot K^*/K^* : F \cdot K^*/K^*] =$$

$$[I_K^{S^*} \cdot K^* : F \cdot K^*] = [I_K^{S^*} : F]/[(I_K^{S^*} \cap K^*) : (F \cap K^*)]$$

It allows us to split the computation of $[C_K : \overline{F}]$ into two parts, the computation of $[I_K^{S^*} : F]$ which is of a purely local nature, and the computation of $[(I_K^{S^*} \cap K^*) : (F \cap K^*)]$ which uses global considerations.

- We have $[I_K^{S^*} : F] = \prod_{\mathfrak{p} \in S} [K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^p]$; since $S \subseteq S^*$, the map

$$I_K^{S^*} \to \prod_{\mathfrak{p} \in S} K_\mathfrak{p}^*/(K_\mathfrak{p}^*)^p$$

with

$$a \mapsto \prod_{\mathfrak{p} \in S} a_\mathfrak{p} \cdot (K_\mathfrak{p}^*)^p$$

is trivially surjective, and its kernel consists precisely of those ideles $a \in I_K^{S^*}$ for which $a_\mathfrak{p} \in (K_\mathfrak{p}^*)^p$ for $\mathfrak{p} \in S$ lie in the kernel; ie the ideles in F. By the local theory we have

$$[K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^p] = p^2 \cdot |p|_\mathfrak{p}^{-1}$$

so that $[I_K^{S^*} : F] = p^{2n} \cdot \prod_{\mathfrak{p} \in S} |p|_\mathfrak{p}^{-1}$ where n is the number of primes in S. Since the primes $\mathfrak{p} \notin S$ do not lie above the prime number p, $|p|_\mathfrak{p} = 1$ for $\mathfrak{p} \notin S$, and the product formula $\prod_{\mathfrak{p} \in S} |p|_\mathfrak{p} = \prod_\mathfrak{p} |p|_\mathfrak{p} = 1$, hence $(I_K^{S^*} : F) = p^{2n}$.

- An elementary calculation shows that

$$[(I_K^{S^*} \cap K^*) : (F \cap K^*)] = [K^{S^*} : (F \cap K^*)] = [K^{S^*} : (K^{S^*})^p]/[(F \cap K^*) : (K^{S^*})^p]$$

where K^{S^*} is the group of S^*-units. We know that this group is finitely generated of rank $n+m-1$ ($n+m$ is the number of primes in S^*). Moreover K^{S^*} contains the p-th roots of unity, and it easily follows that $[K^{S^*} : (K^{S^*})^p] = p^{n+m}$.

Altogether we therefore have

$$[C_K : N_G C_L] \leqslant [C_K : \overline{F}] = p^{n-m} \cdot [(F \cap K^*) : (K^{S^*})^p]$$

and the second fundamental inequality is proved, provided that we can choose the primes $q_1, .., q_m$ splitting in L in such a way that $m = n - 1$, and

$$F \cap K^* = K^* \cap (\prod_{\mathfrak{p} \in S} (K_\mathfrak{p}^*)^p \times \prod_{i=1}^{m} K_{q_i}^* \times \prod_{\mathfrak{p} \notin S^*} U_\mathfrak{p}) =$$

$$K^* \cap \bigcap_{\mathfrak{p} \in S} (K_\mathfrak{p}^*)^p \cap \bigcap_{i=1}^{m} K_{q_i}^* \cap \bigcap_{\mathfrak{p} \notin S^*} U_\mathfrak{p} =$$

$$K^* \cap \bigcap_{\mathfrak{p} \in S} (K_\mathfrak{p}^*)^p \cap \bigcap_{\mathfrak{p} \notin S^*} U_\mathfrak{p} = (K^{S^*})^p$$

using 6.5.4, we formulate this as follows:

Sublemma 6.5.6. *There exist $n-1$ primes of K, $q_1, .., q_{n-1} \notin S$ that split completely in L and satisfy the following condition:*

If $N = K(\sqrt[p]{x})$ is a Kummer extension over K in which all $\mathfrak{p} \in S$ split completely and all $\mathfrak{p} \neq q_1, .., q_{n-1}$ are unramified, then $N = K(\sqrt[p]{x}) = K$.

In fact the desired equality

$$K^* \cap \bigcap_{\mathfrak{p} \in S} (K_\mathfrak{p}^*)^p \cap \bigcap_{\mathfrak{p} \notin S^*} U_\mathfrak{p} = (K^{S^*})^p$$

follows immediately from this. The inclusion $\supseteq$ is trivial. Let $x \in K^* \cap \bigcap_{\mathfrak{p} \in S} (K_\mathfrak{p}^*)^p \cap \bigcap_{\mathfrak{p} \notin S^*} U_\mathfrak{p}$ and $N = K(\sqrt[p]{x})$. By 6.5.4 every $\mathfrak{p} \in S$ splits completely in N, since $x \in (K_\mathfrak{p}^*)^p$. For $\mathfrak{p} \notin S^*$ we have $x \in U_\mathfrak{p} \subseteq U_\mathfrak{p} \cdot (K_\mathfrak{p}^*)^p$, so that every $\mathfrak{p} \notin S^*$ is unramified in N by 6.5.4. Hence the Sublemma yields $N = K(\sqrt[p]{x}) = K$ so that $x \in (K^*)^p$ and because $x \in U_\mathfrak{p}$ for $\mathfrak{p} \notin S^*$, x lies in $(K^*)^p \cap K^{S^*} = (K^{S^*})^p$.

and we have proven Theorem (6.5.5). From the previous Theorems we have the following

Corollary 6.5.7. *Let L/K be a cyclic extension of prime degree p, with Galois group $G = G_{L/K}$ and assume the field K contains the p-th roots of unity, then*

$$H^0(G, C_L) \cong H^2(G, C_L) \cong G$$

and

$$H^1(G, C_L) = 1$$

We prove now the following more general result:

Theorem 6.5.8. *If L/K is a normal extension with Galois group $G = G_{L/K}$, then we have $H^1(G, C_L) = 1$.*

Proof. We prove this by induction on the order n of the group G. The case $n = 1$ is trivial. Let us assume that $H^1(G, C_L) = 1$ for every extension L/K of degree $< n$. If the order $n = |G|$ is not a p-power, then each p-Sylow subgroup $G_\mathfrak{p}$ of G has order smaller than n, so that by the induction hypothesis $H^1(G_\mathfrak{p}, C_L) = 1$ and therefore $H^1(G, C_L) = 1$.

Thus it suffices to prove this for a p-group G. In this case, let $g \subseteq G$ be a normal subgroup of index p; g is the Galois group of an intermediate field M, $K \subseteq M \subseteq L$, $g = G_{L/M}$. Now if $p < n$, then by assumption $H^1(G/g, C_M) = H^1(g, C_L) = 1$ and from the exact sequence

$$1 \to H^1(G/g, C_M) \xrightarrow{inf} H^1(G, C_L) \xrightarrow{res} H^1(g, C_L)$$

we see that $H^1(G, C_L) = 1$.

$$\begin{array}{ccc} L & \text{——} & L' \\ | & & | \\ K & \text{——} & K' \end{array}$$

Assume $p = n$. In order to be able to apply 6.5.7, we replace K by the extension K' obtained by adjoining a primitive p-th root of unity to K, and set $L' = L \cdot K'$. Obviously $[K' : K] \leqslant p - 1 < p = n$ and $[L' : K'] = p$. Because $[K' : K] < n$, we have $H^1(G_{K'/K}, C_{K'}) = H^1(G_{L'/K'}, C_{L'}) = 1$, and from the exact sequence

$$1 \to H^1(G_{K'/K}, C_{K'}) \xrightarrow{inf} H^1(G_{L'/K}, C_{L'}) \xrightarrow{res} H^1(G_{L'/K'}, C_{L'})$$

we obtain $H^1(G_{L'/K}, C_{L'}) = 1$. On the other hand, because the sequence

$$1 \to H^1(G, C_L) \xrightarrow{inf} H^1(G_{L'/K}, C_{L'}) = 1$$

is also exact, we see that $H^1(G_{L'/K}, C_{L'}) = 1$ implies $H^1(G, C_L) = 1$. □

For cyclic extensions Theorem 6.5.8 is just another form of the **Hasse Norm Theorem** mentioned earlier:

Corollary 6.5.9. *If the extension L/K is cyclic, then an element $x \in K^*$ is a norm if and only if it is locally a norm everywhere.*

Proof. The sequence of G-modules $1 \to L^* \to I_L \to C_L \to 1$ yields the exact cohomology sequence

$$H^{-1}(G, C_L) \to H^0(G, L^*) \to H^0(G, I_L) \cong \bigoplus_{\mathfrak{p}} H^0(G_\mathfrak{F}, L^*_\mathfrak{F})$$

Since G is cyclic, $H^{-1}(G, C_L) \cong H^1(G, C_L) = 1$, by Theorem 6.5.8, which implies that the canonical homomorphism

$$K^*/N_{L/K}L^* \to \bigoplus_{\mathfrak{p}} K_{\mathfrak{p}}^*/N_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}L_{\mathfrak{F}}^*$$

is injective; this is precisely the assertion of the Hasse Norm Theorem. □

Theorem 6.5.10. *Let L/K be a normal extension with Galois group $G = G_{L/K}$. Then the order of $H^2(G, C_L)$ is a divisor of the degree $[L : K]$.*

With Theorem 6.5.10 we have not yet reached our goal to show that $H^2(G, C_L)$ is cyclic of the same order as $[L : K]$. To show this, we will associate with the group $H^2(G, C_L)$ an invariant homomorphism, as required by the second Axiom of class formations.

6.6 Idele invariants

Our goal is to show that the extensions L/K form a class formation, so what remains to be shown is that for every normal extension L/K there is an invariant isomorphism

$$H^2(G_{L/K}, C_L) \to \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}$$

which satisfies the compatibility properties that we referred. It is of course essential that we construct the invariant isomorphism in a canonical way to also obtain a canonical law, the **Artin reciprocity law**. In a certain sense we will retrieve the invariant map, and with it the reciprocity law from the local theory, by relating the group $H^2(G_{L/K}, C_L)$ to the group $H^2(G_{L/K}, I_L)$ formed with the idele group I_L as the underlying module.

Let L/K be a normal extension of finite algebraic number fields, and let $G_{L/K}$ be its Galois group. We have already the decomposition

$$H^2(G_{L/K}, I_L) \cong \bigoplus_{\mathfrak{p}} H^2(G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}, L_{\mathfrak{F}}^*)$$

For every prime $\mathfrak{p}$ of K we have from local class field theory the isomorphism

$$inv_{L_{\mathfrak{F}}/K_{\mathfrak{p}}} : H^2(G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}, L_{\mathfrak{F}}^*) \to \frac{1}{[L_{\mathfrak{F}} : K_{\mathfrak{p}}]}\mathbb{Z}/\mathbb{Z} \subseteq \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}$$

where $(\mathfrak{F}|\mathfrak{p})$

The local invariant isomorphism $inv_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}$ is the composition of three homomorphisms, however we do not need to know this map explicitly, but it is important that it satisfies the compatibility conditions of the second axion of a class formation.

Definition 6.6.1. *If $c_{\mathfrak{p}} \in H^2(G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}, L_{\mathfrak{F}}^*)$, where $(\mathfrak{F}|\mathfrak{p})$ are the local components of $c \in H^2(G_{L/K}, I_L)$, then we set*

$$inv_{L/K}c = \sum_{\mathfrak{p}} inv_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}c_{\mathfrak{p}} \in \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}$$

Note: almost all $c_{\mathfrak{p}} = 1$, so that the sum contains only finitely many non-zero summands. In particular we obtain an invariant homomorphism

$$inv_{L/K} : H^2(G_{L/K}, I_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

Proposition 6.6.2. *If $K \subseteq L \subseteq N$ are normal extensions of the field K, then*

$inv_{N/K}c = inv_{L/K}c$ *for* $c \in H^2(G_{L/K}, I_L) \subseteq H^2(G_{N/K}, I_N)$

$inv_{N/L}(res_L c) = [L:K] \cdot inv_{N/K}c$ *for* $H^2(G_{N/K}, I_N)$

$inv_{N/K}(cor_K c) = inv_{N/L}c$ *for* $H^2(G_{N/L}, I_N)$

The last two formulas require only that N/K be normal.

Here we use the convention to interpret the inflation map

$$H^2(G_{L/K}, I_L) \to H^2(G_{N/K}, I_N)$$

as an inclusion, so that $H^2(G_{L/K}, I_L) \subseteq H^2(G_{N/K}, I_N)$.

Proof. Let $c \in H^2(G_{L/K}, I_L)$, then

$$inv_{N/K}c = \sum_{\mathfrak{p}} inv_{N_{\mathfrak{F}'}/K_{\mathfrak{p}}} c_{\mathfrak{p}} = \sum_{\mathfrak{p}} inv_{L_{\mathfrak{F}}/K_{\mathfrak{p}}} c_{\mathfrak{p}} = inv_{L/K}c$$

where $\mathfrak{F}'$ is an arbitrary prime of N over $\mathfrak{p}$ and $\mathfrak{F}$ is the prime of L lying under $\mathfrak{F}'$.

If $c \in H^2(G_{N/K}, I_N)$ and $\mathfrak{F}$ runs through the primes of L, then

$inv_{N/L}(res_L c) = \sum_{\mathfrak{F}} inv_{N_{\mathfrak{F}'}/L_{\mathfrak{F}}}(res_L c)_{\mathfrak{F}} = \sum_{\mathfrak{F}} inv_{N_{\mathfrak{F}'}/L_{\mathfrak{F}}}(res_{L_{\mathfrak{F}}} c_{\mathfrak{p}}) =$

$\sum_{\mathfrak{F}}[L_{\mathfrak{F}} : K_{\mathfrak{p}}] \cdot inv_{N_{\mathfrak{F}'}/K_{\mathfrak{p}}} c_{\mathfrak{p}} = \sum_{\mathfrak{p}} \sum_{\mathfrak{F}|\mathfrak{p}} [L_{\mathfrak{F}} : K_{\mathfrak{p}}] \cdot inv_{N_{\mathfrak{F}'}/K_{\mathfrak{p}}} c_{\mathfrak{p}}$

where $\mathfrak{F}'$ is an arbitrary prime of N over $\mathfrak{F}$ and $\mathfrak{p}$ is the prime of K lying under $\mathfrak{F}$.

By the fundamental equation of number theory

$$\sum_{\mathfrak{F}|\mathfrak{p}} [L_{\mathfrak{F}} : K_{\mathfrak{p}}] = [L:K]$$

then ($\mathfrak{F}'$ a fixed prime of N over $\mathfrak{p}$):

$inv_{N/L}(res_L c) = \sum_{\mathfrak{p}} (\sum_{\mathfrak{F}|\mathfrak{p}} [L_{\mathfrak{F}} : K_{\mathfrak{p}}]) \cdot inv_{N_{\mathfrak{F}'}/K_{\mathfrak{p}}} c_{\mathfrak{p}} =$

$[L:K] \cdot \sum_{\mathfrak{p}} inv_{N_{\mathfrak{F}'}/K_{\mathfrak{p}}} c_{\mathfrak{p}} = [L:K] \cdot inv_{N/K}c$

Finally, for $c \in H^2(G_{N/L}, I_N)$ it follows that

$$inv_{N/K}(cor_K c) = \sum_{\mathfrak{p}} inv_{N_{\mathfrak{F}'/K_{\mathfrak{p}}}}(cor_K c)_{\mathfrak{p}} =$$

$$\sum_{\mathfrak{p}} \sum_{\mathfrak{F}|\mathfrak{p}} inv_{N_{\mathfrak{F}'/K_{\mathfrak{p}}}}(cor_{K_{\mathfrak{p}}} c_{\mathfrak{F}}) = \sum_{\mathfrak{p}} \sum_{\mathfrak{F}|\mathfrak{p}} inv_{N_{\mathfrak{F}'/L_{\mathfrak{F}}} c_{\mathfrak{F}}} = inv_{N/L} c$$

□

Since $H^1(G_{L/K}, I_K) = 1$, it follows that the extensions L/K satisfy with respect to the idele group I_L and the idele homomorphism $inv_{L/K}$ the conditions for a class formation, except for that the homomorphism

$$inv_{L/K} : H^2(G_{L/K}, I_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

is not an isomorphism. To make this so, we have to pass from the idele group I_L to the idele class group C_L. We now introduce the following symbol:

Definition 6.6.3. *Let L/K be an abelian extension. If $a \in I_K$ with local components $a_{\mathfrak{p}} \in K_{\mathfrak{p}}^*$, then we set*

$$(a, L/K) = \prod_{\mathfrak{p}} (a_{\mathfrak{p}}, L_{\mathfrak{F}}/K_{\mathfrak{p}}) \in G_{L/K}$$

For each prime $\mathfrak{p}$, the symbol $(a_{\mathfrak{p}}, L_{\mathfrak{F}}/K_{\mathfrak{p}})$ defines an element of the local abelian Galois group $G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}$ which we always consider as a subgroup of $G_{L/K}$, hence

$$(a_{\mathfrak{p}}, L_{\mathfrak{F}}/K_{\mathfrak{p}}) \in G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}} \subseteq G_{L/K}$$

Since $a_{\mathfrak{p}}$ is a unit for almost all primes $\mathfrak{p}$ and since $L_{\mathfrak{F}}/K_{\mathfrak{p}}$ is unramified for almost all $\mathfrak{p}$ we have $(a_{\mathfrak{p}}, L_{\mathfrak{F}}/K_{\mathfrak{p}}) = 1$ for almost all $\mathfrak{p}$, thus the last product is well defined and is independent of the order of factors since $G_{L/K}$ is abelian. The symbol $(\quad, L/K)$ and the invariant mapping are related as follows,

Lemma 6.6.4. *Let L/K be an abelian extension, $a \in I_K$ and $(a) = a \cdot N_{L/K} I_L \in H^0(G_{L/K}, I_L)$. If $\chi \in \chi(G_{L/K}) = H^1(G_{L/K}, Q/Z)$ then*

$$\chi(a, L/K) = inv_{L/K}((a) \cup \delta\chi) \in \frac{1}{[L:K]} Z/Z$$

If we denote by $\chi_{\mathfrak{p}}$ the restriction of χ to $G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}$ and by $(a_{\mathfrak{p}}) = a_{\mathfrak{p}} \cdot N_{L_{\mathfrak{F}}/K_{\mathfrak{p}}} L_{\mathfrak{F}}^*$ then

$$\chi(a, L/K) = \sum_{\mathfrak{p}} \chi_{\mathfrak{p}}(a_{\mathfrak{p}}, L_{\mathfrak{F}}/K_{\mathfrak{p}}) = \sum_{\mathfrak{p}} inv_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}((a)_{\mathfrak{p}} \cup \delta\chi_{\mathfrak{p}})$$

where it can be shown that the classes $((a_{\mathfrak{p}}) \cup \delta\chi_{\mathfrak{p}}) \in H^2(G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}, L_{\mathfrak{F}}^*)$ are the local components of $(a) \cup \delta\chi \in H^2(G_{L/K}, I_L)$
we only need to note that $a_{\mathfrak{p}} \cdot \delta\chi_{\mathfrak{p}}(\sigma, \tau)$ (respectively $a \cdot \delta\chi(\sigma, \tau)$) is a 2-cocycle of the class $((a_{\mathfrak{p}}) \cup \delta\chi_{\mathfrak{p}})$ (resp. $((a) \cup \delta\chi)$). Thus $\chi(a, L/K) = inv_{L/K}((a) \cup \delta\chi)$ as claimed.

When changing from the idele invariants to the idele class invariants, the following theorem is of central importance. From the exact cohomology sequence associated with the exact sequence

$$1 \to L^* \to I_L \to C_L \to 1$$

we see using that $H^1(G_{L/K}, C_L) = 1$ that the induced homomorphism

$$H^2(G_{L/K}, L^*) \to H^2(G_{L/K}, I_L)$$

is injective.

We use this injection to think $H^2(G_{L/K}, L^*)$ as a subgroup of $H^2(G_{L/K}, I_L)$

ie we view the elements o $H^2(G_{L/K}, L^*)$ as the idele cohomology classes that are represented by cocycles with values in the principal idele group L^*.

Theorem 6.6.5. *If $c \in H^2(G_{L/K}, L^*)$, then $inv_{L/K}c = 0$*

Proof. We start with the simple observation that it suffices to consider the case when $K = \mathbb{Q}$ and L is a cyclic cyclotomic extension of $\mathbb{Q}$. In fact, if $c \in H^2(G_{L/K}, L^*)$ and N is a normal extension of $\mathbb{Q}$ containing L, then

$$c \in H^2(G_{L/K}, L^*) \subseteq H^2(G_{N/K}, N^*) \subseteq H^2(G_{N/K}, I_N)$$

$cor_{\mathbb{Q}}c \in H^2(G_{N/\mathbb{Q}}, N^*)$ and $inv_{L/K}c = inv_{N/K}c = inv_{N/\mathbb{Q}}(cor_{\mathbb{Q}}c)$
by 6.6.2. Hence to show $inv_{L/K}c = 0$ it suffices to consider the case $K = \mathbb{Q}$. Since by 6.4.7 there exists a cyclic cyclotomic extension $L_0/\mathbb{Q}$ with $c \in H^2(G_{L_0/\mathbb{Q}}, L_0^*)$, we can even assume that $L/\mathbb{Q}$ itself is a cyclic cyclotomis extension.

Let χ be a generator of the cyclic character group $\chi(G_{L/\mathbb{Q}}) = H^1(G_{L/\mathbb{Q}}, \mathbb{Q}/\mathbb{Z})$. Then $\delta\chi$ is a generator of $H^2(G_{L/\mathbb{Q}}, \mathbb{Z})$ and Tate's Theorem implies

$$\delta\chi \cup : H^0(G_{L/\mathbb{Q}}, L^*) \to H^2(G_{L/\mathbb{Q}}, L^*)$$

is bijective. Thus each element $c \in H^2(G_{L/\mathbb{Q}}, L^*)$ has the form $c = (a) \cup \delta\chi$ with $(a) = a \cdot N_{L/\mathbb{Q}}L^* \in H^0(G_{L/\mathbb{Q}}, L^*)$ with $a \in \mathbb{Q}^*$. From 6.6.4 we obtain

$$inv_{L/Q}c = inv_{L/\mathbb{Q}}((a) \cup \delta\chi) = \chi(a, L/Q)$$

and we need to show that $(a, L/\mathbb{Q}) = \prod_{\mathfrak{p}}(a, L_{\mathfrak{F}}/\mathbb{Q}_{\mathfrak{p}}) = 1$.

Now L is a cyclotomic extension, ie $L \subseteq \mathbb{Q}(\zeta)$ for some root of unity ζ. The automorphism $(a, L/\mathbb{Q})$ is precisely the restriction of $(a, \mathbb{Q}(\zeta)/\mathbb{Q})$ to L; this follows easily from the behavior of the local norm residue symbol $(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ when passing to the extension $L_{\mathfrak{F}}/\mathbb{Q}_p$. It therefore suffices to show that $(a, \mathbb{Q}(\zeta)/\mathbb{Q}) = 1$ for $a \in \mathbb{Q}^*$. Now $\mathbb{Q}(\zeta)$ is generated by roots of unity of prime power order and it suffices to show the vanishing of $(a, \mathbb{Q}(\zeta)/\mathbb{Q})$ for these generators, hence we may assume that ζ is a primitive l^n-th root of unity (l is a prime number). With this reduction we come to the actual core of the proof.

Let ζ be a primitive l^n-th root of unity; if $l = 2$, we assume $n \geqslant 2$. If p ranges over the prime numbers and the infinite prime over $p = p_\infty$ of $\mathbb{Q}$, then the $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ are the local extensions associated with $\mathbb{Q}(\zeta)/\mathbb{Q}$. The extension $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ is unramified for $p \neq l$ and totally ramified for $p = l$; if $p = p_\infty$ then $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$ means the extension $\mathbb{C}/\mathbb{R}$. We have to show that

for each $a \in \mathbb{Q}^*$, $(a, \mathbb{Q}(\zeta)/\mathbb{Q}) = \prod_p (a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p) = 1$

Here it obviously suffices to assume that a is integral. We consider the effect of the local norm residue symbol $(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)$ on the l^n-th roots of unity ζ.

• 1 For $p \neq l$, $p \neq p_\infty$, we have

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\zeta = \varphi^{v_p(a)}\zeta$$

where v_p is the valuation on $\mathbb{Q}_p$ and φ is the Frobenius automorphism on $\mathbb{Q}_p(\zeta)/\mathbb{Q}_p$. Since the residue field of $\mathbb{Q}_p$ has p elements, clearly $\varphi\zeta = \zeta^p$, thus

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\zeta = \zeta^{p^{v_p(a)}}$$

• 2 For $p = l$, we obtain, writing $a = u \cdot p^m = u \cdot p^{v_p(a)}$, u a unit:

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\zeta = \zeta^r$$

where r is a natural number which is determined $mod\ p^n$ by the congruence $r \equiv u^{-1} \equiv a^{-1} \cdot p^{v_p(a)} mod\ p^n$.

• 3 For $p = p_\infty$ the automorphism $(a, \mathbb{C}/\mathbb{R})$ is either the identity or complex conjugation, depending on whether $a > 0$ or $a < 0$. Thus

$$(a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\zeta = \zeta^{sgna}$$

Combining these we obtain

$$(a, \mathbb{Q}(\zeta)/\mathbb{Q})\zeta = \prod_p (a, \mathbb{Q}_p(\zeta)/\mathbb{Q}_p)\zeta = \zeta^{sgna \cdot \prod_{p \neq l} p^{v_p(a)} \cdot r}$$

but by the product formula

$$sgna \cdot \prod_{p \neq l} p^{v_p(a)} \cdot r \equiv sgna \cdot \prod_{p \neq l} p^{v_p(a)} l^{v_l(a)} \cdot a^{-1} = \frac{1}{\prod_p |a|_p} = 1 mod\ l^n$$

therefore $(a, \mathbb{Q}(\zeta)/\mathbb{Q})\zeta = \zeta$, ie we have $(a, \mathbb{Q}(\zeta)/\mathbb{Q}) = 1$. □

The last Theorem shows that the group $H^2(G_{L/K}, L^*)$ lies in the kernel of the homomorphism $inv_{L/K} : H^2(G_{L/K}, I_L) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$. We have to ask further whether or not it is precisely the kernel, and in addition whether or not $inv_{L/K}$ is a surjective homomorphism. For the cyclic case we have:

Proposition 6.6.6. *If L/K is a cyclic extension, then the sequence*

$$1 \to H^2(G_{L/K}, L^*) \to H^2(G_{L/K}, I_L) \xrightarrow{inv_{L/K}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \to 0$$

is exact.

Proof. • To show that $inv_{L/K}$ is surjective, we assume first $[L : K]$ is a prime power p^r. Because $\frac{1}{[L:K]} + \mathbb{Z}$ generates $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, it suffices to find an element $c \in H^2(G_{L/K}, I_L)$ with $inv_{L/K}c = \frac{1}{[L:K]} + \mathbb{Z}$. We use the decomposition

$$H^2(G_{L/K}, I_L) \cong \bigoplus_{\mathfrak{p}} H^2(G_{L_\mathfrak{F}/K_\mathfrak{p}}, L_\mathfrak{F}^*)$$

and determine c by its local components $c_{\mathfrak{p}} \in H^2(G_{L_{\mathfrak{F}}/K_{\mathfrak{p}}}, L_{\mathfrak{F}}^*)$. Since L/K is cyclic of prime power degree, it follows from 6.5.3 that K contains a prime $\mathfrak{p}_0$ which is inert in L. Since $\mathfrak{p}_0$ is inert , we have $[L_{\mathfrak{F}_0} : K_{\mathfrak{p}_0}] = [L : K]$ where $\mathfrak{F}_0|\mathfrak{p}_0$ and local class field theory yields an element $c_{\mathfrak{p}_0} \in H^2(G_{L_{\mathfrak{F}_0}/K_{\mathfrak{p}_0}}, L_{\mathfrak{F}_0}^*)$ with $inv_{L_{\mathfrak{F}_0}/K_{\mathfrak{p}_0}} = \dfrac{1}{[L_{\mathfrak{F}_0} : K_{\mathfrak{p}_0}]} + \mathbb{Z} = \dfrac{1}{[L : K]} + \mathbb{Z}$. Now if c is the element in $H^2(G_{L/K}, I_L)$ that is determined by the local components

$$..., 1, 1, 1, c_{\mathfrak{p}_0}, 1, 1, 1, ...$$

then

$$inv_{L/K} c = \sum_{\mathfrak{p}} inv_{L_{\mathfrak{F}}/K_{\mathfrak{p}}} c_{\mathfrak{p}} = inv_{L_{\mathfrak{F}_0}/K_{\mathfrak{p}_0}} c_{\mathfrak{p}_0} = \frac{1}{[L : K]} + \mathbb{Z}$$

That $inv_{L/K}$ is also surjective in the general case $[L : K] = n = p_1^{r_1} \cdots p_s^{r_s}$ follows easily from this. For every $i = 1, ..., s$ there obviously exists a cyclic intermediate field L_i of degree $[L_i : K] = p_i^{r_i}$. Consider the decomposition

$$\frac{1}{n} = \frac{n_1}{p_1^{r_1}} + \cdots \frac{n_s}{p_s^{r_s}}$$

into partial fraction. By the previous case there is a $c_i \in H^2(G_{L_i/K}, I_{L_i})$ with

$$inv_{L_i/K} c_i = inv_{L/K} c_i = \frac{n_i}{p_i^{r_i}} + \mathbb{Z}$$

Thus if we set

$$c = c_1 \cdots c_s \in H^2(G_{L/K}, I_L)$$

then

$$inv_{L/K} c = \sum_{i=1}^{s} inv_{L/K} c_i = \sum_{i=1}^{s} \frac{n_i}{p_i^{r_i}} + Z = \frac{1}{n} + \mathbb{Z}$$

which shows that $inv_{L/K}$ is surjective for any cyclic extension.

• We know now that $H^2(G_{L/K}, L^*)$ lies in the kernel of the homomorphism $inv_{L/K}$. To show that the group $H^2(G_{L/K}, L^*)$ in fact equals the kernel of $inv_{L/K}$ we use a simple argument involving the orders of these groups. Since the map $inv_{L/K}$ is surjective, we only need to show that the order of the factor group

$$H^2(G_{L/K}, I_L)/H^2(G_{L/K}, L^*)$$

is at most the order of $\dfrac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}$ ie the degree of $[L : K]$. Using the sequence

$$1 \to L^* \to I_L \to C_L \to 1$$

we obtain, using that $H^1(G_{L/K}, C_L) = 1$ the exact cohomology sequence

$$1 \to H^2(G_{L/K}, L^*) \to H^2(G_{L/K}, I_L) \to H^2(G_{L/K}, C_L)$$

Therefore the order of $H^2(G_{L/K}, I_L)/H^2(G_{L/K}, L^*)$ divides the order of $H^2(G_{L/K}, C_L)$. By 6.5.10 $H^2(G_{L/K}, C_L)$ divides $[L : K]$ and we are done. □

For the following it would be very convenient if we could show that $inv_{L/K}$ is a surjective homomorphism in general. Unfortunately this is not the case. In order for every element of $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ to be in the image of the invariant map, we have to enlarge the field L by forming the compositum with a cyclic extension. For technical reasons it is best to let L range over all normal extensions of K and to consider the union

$$H^2(G_{\Omega/K}, I_\Omega) = \bigcup_L H^2(G_{L/K}, I_L)$$

If $K \subseteq L \subseteq N$ are two normal extensions of K, then

$$H^2(G_{L/K}, I_L) \subseteq H^2(G_{N/K}, I_N)$$

and since by 6.6.2 the invariant map can be extended from $H^2(G_{L/K}, I_L)$ to $H^2(G_{N/K}, I_N)$, we obtain a homomorphism

$$inv_K : H^2(G_{\Omega/K}, I_\Omega) \to \mathbb{Q}/\mathbb{Z}$$

whose restriction to $H^2(G_{L/K}, I_L) \subseteq H^2(G_{\Omega/K}, I_\Omega)$ coincides with the initial invariant map $inv_{L/K}$. If we take into account that for each positive integer m there is a cyclic extension L/K with $m|[L:K]$, we see that $\mathbb{Q}/\mathbb{Z}$ is already covered by the groups $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ coming from cyclic extension L/K. Now the map $inv_{L/K}$ is surjective in the cyclic case, thus we obtain for the invariant map inv_K defined above the following

Theorem 6.6.7. *The homomorphism*

$$inv_K : H^2(G_{\Omega/K}, I_\Omega) \to \mathbb{Q}/\mathbb{Z}$$

is surjective.

6.7 The reciprocity law

Having studied the idele invariants in the previous section, we now want to construct invariants for the elements of the groups $H^2(G_{L/K}, C_L)$. We start with the following observations:

If L/K is a normal extension, then we obtain from the exact sequence

$$1 \to L^* \to I_L \to C_L \to 1$$

using $H^1(G_{L/K}, C_L) = 1 = H^3(G_{L/K}, I_L) = 1$, the exact cohomology sequence

$$1 \to H^2(G_{L/K}, L^*) \to H^2(G_{L/K}, I_L) \xrightarrow{j} H^2(G_{L/K}, C_L)$$

$$\xrightarrow{\delta} H^3(G_{L/K}, L^*) \to 1$$

If $\overline{c} \in H^2(G_{L/K}, C_L)$ and $c \in H^2(G_{L/K}, I_L)$ is such that $\overline{c} = jc$, then we set

$$inv_{L/K}\overline{c} = inv_{L/K}c \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

This definition is independent of the choice of the preimage $c \in H^2(G_{L/K}, I_L)$, because two such preimages differ only by an element in $H^2(G_{L/K}, L^*)$, which we have seen has invariant 0. Of course this only works if the element $\overline{c} \in H^2(G_{L/K}, C_L)$ lies in the image of the homomorphism j. In this case, ie j being surjective would be equivalent to the group $H^3(G_{L/K}, L^*) = 1$ ie being trivial. This is not true in general, but still applies to the cyclic case.

Proposition 6.7.1. *If L/K is a cyclic extension, then the homomorphism*

$$H^2(G_{L/K}, I_L) \xrightarrow{j} H^2(G_{L/K}, C_L)$$

is surjective.

Proof. If L/K is cyclic, then $H^3(G_{L/K}, L^*) \cong H^1(G_{L/K}, L^*) = 1$ □

In order to define an invariant map for arbitrary normal extensions L/K, we proceed in a similar way as we did at the end of the previous section.

Let's note that the homomorphism

$$H^2(G_{L/K}, I_L) \xrightarrow{j} H^2(G_{L/K}, C_L)$$

commutes with the maps inf and res; ie if $K \subseteq L \subseteq N$ are two normal extensions of K, then we have

$$j \circ inf_N = inf_N \circ j$$
$$j \circ res_L = res_L \circ j$$

where in the last formula we only need to assume that N/K is normal. We can define for simplicity

Definition 6.7.2.

$$H^q(L/K) = H^q(G_{L/K}, C_L)$$

Because $H^1(L/K) = 1$, the extensions L/K form a field formation in the sense that we have already mentioned, with respect to the idele group C_L as the module. To simplify things we will as before and in general for every field formation, interpret the injective inflation maps

$$H^2(L/K) \xrightarrow{inf} H^2(N/K)$$

$K \subseteq L \subseteq N$

as inclusions. More precisely, this means that we form the direct limit

$$H^2(\Omega/K) = \varinjlim_L H^2(L/K)$$

where L ranges over all finite normal extensions of K. We view the groups $H^2(L/K)$ as being embedded in $H^2(\Omega/K)$ via the inflation maps. Thinking of the $H^2(L/K)$ as subgroups of $H^2(\Omega/K)$ we have

$$H^2(\Omega/K) = \bigcup_L H^2(L/K)$$

Hence if $K \subseteq L \subseteq N$ are two normal extensions. then we have inclusions

$$H^2(L/K) \subseteq H^2(N/K) \subseteq H^2(\Omega/K)$$

Ω denotes again the field of all algebraic numbers.

we give now the following crucial theorem

Theorem 6.7.3. *If L/K is a normal extension and $L^{'}/K$ a cyclic extension of equal degree $[L^{'} : K] = [L : K]$, then*

$$H^2(L^{'}/K) = H^2(L/K) \subseteq H^2(\Omega/K)$$

Since for every positive integer m there is a cyclic extension L/K of degree m, this theorem has the following

Corollary 6.7.4.

$$H^2(\Omega/K) = \bigcup_{L/K\ cyclic} H^2(L/K)$$

Proof. of 6.7.3

We first show that $H^2(L^{'}/K) \subseteq H^2(L/K)$. If $N = L \cdot L^{'}$ is the compositum of L and $L^{'}$, then a simple group theoretic argument shows that if the extension $L^{'}/K$ is cyclic, then the extension N/L is also cyclic. Now let $\overline{c} \in H^2(L^{'}/K) \subseteq H^2(N/K)$. Because of the exact sequence

$$1 \to H^2(L/K) \to H^2(N/K) \xrightarrow{res_L} H^2(N/L)$$

an element $\overline{c} \in H^2(N/K)$ is an element of $H^2(L/K)$ if and only if $res_L\overline{c} = 1$. To show this, we use the idele invariants. By 6.7.1 the homomorphism

$$H^2(G_{L^{'}/K}, I_{L^{'}}) \xrightarrow{j} H^2(L^{'}/K)$$

is surjective, so that $\overline{c} = jc$, and $c \in H^2(G_{L^{'}/K}, I_{L^{'}}) \subseteq H^2(G_{N/K}, I_N)$. From the remarks made above, we know that the map j commutes with inflation (interpreted here as inclusion) and with restriction, hence we have the formulas

$$res_L\overline{c} = res_L(jc) = jres_Lc$$

Thus $res_L\overline{c} = 1$ if and only if res_Lc lies in the kernel of j and therefore in $H^2(G_{N/L}, N^*)$. Since N/L is cyclic, this holds by 6.6.6 if and only if $inv_{N/L}(res_Lc) = 0$ and this holds indeed since

$$inv_{N/L}(res_Lc) = [L : K] \cdot inv_{N/K}c = [L^{'} : K] \cdot inv_{L^{'}/K}c = 0$$

Therefore $H^2(L^{'}/K) \subseteq H^2(L/K)$.

To show that the above inequality is in fact an equality we consider orders. Because $H^1(L^{'}/K) = 1$ and $H^3(G_{L^{'}/K}, L^{'*}) \cong H^1(G_{L^{'}/K}, L^{'*}) = 1$ we obtain the exact cohomology sequence

$$1 \to H^2(G_{L^{'}/K}, L^{'*}) \to H^2(G_{L^{'}/K}, I_{L^{'}}) \to H^2(L^{'}/K) \to 1$$

where $|H^2(L^{'}/K)| = [L^{'} : K] = [L : K]$. On the other hand $|H^2(L/K)|$ divides the degree $[L : K]$, hence $H^2(L^{'}/K) = H^2(L/K)$. □

Let $K \subseteq L \subseteq N$ be two normal extensions. Because the map

$$H^2(G_{L/K}, I_L) \xrightarrow{j} H^2(L/K)$$

is compatible with inflation, it can be extended to a canonical homomorphism

$$H^2(G_{N/K}, I_N) \xrightarrow{j} H^2(N/K)$$

Thus we obtain a homomorphism

$$H^2(G_{\Omega/K}, I_\Omega) \xrightarrow{j} H^2(\Omega/K)$$

whose restriction to the groups $H^2(G_{L/K}, I_L)$ are the initial homomorphisms $H^2(G_{L/K}, I_L) \to H^2(L/K)$. If these are not surjective, then we still have

Theorem 6.7.5. *The homomorphism*

$$H^2(G_{\Omega/K}, I_\Omega) \xrightarrow{j} H^2(\Omega/K)$$

is surjective.

Proof. If $\overline{c} \in H^2(\Omega/K)$, then it follows from the previous theorem that there is a cyclic extension L/K such that $\overline{c} \in H^2(L/K)$. Since for a cyclic extension the map

$$H^2(G_{L/K}, I_L) \xrightarrow{j} H^2(L/K)$$

is surjective, $\overline{c} = jc$ for some $c \in H^2(G_{L/K}, I_L) \subseteq H^2(G_{\Omega/K}, I_\Omega)$. □

Given this theorem, it is easy to obtain class invariants for the elements of $H^2(\Omega/K) = \bigcup_L H^2(L/K)$ from the invariant map of the idele cohomology classes. From the homomorphism

$$inv_K : H^2(G_{\Omega/K}, I_\Omega) \to \mathbb{Q}/\mathbb{Z}$$

which is surjective as we have seen in the previous section, we in fact come to the following

Definition 6.7.6. *If $\overline{c} \in H^2(\Omega/K)$ and $\overline{c} = jc$, $c \in H^2(G_{\Omega/K}, I_\Omega)$, then we define*

$$inv_K \overline{c} = inv_K c \in \mathbb{Q}/\mathbb{Z}$$

Of course we have to convince ourselves that this definition is independent of the choice of the choice of the preimage $c \in H^2(G_{\Omega/K}, I_\Omega)$. Let's say that there is another element $c' \in H^2(G_{\Omega/K}, I_\Omega)$ with $\overline{c} = jc'$. then $c, c' \in H^2(G_{L/K}, I_L) \subseteq H^2(G_{\Omega/K}, I_\Omega)$ for a sufficiently large normal extension L/K, where we may assume that this extension is so large that $\overline{c} \in H^2(L/K)$, Because $\overline{c} = jc = jc'$, then of course c and c' differ only by an element in the kernel of the mapping $j : H^2(G_{L/K}, I_L) \to H^2(L/K)$ and thus by an element of $H^2(G_{L/K}, L^*)$ as we can see by definition and this has invariant 0. We proved it in the last section..

From the last definition we obtain a homomorphism

$$inv_K : H^2(\Omega/K) \to \mathbb{Q}/\mathbb{Z}$$

the restriction of inv_K to the group $H^2(L/K)$ coming from a finite normal extension L/K yields a homomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

because the orders of the elements in $H^2(L/K)$ divide the degree $[L:K]$ and consequently are mapped to the only subgroup $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$ of $\mathbb{Q}/\mathbb{Z}$ of order $[L:K]$.

We briefly recall the construction of the map

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

If $\overline{c} \in H^2(L/K)$, then we obtain the invariant $inv_{L/K}\overline{c}$ by choosing a cyclic extension L'/K of equal degree $[L' : K] = [L : K]$ so that by 6.7.3 $H^2(L'/K) = H^2(L/K)$; in particular $\overline{c} \in H^2(L'/K)$. In this cyclic case we have by 6.7.1 an idele cohomology class $c \in H^2(G_{L'/K}, I_{L'})$ with $\overline{c} = jc$ and we obtain

$$inv_{L/K}\overline{c} = inv_{L'/K}\overline{c} = inv_{L'/K}c = \sum_{\mathfrak{p}} inv_{L'_{\mathfrak{P}}/K_{\mathfrak{p}}} c_{\mathfrak{p}} \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

The detour using cyclic extensions, which we have described by introducing the groups $H^2(G_{\Omega/K}, I_\Omega)$ and $H^2(\Omega/K)$ and interpreting inflations as inclusions is necessary, because in general the map

$$H^2(G_{L/K}, I_L) \xrightarrow{j} H^2(L/K)$$

is not surjective. However for the elements in the image of j we immediately obtain from the last definition

Proposition 6.7.7. *If $\overline{c} = jc$, where $\overline{c} \in H^2(L/K)$, $c \in H^2(G_{L/K}, I_L)$, then*

$$inv_{L/K}\overline{c} = inv_{L/K}c$$

Theorem 6.7.8. *The invariant maps*

$$inv_K : H^2(\Omega/K) \to \mathbb{Q}/\mathbb{Z}$$

and

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

are isomorphisms.

Proof. It suffices to verify that $inv_{L/K}$ is bijective. Let L'/K be a cyclic extension of degree $[L' : K] = [L : K]$, so that $H^2(L'/K) = H^2(L/K)$. If $a \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, then by last section there is a $c \in H^2(G_{L'/K}, I_{L'})$ with $inv_{L'/K}c = a$. Set $\overline{c} = jc \in H^2(L'/K) = H^2(L/K)$. Then $inv_{L/K}\overline{c} = inv_{L'/K}\overline{c} = inv_{L'/K}c = a$, ie $inv_{L/K}$ is surjective.

That $inv_{L/K}$ is bijective follows now easily from the fact that the order of $H^2(L/K)$ is a divisor of the degree $[L : K]$ and therefore a divisor of the order of $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$

□

..we now come to the main theorem of class field theory. Let K_0 be a fixed algebraic number field, Ω the field of all algebraic numbers, and $G = G_{\Omega/K_0}$ the galois group of Ω/K_0. We form the union $C_\Omega = \bigcup_K C_K$ where K runs through all finite extensions of K_0. Then C_Ω is canonically a G-module: If $\overline{c} \in C_\Omega$, say $\overline{c} \in C_L$ for an appropriate finite normal extension L/K_0, we set

$$\sigma\overline{c} = \sigma|_L\overline{c} \in C_L \subseteq C_\Omega$$

where $\sigma \in G$

The pair (G, C_Ω) is obviously a formation and the fundamental result of all our constructions is the following

Theorem 6.7.9. *The formation (G, C_Ω) is a class formation with respect to the invariant map introduced in the definition* 6.7.6.

Proof. For the proof we have to verify the axioms,

Axiom I: $H^1(L/K) = 1$ for every normal extension L/K of each finite extension field of K_0.

Axiom II: For every normal extension L/K of each finite extension field of K_0, we have by the last Theorem the isomorphism

$$inv_{L/K} : H^2(L/K) \to \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

• if $K \subseteq L \subseteq N$ are two normal extensions and $\overline{c} \in H^2(L/K)$, then $\overline{c} \in H^2(N/K)$ and

$$inv_{N/K}\overline{c} = inv_{L/K}\overline{c}$$

since $inv_{N/K}$, and $inv_{L/K}$ are defined as the restrictions of inv_K to $H^2(N/K)$ and $H^2(L/K) \subseteq H^2(N/K)$ respectively.

• Let $K \subseteq L \subseteq N$ be two extension fields of K with N/K normal. If $\overline{c} \in H^2(N/K)$ then $res_L\overline{c} \in H^2(N/L)$. For the proof of the formula

$$inv_{N/L}(res_L\overline{c}) = [L : K] \cdot inv_{N/K}\overline{c}$$

we use the analogous formula for the idele invariants 6.6.2. By 6.7.5 there is a $c \in H^2(G_{\Omega/K}, I_\Omega)$ with $jc = \bar{c}$ where we can assume that there is a normal extension M/K containing N, $K \subseteq L \subseteq N \subseteq M$ such that $c \in H^2(G_{M/K}, I_M)$. From the formula in 6.6.2 and using the convention that the inflation maps are to be interpreted as inclusions, we have by 6.7.7

$$inv_{N/L}(res_L \bar{c}) = inv_{M/L}(res_L jc) = inv_{M/L}(jres_L c) = inv_{M/L}(res_L c) =$$

$$[L:K] \cdot inv_{M/K} c = [L:K] \cdot inv_{M/K} jc = [L:K] \cdot inv_{N/K} \bar{c}$$

□

Because of this theorem we can now apply the entire abstract theory of class formations to the case of algebraic number fields. If we again denote by

$$u_{L/K} \in H^2(L/K)$$

the **fundamental class** of the normal extension L/K, which is uniquely determined by the formula $inv_{L/K} u_{L/K} = \frac{1}{[L:K]} + \mathbb{Z}$, then we have the general

Theorem 6.7.10. *The homomorphism cup product with the fundamental class*

$$u_{L/K} \cup : H^q(G_{L/K}, \mathbb{Z}) \to H^{q+2}(L/K)$$

is bijective.

From this we immediately obtain the

Corollary 6.7.11.

$$H^3(L/K) = 1$$

and

$$H^4(L/K) \cong \chi(G_{L/K})$$

For the case $q = -2$ this yields **Artin's Reciprocity law:**

Theorem 6.7.12. *The map cup product with the fundamental class*

$$G_{L/K}^{ab} \cong H^{-2}(G_{L/K}, \mathbb{Z}) \xrightarrow{u_{L/K} \cup} H^0(L/K) = C_K / N_{L/K} C_L$$

yields a canonical isomorphism, ie the ***reciprocity map*** *between the abelianization $G_{L/K}^{ab}$ of the Galois group $G_{L/K}$ and the norm residue group $C_K/N_{L/K}C_L$ of the idele group C_K*

$$\theta_{L/K} : G_{L/K}^{ab} \to C_K / N_{L/K} C_L$$

The inverse of the reciprocity map $\theta_{L/K}$ is induced from the homomorphism $(\ ,L/K) : C_K \to G_{L/K}^{ab}$ with kernel $N_{L/K}C_L$, the ***norm residue symbol****.*

Bibliography

[1] Juergen Neukirch. *Class Field Theory. -The Bonn Lectures- Edited by Alexander Schmidt-Springer-Verlag Berlin Heidelberg (2013).*

[2] Neukirch J., Schmidt A., Wingberg K. *Cohomology of number fields. Second edition. Springer-Verlag Berlin, Heidelberg, New York (2015).*

[3] Juergen Neukirch. *Algebraische Zahlentheorie. Springer-Verlag Berlin Heidelberg 1999*

[4] J.S. Milne. *Algebraic number theory, Class field theory.* `http://www.jmilne.org/math/CourseNotes/`

[5] Emil Artin and John Tate. *Class Field Theory.* Benjamin, New York, 1967

[6] Serge Lang. *Algebraic number theory.* Springer-Verlag New York, Inc. 1994

[7] Oron Propp. *lecture notes on class field theory,taught by Sam Raskin at MIT* `https://ocw.mit.edu/courses/mathematics/18-786-number-theory-ii-class-field-theory-spring-2016/lecture-notes/`

[8] Joachim Mahnkopf. *Klassenkoerpererweiterungen.* (German) [Lecture on Class Field Theory at the University of Vienna, SS 2016.]