ALGEBRA 2: CLASS FIELD THEORY

DR. EDGAR ASSING

Abstract. In this lecture we will develop class field theory using the abstract cohomological approach. The main references are [4] and [5]. These notes are for personal use only and are likely to contain mistakes and misprints. At this place I would like to thank the students of my course (WS 22/23 Bonn) who helped to find and fix many misprints already. This script includes supplementary exercises (without solutions), which where prepared with the help of Dr. B. Michels.

Contents

1. Introduction 2
2. Recap: Galois Theory and pro-finite Groups 6
3. Local Fields 10
4. Cohomology of finite Groups 23
4.1. G-modules, group rings and basic definitions 23
4.2. The long exact sequence 31
4.3. Induced Modules and dimension shift 35
4.4. Inflation, Restriction, Corestriction 39
4.5. The cup-product 49
4.6. The Herbrand quotient 53
4.7. A theorem of Tate 57
4.8. Examples from Galois theory 60
5. Abstract Class Field Theory 62
6. Local Class Field Theory 70
7. Adeles and Ideles 84
8. Global Class Field Theory 90
8.1. Cohomological Preparations 90
8.2. The main theorems of Global Class Field Theory 109
8.3. Reflections on the Ideal Theoretic Formulation 120
References 121

1. Introduction

We start with a brief motivation using ideas from [6]. Let $f \in \mathbb{Z}[X]$ be a monic irreducible polynomial and let p be prime. Write $f_p(X) \in \mathbb{F}_p[X]$ for the unique polynomial with

$$f_p(X) \equiv f(X) \bmod p.$$

Note that f_p will not remain irreducible in general. One possibility is that $f_p(X)$ factors into a product of distinct linear factors. In this case we say $f(X)$ *splits completely modulo* p. Set

$$\mathrm{Spl}(f) = \{p\colon f(X) \text{ splits completely modulo } p\}.$$

Question. Can we *describe* the factorization behavior of $f_p(X)$ as a function of p? Or can we at least give a *rule* determining the set $\mathrm{Spl}(f)$?

An answer to this ill posed question is a *reciprocity law*.

Example 1.1. Suppose $f(X) = X^2 - q$ for some fixed odd prime q. There are obviously three possible ways in which f_p can factor:

$$f_p(X) = (X - a_p)^2 \Leftrightarrow p \in \{2, q\},$$
$$f_p(X) = (X - a_p)(X + a_p) \Leftrightarrow p \in \mathrm{Spl}(f) \Leftrightarrow \left(\frac{q}{p}\right) = 1,\ p \neq 2, q \text{ and}$$
$$f_p(X) \text{ is irreducible } \Leftrightarrow \left(\frac{q}{p}\right) = -1,\ p \neq 2, q.$$

A direct consequence of quadratic reciprocity is that for $p \neq q, 2$ we have

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } q \equiv 1 \bmod 4, \\ (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) & \text{if } q \equiv 3 \bmod 4. \end{cases}$$

This gives us a clean description of the set $\mathrm{Spl}(f)$ in terms of congruence conditions modulo $4q$.

Exercise 1.1. *Let Φ_n be the nth cyclotomic polynomial, then it can be shown that*

$$\mathrm{Spl}(\Phi_n) = \{p\colon p \equiv 1 \ \textit{mod}\ n\}.$$

For more general f the situation becomes very complicated. Let's take a look anyway. We factor

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i) \in \mathbb{C}[X] \text{ for } n = \deg(f).$$

The splitting field $K_f = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ of f is a finite Galois extension of $\mathbb{Q}$. For simplicity we write $G_f = \mathrm{Gal}(K_f|\mathbb{Q})$. Let $\mathcal{O} = \mathcal{O}_{K_f}$ be the ring of integers of K_f

and recall that this is a Dedekind domain. In particular we can decompose

$$p\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{P}_i^e.$$

and we have $\mathcal{O}/\mathfrak{P}_i \cong \mathbb{F}_{p^f}$ for all i. (**Facts from Algebra 1:** If $e > 1$, then $p \mid D_{K_f}$. Furthermore we have $ref = n$.)

Recall that $\mathrm{Gal}(\mathbb{F}_{p^f}|\mathbb{F}_p)$ is generated by the Frobenius automorphism

$$\varphi\colon a \mapsto a^p.$$

This leads us to the following definition:

Definition 1.1. For $p \nmid D_{K_f}$ we define the *Artin Symbol* $\sigma_{\mathfrak{P}_i} \in \mathrm{Gal}(K_f|\mathbb{Q})$ of $\mathfrak{P}_i$ by requiring

$$\sigma_{\mathfrak{P}_i}(a) \equiv a^p \bmod \mathfrak{P}_i$$

for all $a \in \mathcal{O}$.

Note that if $\mathfrak{P}_i \neq \mathfrak{P}_j$, then there is $\tau \in \mathrm{Gal}(K_f|\mathbb{Q})$ such that $\tau(\mathfrak{P}_i) = \mathfrak{P}_j$ and one has

$$\sigma_{\mathfrak{P}_j} = \tau\sigma_{\mathfrak{P}_i}\tau^{-1}.$$

Thus we define the *Artin Symbol* σ_p of p to be the conjugacy class

$$\sigma_p = C_{\mathrm{Gal}(K_f|\mathbb{Q})}(\sigma_{\mathfrak{P}_i}) \subseteq \mathrm{Gal}(K_f|\mathbb{Q})$$

for some i.

From now on we suppose that $\mathrm{Gal}(K_f|\mathbb{Q})$ is abelian (i.e. f is an abelian polynomial). Let

$$\Gamma_{D_{K_f}} = \langle p\colon p \nmid D_{K_f}\rangle \subseteq \mathbb{Q}^\times.$$

In this case the Artin symbol gives rise to a group homomorphism

$$\sigma\colon \Gamma_{D_{K_f}} \to G(f),$$

the so called Artin Map.

Lemma 1.2. *Suppose f is an abelian polynomial. Up to finitely many exceptions we have $p \in \mathrm{Spl}(f)$ if and only if σ_p is trivial.*

Proof. See Sheet 3, Exercise 1 below. ∎

We have the following deep result (containing essentially all the class field theory over $\mathbb{Q}$):

Theorem 1.3 ($\mathbb{Q}$-version of Artin Reciprocity)**.** *Suppose* $\mathrm{Gal}(K_f|\mathbb{Q})$ *is abelian. Then the Artin Symbol gives rise to a surjective group homomorphism* $\sigma\colon \Gamma_{D_{K_f}} \to \mathrm{Gal}(K_f|\mathbb{Q})$ *whose kernel contains the so called ray class group*

$$\Gamma_a^{\mathrm{ray}} = \{r \in \mathbb{Q}^\times\colon r = \frac{c}{d},\ (c, da) = 1 \text{ and } c \equiv d \bmod a\}$$

for a suitable a consisting of ramified primes (i.e. primes dividing D_{K_f}).

Proof. This will follow from a more general theorem at the end of the course. ∎

Equipped with these tools we can return to our question of determining $\mathrm{Spl}(f)$. Indeed we get

$$\{p\colon p \equiv 1 \bmod a\} \subseteq^* \mathrm{Spl}(f),$$

where $\subseteq^*$ stands for inclusion up to the possibility of finitely many exceptions. To make the set a little nicer to study we put

$$\widetilde{\mathrm{Spl}}(f) = [\mathrm{Spl}(f) \cup \{p \equiv 1 \bmod a\}] \setminus \{p \mid a\}.$$

One is led to the following very pleasing result:

Theorem 1.4 (Abelian Polynomial Theorem)**.** *If f is abelian, the $\widetilde{\mathrm{Spl}}(f)$ can be described by congruence conditions with respect to a modulus that only depends on f. Furthermore, if $\widetilde{\mathrm{Spl}}(f)$ is described by congruence conditions, then f is abelian.*

A key ingredient for the second part of the theorem is:

Theorem 1.5. *Let $f, g \in \mathbb{Z}[X]$ be irreducible polynomials. Then*

$$K_f \subseteq K_g \Leftrightarrow \mathrm{Spl}(g) \subseteq^* \mathrm{Spl}(f).$$

To highlight the strength of this result suppose that we know

$$\{p \equiv 1 \bmod n\} \subseteq^* \mathrm{Spl}(f)$$

for some n. Then, recalling that $\mathrm{Spl}(\Phi_n) = \{p \equiv 1 \bmod n\}$ we find that

$$\mathbb{Q} \subseteq K_f \subseteq K_{\Phi_n}.$$

This implies that f is abelian. But we have seen even more:

Theorem 1.6 (Kronecker-Weber, 1853)**.** *Every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.*

This classical theorem can be thought of in some sense as the origin of class field theory.

Sheet 0, Exercise 1: Let d be a square free integer. Show that there is a mth root of unity ζ_m so that $\mathbb{Q}(\sqrt{d})$ is contained in the cyclotomic field $\mathbb{Q}(\zeta_m)$. (**Remark:** This is a special case of the Kronecker-Weber Theorem we will prove later in the lecture.)
Sheet 0, Exercise 2: Let p be a prime and $n > 2$. Show that the nth cyclotomic polynomial Φ_n factors into distinct linear factors modulo p if and only if $p \equiv 1 \bmod n$. (Hint: The following result can be used. Let $a \in \mathbb{F}_p$ be an nth root of unity so that $a^d \neq 1$ for all proper divisors d of n. Then $X - a$ divides Φ_n.)
Sheet 1, Exercise 1: Let $K = \mathbb{Q}(\zeta_n)$ be the nth cyclotomic field. Recall the definition of

$$\Gamma_n = \{\frac{c}{d} \in \mathbb{Q}^\times\colon (c,d) = (cd,n) = 1\}$$

as well as the definition of the Artin map

$$\sigma\colon \Gamma_n \to \mathrm{Gal}(K|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

above. Compute σ explicitly and determine its kernel.

Sheet 2, Exercise 1: Let μ_n be a primitive nth root of unity and let $\mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_n)$ be a tower of filed extensions. Write D_K for the discriminant of K. Recall the definition of Γ_n from Sheet 1, Exercise 1. We define the Artin maps

$$\sigma^{(K)}\colon \Gamma_{D_K} \to \mathrm{Gal}(K|\mathbb{Q}) \text{ and } \sigma^{(\mathbb{Q}(\zeta_n))}\colon \Gamma_n \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$$

as above. Show that the diagram

$$\begin{array}{ccc} \Gamma_n & \xrightarrow{\sigma^{(\mathbb{Q}(\zeta_n)}} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \\ \big\downarrow & & \big\downarrow \\ \Gamma_{D_K} & \xrightarrow{\sigma^{(K)}} & \mathrm{Gal}(K|\mathbb{Q}) \end{array}$$

commutes and use the result from Sheet 1, Exercise 1 to deduce that the Artin map $\sigma^{(K)}\colon \Gamma_{D_K} \to \mathrm{Gal}(K|\mathbb{Q})$ is surjective.

Sheet 3, Exercise 1: Let $L|K$ be a finite Galois extension of algebraic number fields and let $\mathfrak{p}$ be unramified in L such that $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ for distinct primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$. Consider the local fields $F = K_\mathfrak{p}$ and $E_i = L_{\mathfrak{P}_i}$. Recall the identification

$$G(\mathfrak{P}_i) = \{\sigma \in \mathrm{Gal}(L|K)\colon \sigma\mathfrak{P}_i = \mathfrak{P}_i\} = \mathrm{Gal}(E_i|F)$$

of the decomposition group with the Galois group of $E_i|F$. Under this identification the Frobenius automorphism[1] is defined by

$$\left(\frac{L|K}{\mathfrak{P}_i}\right) = \varphi_{E_i|F}.$$

(1) Show that $\mathfrak{p}$ splits completely in K if and only if $\left(\frac{L|K}{\mathfrak{P}_i}\right) = 1$ for some i.

Assume that $L|K$ is abelian and let S denote the set of ramified primes $\mathfrak{p}'$ of K. Write I_K^S for the group of fractional ideals in K generated by all primes not in S. Then we can define the Artin Map $\sigma_{L|K}\colon I_K^S \to \mathrm{Gal}(L/K)$ by extending $\mathfrak{p} \mapsto \left(\frac{L|K}{\mathfrak{P}_i}\right)$ multiplicatively. Write I_L^S for the pre-image of I_K^S under the norm map $\mathrm{Nr}_{L|K}$.

(2) Show that $\mathrm{Nr}_{L|K}(I_L^S) \subseteq \ker(\sigma_{L|K})$.

Sheet 10, Exercise 3: Let $K = \mathbb{Q}(\sqrt{d}) \neq \mathbb{Q}$. Show that K has an abelian extension which is not contained in $K(\zeta)$ for any root of unity ζ. (Hint: Find $u \in K$ such that $K(\sqrt{u})$ is not normal over $\mathbb{Q}$.)

[1] In the first lecture we used $\sigma_\mathfrak{P}$, because we were only working over $\mathbb{Q}$. This notation is slightly more standard keeping track of the extension $L|K$.

2. Recap: Galois Theory and pro-finite Groups

We assume some familiarity with the Galois theory of finite extensions. The theory for infinite extensions is slightly different and a brief introduction can be found for example in [3, Chapter IV]. We start with an example:

Example 2.1. Consider the field $\mathbb{F}_p$ with algebraic closure $\overline{\mathbb{F}}_p$. Then the Galois group $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}_p}|\mathbb{F}_p)$ contains the **Frobenius automorphism** φ given by

$$\varphi(x) = x^p \text{ for all } x \in \overline{\mathbb{F}}_p.$$

Note that the fixed field of $\langle\varphi\rangle = \{\varphi^n \colon n \in \mathbb{Z}\}$ is also $\mathbb{F}_p$. But it can be shown that $\langle\varphi\rangle$ is not $G_{\mathbb{F}_p}$, which is somehow counter intuitive from the point of view of classical Galois theory.

To fix the theory we have to introduce some topology and define pro-finite groups.

Lemma 2.2. *Let T be a Hausdorff topological space. Then the following are equivalent:*

1. *T is the topological inverse limit of finite discrete spaces;*
2. *T is compact and every point in T has a basis of neighborhoods consisting of subsets that are closed and open;*
3. *T is compact and totally disconnected.*

Proof. **(1) $\Longrightarrow$ (2):** Since finite discrete spaces are compact and the inverse limit of compact spaces is compact we can focus on the second property of T in (2). But by definition of the inverse limit topology every point in T has a basis of neighbourhoods consisting of sets of the from $f^{-1}(W)$, where W is a subset of a finite discrete space V and $f\colon T \to V$ is a continuous map. These sets must be open and closed.

(2) $\Longrightarrow$ (3): Let $t \in T$ be a point and let C_t be the connected component of t. Since T is compact, C_t is the intersection of all closed and open subsets containing t. But since T is Hausdorff we obtain $C_t = \{t\}$ by (2). This shows that T is totally disconnected.

(3) $\Longrightarrow$ (1): We write I for the set of equivalence relations $R \subseteq T \times T$ on T such that T/R is finite and discrete in the quotient topology. The set I is partially ordered by inclusion. Further it is directed, since $R_1 \cap R_2$ is in I if R_1 and R_2 are. We will show that the canonical map $\phi\colon T \to \varprojlim_{R\in I} T/R$ is a homeomorphism.

Surjectivity can be shown as follows. For an element $\{t_R\}_{R\in I} \in \varprojlim_{R\in I} T/R$ the sets $(p_R \circ \phi)^{-1}(t_R)$ are non-empty and compact. A finite intersection of these sets will be still non-empty and by compactness

$$\phi^{-1}(\{t_R\}_{R\in I}) = \bigcap_{R\in I} (p_R \circ \phi)^{-1}(t_R) \neq \emptyset.$$

To see that this map is injective we take $t, s \in T$ with $t \neq s$. Since s is not in the connnected component of t there exists an open closed subset $U \subseteq T$ with $t \in U$ and $s \notin U$. We define an equivalence relation R by $(x, y) \in R$ if and only if $x, y \in U$ or $x, y \notin U$. Note that $R \in I$ and $(r, s) \notin R$.

We are done since a continuous bijection between compact spaces is a homeomorphism. ∎

Definition 2.1. A totally disconnected compact (Hausdorff) space T is called a *pro-finite* space.

A topological group G is a group equipped with a topology so that the maps $G \to G, g \mapsto g^{-1}$ and $G \times G \to G, (g, h) \mapsto gh$ are continuous.

Lemma 2.3. *Let G be a Hausdorff topological group. Then the following are equivalent:*

(1) *G is the topological inverse limit of finite discrete groups;*
(2) *G is compact and the identity in G has a basis of neighborhoods that consists of normal subgroups that are open and closed;*
(3) *G is compact and totally disconnected.*

Proof. **(1) $\implies$ (3):** This is obvious since the inverse limit of compact and totally disconnected spaces is compact and totally disconnected.

(2) $\implies$ (1): Let U run through a system of neighbourhoods of the unit element $e \in G$, which consists of open normal subgroups. We claim that the canonical homomorphism

$$\phi \colon G \to \varprojlim_U G/U$$

is an isomorphism. Since G is Hausdorff the map is clearly injective. Now we take $x = \{x_U\}_U \in \varprojlim_U G/U$. Arguing as earlier (finite intersections are non-empty and we are intersecting compact spaces) we find that

$$\phi^{-1}(x) = \bigcap_U \phi_U^{-1}(x_U) \neq \emptyset$$

so that the map is surjective. Since ϕ is open it must be a homeomorphism. Note that the quotients G/U are discrete and compact and therefore finite.

(3) $\implies$ (2): We already know that the underlying topological space is profinite. In particular, every point has a basis of neighbourhoods consisting of open closed subsets. Recall that an open subgroup is automatically closed (as it is the complement of the union of its non-trivial cosets). Take any open closed neighbourhood of the unit element e. We define

$$V = \{v \in U \colon Uv \subseteq U\} \text{ and } H = \{h \in V \colon h^{-1} \in V\}.$$

We claim that H is an open subgroup of G. Firstly we need to establish openness. Fix $v \in V$, so that by definition $uv \in U$ for all $u \in U$. Thus there is a neighbourhood U_u of u and a neighbourhood V_u of v such that $U_u V_u \subseteq U$. The open sets U_u

cover U and by compactness we find a finite sub-cover $U_{u_1}, \ldots, U_{u_n}$. Define

$$V_v = V_{u_1} \cap \ldots \cap V_{u_n}.$$

This is an open neighbourhood of v contained in V. Doing this for every $v \in V$ shows that V is open and we conclude that $H = V \cap V^{-1}$ is open. To see that H is a group we first note that $e \in H$ and that $H^{-1} = H$. Now take $x, y \in H$. We find that $Uxy \subseteq Uy \subseteq U$ so that $xy \in V$. Similarly we see that $y^{-1}x^{-1} \in V$. This directly implies $xy \in H$ as desired. Thus we have found an open subgroup H of G contained in U. In particular H has finite index in G and there are only finitely many distinct conjugates of H in G. Taking the intersection of these yields an open closed normal subgroup of G contained in G. ∎

Definition 2.2. A totally disconnected compact (Hausdorff) topological group is called a *pro-finite group*.

Example 2.4. Let p be a prime number. The rings $\mathbb{Z}/p^n\mathbb{Z}$ with $n \in \mathbb{N}$, form a inverse system with respect to the projections $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ for $n \geq m$. The inverse limit

$$\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$$

is the ring of p-adic integers. Viewed as an additive group it is pro-finite. Similarly we can consider the inverse system $\mathbb{Z}/n\mathbb{Z}$ with projections $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ when $n \mid m$. The inverse limit of this system is the so called **Prüfer ring**:

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n\mathbb{Z}.$$

It can be shown that $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

Given a field F we write $\overline{F}$ for a separable algebraic closure of F. Given a finite extension E of F we write $G_E = \mathrm{Gal}(\overline{F}|E)$. In particular G_F is the absolute Galois group of F. Our goal is to equip G_F with a topology, the so called **Krull topology**, turning it into a pro-finite group.

Let $\sigma \in G_F$, then a basis of (open) neighborhoods of σ is given by cosets $\sigma \cdot G_E$, where E ranges over finite Galois extensions of F (in $\overline{F}$).

Proposition 2.5. *Equipped with the Krull topology G_F is a pro-finite group. Furthermore we have*

$$G_F \cong \varprojlim \mathrm{Gal}(E|F)$$

where we consider the inverse family of finite Galois groups $\mathrm{Gal}(E|F)$ *indexed by finite Galois extensions E of F.*

Proof. Multiplication and taking inverses are obviously continuous with respect to this topology, so that G_F is a topological group.

Next we show that G_F is Hausdorff. Given $\sigma, \tau \in G_F$ with $\sigma \neq \tau$, then there exists a finite Galois extension $E|F$ (in $\overline{F}$) such that $\sigma|_E \neq \tau|_E$. Thus we have $\sigma G_E \cap \tau G_E = \emptyset$.

That G_F is pro-finite now follows from Lemma 2.3. The representation as projective limit is immediate. ∎

Corollary 2.6. *We have*

$$G_{\mathbb{F}_q} \cong \widehat{\mathbb{Z}}.$$

Proof. Recall that we have the isomorphisms $\mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q) \to \mathbb{Z}/n\mathbb{Z}$ given by sending the Frobenius automorphism φ_n to 1 mod $n\mathbb{Z}$. Taking projective limits concludes the proof. ∎

Theorem 2.7 (Fundamental theorem of infinite Galois theory)**.** *The assignment $K \mapsto \mathrm{Gal}(\overline{F}|K)$ is a one to one correspondence between extensions $K|F$ (in $\overline{F}$) and closed subgroups of G_F. The open subgroups of G_F correspond precisely to the finite extensions of F (in $\overline{F}$).*

Proof. First note that every open subgroup of G_F is also closed. Indeed it is the complement of the union of its non-trivial open cosets.

Next, suppose $E|F$ is a finite extension and let $N|E$ be the normal closure of E. Then G_E is open, since each $\sigma \in G_E$ has the open neighborhood $\sigma \cdot G_N \subset G_E$.

We can now show that given an arbitrary extension $K|F$ the Galois group $\mathrm{Gal}(\overline{F}|K)$ is closed. Indeed

$$\mathrm{Gal}(\overline{F}|K) = \bigcap_i G_{K_i},$$

where $K_i|F$ varies over all finite sub-extensions of $K|F$. Thus, according to our previous observations, $\mathrm{Gal}(\overline{F}|K)$ is the intersection of closed subgroups and therefore closed.

Note that the assignment is obviously injective, because K is the fixed field of $\mathrm{Gal}(\overline{F}|K)$. It remains to be seen that it is surjective. Let H be an arbitrary closed subgroup of G_F and denote the fixed field of H by K. We obviously have the inclusion $H \subseteq \mathrm{Gal}(\overline{F}|K)$. To see that equality holds we argue as follows. Let $\sigma \in \mathrm{Gal}(\overline{F}|K)$. Given a finite Galois subextension $L|K$ of $\overline{F}|K$, we see that $\sigma \cdot \mathrm{Gal}(\overline{F}|L)$ is a fundamental open neighborhood in $\mathrm{Gal}(\overline{F}|K)$. The map $H \to \mathrm{Gal}(L|K)$ is surjective by the main theorem of finite Galois theory. Therefore, we can choose $\tau \in H$ such that $\tau|_L = \sigma|_L$ (i.e. $\tau \in H \cap \sigma \cdot \mathrm{Gal}(\overline{F}|L)$). Therefore, σ belongs to the closure of H in $\mathrm{Gal}(\overline{F}|K)$. Since H is closed we conclude that $\sigma \in H$. Thus we have seen that $H = \mathrm{Gal}(\overline{F}|K)$.

Finally let $H \subseteq G_F$ be an open subgroup. Then H is also closed. By the first part of the theorem we find that $H = \mathrm{Gal}(\overline{F}|K)$. Note that we can cover G_F with the cosets of H, which are open and disjoint. By compactness we conclude that there is only a finite number of these. In other words, $H = \mathrm{Gal}(\overline{F}|K)$ has finite index in G_F. This implies that $K|F$ is of finite degree and the proof is complete. ∎

Sheet 1, Exercise 2: Let p be a prime and consider the finite field $\mathbb{F}_p$ with algebraic closure $\overline{\mathbb{F}}_p$. Let φ be the Frobenius automorphism in $G_{\mathbb{F}_p} = \mathrm{Gal}(\overline{\mathbb{F}}_p|\mathbb{F}_p)$ and let $H = \langle\varphi\rangle \subseteq G_{\mathbb{F}_p}$ be the group it generates.

(1) Construct a non-trivial sequence $\{a_n\}_{n\in\mathbb{N}}$ of positive integers such that
$$a_n \equiv a_m \bmod m$$
whenever $m \mid n$. (The following two sequences are trivial: The constant sequence $a_n = a$ for some $a \in \mathbb{N}$ and the identity sequence $a_n = n$.)
(2) Use the sequence from a) to construct an element in $G_{\mathbb{F}_p} \setminus H$, showing that $H \neq G_{\mathbb{F}_p}$.

Sheet 1, Exercise 3: Let G be a group and let $\{H_r\}_{r\in\mathbb{N}}$ be a sequence of normal subgroups of finite index satisfying $H_r \supseteq H_{r+1}$ and such that $\bigcap_r H_r$ is trivial. We call a sequence $(x_n)_{n\in\mathbb{N}}$ a Cauchy sequence (in G) if for every $r \in \mathbb{N}$ there is $N \in \mathbb{N}$ such that for all $n, m \geq N$ we have $x_n x_m^{-1} \in H_r$. Let C denote the set of all Cauchy sequences in G. Further we call $(x_n)_{n\in\mathbb{N}}$ a Null sequence, if for all $r \in \mathbb{N}$ there is $N \in \mathbb{N}$ such that for all $n \geq N$ we have $x_n \in H_r$. Let N denote the set of all Null sequences.

(1) Show that C is a group with respect to the term wise product and that $N \subseteq C$ is a normal subgroup. This allows us to define the completion $\widehat{G} = C/N$ of G. Further, show that the map $G \ni x \mapsto (x, x, \ldots) \in C$ induces an embedding $G \to \widehat{G}$.
(2) Show that the completion $\widehat{G}$ and the inverse limit $\varprojlim G/H_r$ are isomorphic.

Sheet 1, Exercise 4: Show that $\widehat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ as topological groups. (The definition of the pro-finite groups $\widehat{\mathbb{Z}}$ and $\mathbb{Z}_p$ (for p prime) can be found in Example 2.4 above.)
Sheet 10, Exercise 2: Let G be a pro-finite group. A closed subgroup $H \subseteq G$ is called a p-Sylow subgroup of G, if for every open normal subgroup $N \subseteq G$ the group HN/N is a p-Sylow subgroup of G/N. Compute the p-Sylow groups of $\widehat{\mathbb{Z}}$ and $\mathbb{Z}_p^\times$.

3. Local Fields

Roughly speaking local fields are certain locally compact fields. (Note that every field with the discrete topology is locally compact, so that we will need to be more precise.) We will roughly follow the exposition from [3, Chapter II].

Definition 3.1. Let F be a field. An **absolute value** of F is a map $|\cdot|\colon F \to \mathbb{R}$ such that

(1) $|x| \geq 0$ and $|x| = 0$ if and only if $x = 0$;
(2) $|xy| = |x||y|$,
(3) $|x + y| \leq |x| + |y|$.

The last property is called **triangle inequality**. A tuple $(F, |\cdot|)$ of a field F and an absolute value of F is called a **valued field**.

Example 3.1. The fields $\mathbb{R}$ and $\mathbb{C}$ can be equipped with the well known standard absolute value $|\cdot|_\infty$.

Example 3.2. Let F be a field equipped with a discrete valuation v (i.e. the field of fractions of a DVR). Then $|x| = c^{-v(x)}$ with $c > 1$ defines an absolute value on F. Note that we have

$$|x+y| = c^{-v(x+y)} \leq c^{-\min(v(x),v(y))} \leq \max(|x|,|y|).$$

Definition 3.2. Let F be a field with absolute value $|\cdot|$.

(1) The absolute value $|\cdot|$ defines a topology on F via the metric $d(x,y) = |x-y|$.
(2) If $|\cdot|_*$ is another absolute value, we say that $|\cdot|$ and $|\cdot|_*$ are **equivalent** when they define the same topology on F.
(3) The absolute value $|\cdot|$ is called **non-archimedean** if it satisfies the strong triangle inequality

$$|x+y| \leq \max(|x|,|y|).$$

Otherwise $|\cdot|$ is called archimedean.

Note that the trivial absolute value is given by $|x| = \delta_{x=0}$. Since it defines the discrete topology on F it will be excluded from now on.

Proposition 3.3. *Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on F are equivalent if and only if there exists a real number $s > 0$ such that one has*

$$|x|_1 = |x|_2^s \text{ for all } x \in F.$$

Proof. Obviously $|\cdot|$ and $|\cdot|^s$ define the same topology. Now let $|\cdot|_1$ and $|\cdot|_2$ be two equivalent absolute values. In particular we have the implication

$$|x|_1 < 1 \implies |x|_2 < 1.$$

(This is because $|x|_1 < 1$ amounts to $\{x^n\}_{n\in\mathbb{N}}$ converging to 0.) We fix $y \in F$ with $|y|_1 > 1$. For $x \in F^\times$ we find $\alpha \in \mathbb{R}$ so that $|x|_1 = |y|_1^\alpha$. We can take a rational approximation $\frac{m_i}{n_i} \to \alpha$ from above. In particular we obtain

$$|\frac{x^{n_i}}{y^{m_i}}|_1 < 1 \implies |\frac{x^{n_i}}{y^{m_i}}|_2 < 1.$$

We conclude $|x|_2 \leq |y|_2^{\frac{m_i}{n_i}}$. By taking the limit we see that $|x|_2 \leq |y|_2^\alpha$. Approximating α from below yields the opposite inequality so that

$$|x|_2 = |y|_2^\alpha.$$

We get

$$\frac{\log(|x|_1)}{\log(|x|_2)} = \frac{\log(|y|_1)}{\log(|y|_2)} = s.$$

Clearly s is positive, since $|y|_1 > 1$ so that also $|y|_2 > 1$. ∎

Remark 3.4. Note that if v is a discrete valuation on a field F, then the two absolute values $|\cdot|_1 = c_1^{-v(\cdot)}$ and $|\cdot|_2 = c_2^{-v(\cdot)}$ define equivalent absolute values on F.

Theorem 3.5 (Approximation Theorem)**.** *Let $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent absolute values of a field F. For all $a_1, \ldots, a_n \in F$ and every $\epsilon > 0$ there exists $x \in F$ so that*

$$|x - a_i|_i < \epsilon \text{ for all } i = 1, \ldots, n.$$

Proof. We first claim that there is $z \in F$ such that $|z|_1 > 1$ and $|z|_j < 1$ for $j = 2, \ldots, n$. This is done by induction. For $n = 2$ we argue as follows. Since $|\cdot|_1$ and $|\cdot|_n$ are inequivalent there are $\alpha, \beta \in F$ so that $|\alpha|_1 < 1 \leq |\alpha|_n$ and $|\beta|_n < 1 \leq |\beta|_1$. We set $y = \frac{\beta}{\alpha}$ to find an element with $|y|_n < 1 < |y|_1$. We can take $z = y$. For $n > 2$ we assume that we have found z' with $|z'|_1 > 1$ and $|z'|_j < 1$ for $j = 2, \ldots, n-1$. Suppose $|z'|_n \leq 1$, then $z = z'^m y$ will do the job for m sufficiently large. If $|z'|_n > 1$, then we consider the sequence $t_m = \frac{z'^m}{1+z'^m}$. We observe that this sequence converges to 1 with respect to $|\cdot|_1, |\cdot|_n$ and to 0 with respect to $|\cdot|_j$ for $j = 2, \ldots, n-1$. For m sufficiently large we can set $z = t_m y$.

Now by permuting the indices we can run the same argument and find $z_1, \ldots, z_n$ such that $t_m^{(i)} = \frac{z_i^m}{1+z_i^m}$ converges to 1 with respect to $|\cdot|_i$ and to 0 with respect to the other absolute values. We can then take

$$x = a_1 t_{m_1}^{(1)} + \ldots + a_n t_{m_n}^{(n)}$$

for sufficiently large integers $m_1, \ldots, m_n$. ∎

Proposition 3.6. *An absolute value $|\cdot|$ on a field F is non-archimedean if and only if the sequence $(|n|)_{n \in \mathbb{N}}$ is bounded.*

Proof. If F is non-archimedean then the strong triangle inequality shows

$$|n| = |1 + \ldots + 1| \leq 1.$$

To see the other direction we assume that $|n| \leq N$ for all $n \in \mathbb{N}$. For any $x, y \in F$ with $|x| \geq |y|$ we have $|x|^v |y|^{n-v} \leq |x|^n$ for $v \geq 0$. We get

$$|x + y|^n \leq \sum_{v=0}^{n} |\binom{n}{v}| |x|^v |y|^{n-v} \leq N(n+1)|x|^n.$$

We get

$$|x + y| \leq N^{\frac{1}{n}} (1+n)^{\frac{1}{n}} \max(|x|, |y|).$$

We obtain the strong triangle inequality by taking $n \to \infty$. ∎

Exercise 3.1. *Classify all absolute values of $\mathbb{Q}$ up to equivalence. More precisely, show that all absolute values of $\mathbb{Q}$ are equivalent to $|\cdot|_\infty$ (when they are archimedean) or $|\cdot|_p$ for some prime p (when they are non-archimedean).*

Definition 3.3 (and Lemma)**.** Let F be a field equipped with a non-archimedean absolute value $|\cdot|$. Then we define the **valuation ring** of F by $\mathcal{O} = \{x \in F \colon |x| \leq 1\}$. The units in $\mathcal{O}$ are $\mathcal{O}^\times = \{x \in F \colon |x| = 1\}$ and $\mathcal{O}$ has a unique maximal ideal $\mathfrak{p} = \{x \in F \colon |x| < 1\}$. (In particular the ring $\mathcal{O}$ is a valuation ring.) The **residue field** of $\mathcal{O}$ is $\mathfrak{k} = \mathcal{O}/\mathfrak{p}$.

Proof. **Exercise.** ∎

Definition 3.4. We define the valuation v on F associated to $|\cdot|$ by $v(x) = -\log(|x|)$. If there is a positive $s \in \mathbb{R}$ such that $v(F^\times) = s\mathbb{Z}$, then v is called discrete. We say that v is normalized if $s = 1$.

Remark 3.7. If v is discrete and normalized, then $\mathcal{O}$ is a DVR and all non-zero ideals of $\mathcal{O}$ are given by $\mathfrak{p}^n = \varpi^n \cdot \mathcal{O} = \{x \in F \colon v(x) \geq n\}$, where ϖ is a uniformizer (i.e. a fixed element $\varpi \in F$ with $v(\varpi) = 1$). Furthermore, one has $\mathfrak{p}^n/\mathfrak{p}^{n+1} \cong \mathfrak{k}$.

Note that one can always assume that the valuation associated to $|\cdot|$ is normalized after possible replacing $|\cdot|$ by an equivalent absolute value.

Given a field F with non-archimedean absolute value $|\cdot|$ so that the associated valuation v is discrete and normalized we introduce the following additional notation: We write $U^n = 1 + \mathfrak{p}^n$ for the higher unit groups. For convenience we set $U^0 = \mathcal{O}^\times$. Further, if $\mathfrak{k}$ is finite, let $\sharp\mathfrak{k} = q = p^f$, where p is the characteristic of $\mathfrak{k}$. Recall that f is the degree of $\mathfrak{k}$ over $\mathbb{F}_p$ and $q = (\mathcal{O} \colon \mathfrak{p})$. The (normalized) absolute value associated to v is given by

$$|x| = q^{-v(x)}.$$

Recall that a noetherian integal domain R is a Dedekind domain if and only if the localizations $R_\mathfrak{p}$ are DVR's for all prime ideals $\mathfrak{p} \neq 0$ of R. Thus our discussion so far applies to localizations of Dedekind domains and their fields of fractions equipped with the appropriate absolute value. This will later turn out to be our main source for *local fields*.

Before we further venture in this direction we return to the more general situation of a field F equipped with a non-trivial absolute value.

Definition 3.5. A valued field $(F, |\cdot|)$ is called complete if every Cauchy sequence $(a_n)_{n\in\mathbb{N}}$ in F converges to an element $a \in F$. (i.e. $\lim_{n\to\infty} |a_n - a| = 0$.)

Remark 3.8. Any valued field $(F, |\cdot|)$ gives rise to a complete valued field $(\widehat{F}, |\cdot|)$ via the usual completion process, which should be well known from Analysis 1. (See the basic example $(\mathbb{Q}, |\cdot|_\infty) \rightsquigarrow (\mathbb{R}, |\cdot|_\infty)$.)

Theorem 3.9 (Ostrowski)**.** *Let $(F, |\cdot|)$ be a complete valued field and suppose that $|\cdot|$ is archimedean. Then there is an isomorphism σ from F onto $\mathbb{R}$ or $\mathbb{C}$ satisfying*

$$|x| = |\sigma(x)|_\infty^s$$

for all $x \in F$ and some fixed $s > 0$.

Proof. Note that since $|\cdot|$ is archimedean the characteristic of F must be 0 so that it contains $\mathbb{Q}$. By replacing $|\cdot|$ by $|\cdot|^{-s}$ we can assume without loss of generality, that the absolute value restricted to $\mathbb{Q}$ coincides with the normal absolute value $|\cdot|_\infty$. Since F is complete it must contain a completion of $\mathbb{Q}$ which is isomorphic to $\mathbb{R}$. Thus there is an isomorphism $\sigma\colon \mathbb{R} \to \widehat{\mathbb{Q}} \subseteq F$ so that $|a| = |\sigma(a)|$.

We conclude the proof by showing that each $x \in F$ satisfies a quadratic equation over $\mathbb{R}$. Define

$$f(z) = |x^2 - \mathrm{Tr}_{\mathbb{C}|\mathbb{R}}(z)x + \mathrm{Nr}_{\mathbb{C}|\mathbb{R}}(z)|.$$

Note that the image of f is in $[0, \infty)$. Because $\lim_{z\to\infty} f(z) = \infty$ we find that $f(z)$ has a minimum, say m which is attained:

$$S = \{z \in \mathbb{C}\colon f(z) = m\} \neq \emptyset.$$

We claim that $m = 0$, which concludes the proof.

We take $z_0 \in S$ such that $|z_0| \geq |z|$ for all $z \in S$. This is possible because S is nonempty bounded and closed. Suppose that $m > 0$. We look at

$$g(X) = X^2 - \mathrm{Tr}_{\mathbb{C}|\mathbb{R}}(z_0)X + \mathrm{Nr}_{\mathbb{C}|\mathbb{R}}(z_0) + \epsilon, \text{ for } 0 < \epsilon < m.$$

Let z_1, z_1' be the two complex roots of this polynomial. These satisfy

$$z_1 z_1' = \mathrm{Nr}_{\mathbb{C}|\mathbb{R}}(z_0) + \epsilon,$$

so that

$$|z_1| > |z_0|. \tag{1}$$

We consider the auxiliary polynomial

$$G(X) = [g(X) - \epsilon]^n - (-\epsilon)^n = \prod_{i=1}^{2n}(X - \alpha_i).$$

Obviously $G(z_1) = 0 = G(z_1')$ so that without loss of generality we can assume $z_1 = \alpha_1$. Evaluating at x and rearranging products we find

$$|G(x)|^2 = \prod_{i=1}^{2n} f(\alpha_i) \geq f(z_1)m^{2n-1}.$$

On the other hand we can estimate

$$|G(x)| \leq f(z_0)^n + \epsilon^n = m^n + \epsilon^n.$$

We obtain

$$\frac{f(z_1)}{m} \leq \left(1 + \left(\frac{\epsilon}{m}\right)^n\right)^2.$$

Taking $n \to \infty$ we find that $f(z_1) \leq m$. By definition of m this implies $f(z_1) = m$ so that $z_1 \in S$. Now (1) is a contradiction to the maximality of z_0. ∎

Remark 3.10. We call the fields $\mathbb{R}$ and $\mathbb{C}$ **archimedean local fields**.

Definition 3.6. A non-archimedean complete valued field $(F, |\cdot|)$ whose associated valuation is discrete and the residue field is finite is called a **non-archimedean local field**. A **local field** F is a field that can be equipped with an absolute value $|\cdot|$ so that $(F, |\cdot|)$ is either a archimedean or non-archimedean local field.

Remark 3.11. Alternatively one can define a local field to be a non-discrete locally compact topological field. This is somehow the cleaner definition, but for our purposes the route taken appears to be quicker.

Proposition 3.12. *Let $(F, |\cdot|)$ be a non-archimedean valued field with completion $(\widehat{F}, |\cdot|)$. Then we have $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$ (i.e. the residue field is invariant under taking completions). Furthermore, if the valuation v associated to $|\cdot|$ is discrete, then we have*

$$\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n \text{ and } \widehat{\mathcal{O}} \cong \varprojlim_n \mathcal{O}/\mathfrak{p}^n.$$

Similarly one has $\widehat{\mathcal{O}}^\times = \varprojlim_n \mathcal{O}^\times/U^n$.

Proof. **Exercise.** (See Sheet 3, Exercise 3 at the end of this section.) □

Lemma 3.13 (Hensel)**.** *Let $(F, |\cdot|)$ be a complete valued field with non-archimedean absolute value $|\cdot|$. Suppose that $f \in \mathcal{O}[X]$ admits a factorization*

$$f \equiv \overline{g}\overline{h} \text{ mod } \mathfrak{p} \tag{2}$$

modulo $\mathfrak{p}$ into relative prime polynomials $\overline{g}, \overline{h} \in \mathfrak{k}[X]$. Then f admits a factorization $f = gh$ into polynomials $g, h \in \mathcal{O}[X]$ such that $\deg(g) = \deg(\overline{g})$ and $g \equiv \overline{g}$ mod $\mathfrak{p}$ and $h \equiv \overline{h}$ mod $\mathfrak{p}$.

Proof. Put $d = \deg(f)$ and $m = \deg(\overline{g})$. We must have $d - m \geq \deg(\overline{h})$. We take any polynomial $g_0, h_0 \in \mathcal{O}[X]$ such that $g_0 \equiv \overline{g} \bmod \mathfrak{p}$, $h_0 \equiv \overline{h} \bmod \mathfrak{p}$, $\deg(g_0) = m$ and $\deg(h_0) \leq d - m$. Since $\overline{h}$ and $\overline{g}$ are relative prime there are polynomials $a, b \in \mathcal{O}[X]$ so that

$$ag_0 + bh_0 \equiv 1 \bmod \mathfrak{p}.$$

Consider the polynomials $f - g_0h_0$ and $ag_0 + bh_0 - 1$ and pick a coefficient of minimal absolute value. We call this coefficient ϖ. (Note that $\varpi \in \mathfrak{p}$.) Starting here we want to define sequences g_n and h_n inductively and take the limit. Thus we take $n \geq 1$ and suppose that g_{n-1} and h_{n-1} are defined such that $f \equiv g_{n-1}h_{n-1} \bmod (\varpi^n)$, $g_n \equiv g_{n-1} \bmod (\varpi^n)$ and $h_n \equiv h_{n-1} \bmod (\varpi^n)$. Put $f_n = \varpi^{-n}(f - g_{n-1}h_{n-1}) \in \mathcal{O}[X]$. We make the Ansatz

$$g_n = g_{n-1} + \varpi^n \cdot p_n \text{ and } h_n = h_{n-1} + \varpi^n \cdot q_n,$$

for some polynomials $p_n, q_n \in \mathcal{O}[X]$ with $\deg(p_n) < m$ and $\deg(q_n) \leq d - m$ as follows. Since

$$f - g_nh_n = \varpi^n(f_n - g_{n-1}q_n - h_{n-1}p_n)$$

we get the condition

$$g_{n-1}q_n + h_{n-1}p_n \equiv g_0q_n + h_0p_n \equiv f_n \bmod (\varpi).$$

We define p_n by[2]

$$b \cdot f_n = qg_0 + p_n$$

for $\deg(p_n) < \deg(g_0) = m$. Since, by construction, the highest coefficient of g_0 is a unit we have $q \in \mathcal{O}[X]$ and get

$$g_0(af_n + h_0q) + h_0p_n \equiv f_n \bmod (\varpi).$$

We let q_n be the polynomial obtained from q by dropping all coefficients divisible by ϖ. It is easy to check that $\deg(q_n) \leq d - m$. This completes the inductive process.

Obviously $g = \lim_{n\to\infty} g_n$ and $h = \lim_{n\to\infty} h_n$ exist (due to completeness) and do the desired job. □

Theorem 3.14. *Let $(F, |\cdot|)$ be a complete valued field. Then $|\cdot|$ may be extended in a unique way to an absolute value on any given algebraic extension $E|F$. If $E|F$ is of degree $n < \infty$, then the extension is given by*

$$|\alpha| = |\mathrm{Nr}_{E|F}(\alpha)|^{\frac{1}{n}} \tag{3}$$

and $(E, |\cdot|)$ is again complete.

Proof. The archimedean situation can be easily treated using Ostrowski's theorem. Thus we assume that we are in the non-archimedean situation.

Note that (3) defines a valuation for finite extensions. Since every algebraic extension is the union of finite subextensions this shows the existence of an extended valuation. Thus we only need to show uniqueness. Suppose $|\cdot|'$ is another extension with valuation ring $\mathcal{O}'_E$. We claim that

$$\mathcal{O}_E = \{\alpha \in E \colon \mathrm{Nr}_{E|F}(\alpha) \in \mathcal{O}_F\} \subseteq \mathcal{O}'_E.$$

Indeed take $\alpha \in \mathcal{O}_E \setminus \mathcal{O}'_E$ with minimal polynomial

$$f(x) = x^d + a_1x^{d-1} + \ldots + a_d \text{ for } a_1, \ldots, a_d \in \mathcal{O}_F.$$

Note that $\alpha^{-1} \in \mathfrak{p}'_E$, where $\mathfrak{p}'_E$ is the unique maximal ideal of $\mathcal{O}'_E$. Inserting α in f, dividing by α^d yields

$$0 = 1 + a_1\alpha^{-1} + \ldots + a_d\alpha^{-d} \in 1 + \mathfrak{p}'_E,$$

which is a contradiction. Thus $\mathcal{O}_E \subseteq \mathcal{O}'_E$ and

$$|\alpha| \leq 1 \implies |\alpha|' \leq 1.$$

The latter implies that the valuations $|\cdot|$ and $|\cdot|'$ are equivalent. (This is a quick application of the approximation theorem.) Equality follows, since they agree on F.

[2]We would want to use $g_0af_n + h_0bf_n \equiv f_n \bmod (\varpi)$. The only problem with this is that the degree might become too large.

Completeness can be reduced to standard analytic facts for finite dimensional vector spaces and we omit the details. ◻

Theorem 3.15. *The non-archimedean local fields are precisely the finite extensions of the fields $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$.*

Proof. That finite extensions of $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are non-archimedean local fields should be clear.

Conversely, let $(F, |\cdot|)$ be a non-archimedean local field. We write p for the characteristic of the residual field and q for its size. If the characteristic of F is 0, then F contains $\mathbb{Q}$ and the restriction of $|\cdot|$ to $\mathbb{Q}$ must be equivalent to $|\cdot|_p$. We directly obtain $\mathbb{Q}_p \subseteq F$. That the extension is finite follows from standard topological considerations (i.e. local compactness). If the characteristic of F is positive, one can show that $F = \mathbb{F}_q(t)$ and $\mathbb{F}_p((t)) \subseteq F$. ◻

We gather some important facts on the unit group of a non-archimedean local field F.

Theorem 3.16. *Let F be a non-archimedean local field. We have a decomposition*

$$F^\times = \mathcal{O}^\times \times \langle \varpi \rangle,$$

where ϖ is a generator of $\mathfrak{p}$ (i.e. ϖ is a uniformizer).

Proof. Once ϖ is fixed every element $x \in F^\times$ can be written as $x = u \cdot \varpi^k$ with $u \in \mathcal{O}^\times$ and $k = v(x) \in \mathbb{Z}$. This gives the sequence

$$1 \to \mathcal{O}^\times \to F^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

which splits. ◻

Theorem 3.17. *Let F be a non-archimedean local field. The group $\mathcal{O}^\times$ is an open compact subgroup of $F^\times$. (In particular it is closed.) Furthermore, the group $F^\times$ is locally compact.*

Proof. We can cover $\mathcal{O}^\times$ by the open sets $a \cdot U^1 = a + \mathfrak{p}$ where a ranges over $a \in \mathcal{O} \setminus \mathfrak{p}$. Therefore $\mathcal{O}^\times$ is open. Compactness follows by the (topological) isomorphism $\mathcal{O}^\times \cong \varprojlim \mathcal{O}^\times / U^n$. Every point in $F^\times$ is contained in the compact set $\varpi^n \cdot \mathcal{O}^\times$ for some $n \in \mathbb{Z}$. This makes $F^\times$ locally compact and concludes the proof. ◻

Lemma 3.18. *Let F be a non-archimedean local field of characteristic zero. For $m \in \mathbb{N}$ and sufficiently large $n \in \mathbb{N}$ the map $x \mapsto x^m$ induces an isomorphism*

$$U^n \to U^{n+v(m)}.$$

Proof. Take $x = 1 + a \cdot \varpi^n$ and compute

$$x^m = (1 + a \cdot \varpi^n)^m = 1 + a \cdot m \cdot \varpi^n + \binom{m}{2} \cdot a^2 \cdot \varpi^{2n} + \ldots \equiv 1 \bmod \mathfrak{p}^{n+v(m)}.$$

To see surjectivity we need to solve the equation

$$1 + a \cdot \varpi^{n+v(m)} = 1 + m \cdot \varpi^n \cdot x + \varpi^{2n} f(x)$$

in x. Note that $f \in \mathbb{Z}[X]$. Writing $m = u \cdot \varpi^{v(m)}$ yields the equivalent equation

$$-a + u \cdot x + \varpi^{n-v(m)} \cdot f(x) = 0.$$

For $m > v(n)$ this can be solved using Hensel's lemma.

If we choose n large enough, so that U^n contains no m-th roots of unity, then the map is also injective. ∎

Corollary 3.19. *Let F be a non-archimedean local field of characteristic zero. For every $m \in \mathbb{N}$ the group of m-th powers $F^{m\times}$ is an open subgroup of $F^\times$. Furthermore,*

$$\bigcap_{m=1}^{\infty} F^{m\times} = \{1\}.$$

Proof. Take $x^m \in F^{m\times}$. Then, for sufficiently large n, we have

$$x^m \cdot U^{n+v(m)} = (x \cdot U^n)^m \subseteq F^{m\times}.$$

This is a neighbourhood of x.

Next take $a \in \bigcap_{m=1}^{\infty} F^{m\times}$. Then we must have $a \in \mathcal{O}^\times$. Thus we can write $a = u_m^m$ with $u_m \in \mathcal{O}^\times$ for all m. This can only be true if $a \in \bigcap_{n\geq 1} U^n = \{1\}$. ∎

Theorem 3.20. *Let F be a non-archimedean local field. The index of $(F^\times)^m$ in $F^\times$ is finite and given by*

$$[F^\times : F^{m\times}] = m \cdot q^{v(m)} \cdot \sharp F_m = \frac{m}{|m|} \cdot \sharp F_m,$$

where F_m is the group of m-th roots of unity in F. If F has positive characteristic p, then we need to assume that $(m, p) = 1$.

Proof. One way to see this is by using structural properties of $\mathcal{O}_F^\times$. However, there is (in our opinion) a more elegant way to see this using the Herbrand quotient, which we will introduce later. Therefore we postpone the proof to Sheet 7, Exercise 2 below. ∎

Corollary 3.21. *Let F be a non-archimedean local field of characteristic zero. We have $[\mathcal{O}_F : (\mathcal{O}_F)^m] = |m|^{-1} \cdot \sharp F_m$.*

Let $(F, |\cdot|_F)$ be a non-archimedean local field and let v_F be the associated normalized discrete valuation. We will consider a finite extension $E|F$ of degree n. Then $(E, |\cdot|_E)$ is a non-archimedean local field where $|\cdot|_E$ is the unique extension of $|\cdot|_F$. The associated valuation is given by

$$w_E(\cdot) = \frac{1}{n} v_F(\mathrm{Nr}_{E|F}(\cdot)).$$

In particular $v_F(F^\times) \subseteq w_E(E^\times)$. Similarly we have an inclusion of residue fields $\mathfrak{k}_F \subset \mathfrak{k}_E$.

Definition 3.7. The index $e = e(E|F) = [w_E(E^\times)\colon v_F(F^\times)]$ is called the **ramification index** of the extension $E|F$. The degree $f = f(E|F) = [\mathfrak{k}_E\colon \mathfrak{k}_F]$ is called the **inertia degree**.

Proposition 3.22. *Let $E|F$ be a finite extension of non-archimedean local fields. One has $[E\colon F] = ef$.*

Proof. The inequality $[E\colon F] \geq ef$ holds in general and does not need any assumptions on the valuations. Indeed we can argue as follows. We choose a basis $\omega_1, \ldots, \omega_f$ of $\mathfrak{k}_E|\mathfrak{k}_F$. We can lift this basis to $\mathcal{O}_E$ (by choosing representatives). Abusing notation we will again denote the lifted basis by $\omega_1, \ldots, \omega_f$. Next take $\pi_0, \ldots, \pi_{e-1} \in \mathcal{O}_E \setminus \{0\}$ to be representatives of the cosets in $w_E(E^\times)/v_F(F^\times)$. We claim that $\omega_j\pi_i$ are linearly independent over F. Suppose

$$\sum_{i=0}^{e-1}\sum_{j=1}^{f} a_{ij}\omega_j\pi_i = 0,$$

where $a_{ij} \in F$ are not all 0. We consider the j-sums $s_i = \sum_{j=1}^f a_{ij}\omega_j$. If $s_i \neq 0$, then $w_E(s_i) \in v_F(F^\times)$. Now there are at least two indices i_1, i_2 so that $w_E(s_{i_1}\pi_{i_1}) = w_E(s_{i_2}\pi_{i_2})$, but this contradicts the choice of the π_i's.

To see equality we need to use completeness.[3] Put $M = \sum_{i=0}^{e-1}\sum_{j=1}^{f}\mathcal{O}_F\omega_j\pi_i$. We claim that $\mathcal{O}_E = M$, which then completes the proof. First note that $\mathcal{O}_E = M + \mathfrak{p}_F\mathcal{O}_E$. But since $\mathfrak{p}_F^i M \subseteq M$ we get

$$\mathcal{O}_E = M + \mathfrak{p}_F^v\mathcal{O}_E$$

for all $v \geq 1$. We conclude that M is dense in $\mathcal{O}_E$. This completes the proof, since M is closed by construction. ∎

Definition 3.8. A finite extension $E|F$ is called **unramified** if the extension of the residue fields $\mathfrak{k}_E|\mathfrak{k}_F$ is separable and one has $[E\colon F] = [\mathfrak{k}_E\colon \mathfrak{k}_F]$. An arbitrary algebraic extension is called unramified if it is the union of finite unramified extensions.

Proposition 3.23. *Let $E|F$ and $F'|F$ be two extensions of a non-archimedean local field F (inside $\overline{F}$). Put $E' = EF'$. Then $E|F$ is unramified implies that $E'|F'$ is unramified. In particular, each subextension of an unramified extension is unramified and the composite of two unramified extensions is unramified.*

Proof. As usual we can assume that $E|F$ is finite. Note that the extension of residue fields $\mathfrak{k}_E|\mathfrak{k}_F$ is separable and finite and thus generated by a primitive element $\overline{\alpha}$. Let $\alpha \in \mathcal{O}_E$ be some lift of $\overline{\alpha}$ with minimal polynomial $f \in \mathcal{O}_F[X]$. We

[3] One could also assume that $E|F$ is separable and v_F is discrete.

have the inequality

$$[\mathfrak{k}_E\colon \mathfrak{k}_F] \leq \deg(\overline{f}) = \deg(f) = [F(\alpha)\colon F] \leq [E\colon F] = [\mathfrak{k}_E\colon \mathfrak{k}_F].$$

We conclude that $E = F(\alpha)$ and $\overline{f}$ is the minimal polynomial of $\overline{\alpha}$ over $\mathfrak{k}_F$. This implies $E' = F'(\alpha)$.

To see that $E'|F'$ is unramified we consider the minimal polynomial $g \in \mathcal{O}_{F'}[X]$ of α over F'. In view of Hensel's Lemma the reduction $\overline{g}$ of g must be irreducible so that we get

$$[\mathfrak{k}_{E'}\colon \mathfrak{k}_{F'}] \leq [E'\colon F'] = \deg(g) = \deg(\overline{g}) = [\mathfrak{k}_{F'}(\overline{\alpha})\colon \mathfrak{k}_{F'}] \leq [\mathfrak{k}_{E'}\colon \mathfrak{k}_{F'}].$$

We find that $[E'\colon F'] = [\mathfrak{k}_{E'}\colon \mathfrak{k}_{F'}]$ so that the extension is unramified. ◻

Definition 3.9. Let F be an non-archimedean local field and let $E|F$ be an algebraic extension. Then the composite $T|F$ of all unramified subextensions is called the **maximal unramified subextension** of $E|F$.

Proposition 3.24. *The residue field $\mathfrak{k}_T$ of T is the separable closure of $\mathfrak{k}_F$ in the extension of $\mathfrak{k}_E|\mathfrak{k}_F$. The value group of T equals that of F.*

Proof. Let $\overline{\alpha} \in \mathfrak{k}_E$ be separable over $\mathfrak{k}_F$. We need to show that $\overline{\alpha}$ is in the residue field of T. Let $\overline{f} \in \mathfrak{k}_F[X]$ be the minimal polynomial of $\overline{\alpha}$ with lift $f \in \mathcal{O}_F[X]$. Then f is irreducible and using Hensel's Lemma we see that it has a root α so that $\alpha \equiv \overline{\alpha} \bmod \mathfrak{p}_E$. This means $[F(\alpha)\colon F] = [\mathfrak{k}_F(\overline{\alpha})\colon \mathfrak{k}_F]$ so that $F(\alpha)|F$ is unramified. This gives $F(\alpha) \subseteq T$ and thus $\overline{\alpha}$ is in the desired residue field.

The claim concerning the value groups is immediate. ◻

The following construction makes unramified extensions so important. Recall that if $E|F$ is an unramified extension, then we have $e = 1$ so that

$$[E\colon F] = [\mathfrak{k}_E\colon \mathfrak{k}_F].$$

The unramified extension is always normal and we have

$$\mathrm{Gal}(E|F) \cong \mathrm{Gal}(\mathfrak{k}_E|\mathfrak{k}_F).$$

The isomorphism is explicitly given by

$$\overline{\sigma}(x + \mathfrak{p}_E) = \sigma x + \mathfrak{p}_E.$$

Recalling that the group $\mathrm{Gal}(\mathfrak{k}_E|\mathfrak{k}_F)$ is cyclic and generated by a canonical automorphism leads to the following definition

Definition 3.10. The automorphism $\varphi_{E|F} \in \mathrm{Gal}(E|F)$ that induces the automorphism

$$\overline{x} \mapsto \overline{x}^{q_F}, \text{ for } \overline{x} \in \mathfrak{k}_E.$$

on the residue field $\mathfrak{k}_E$ is called the **Frobenius Automorphism**.

Theorem 3.25. *Let $L \supseteq E \supseteq F$ be two unramified extensions of F. We have*

$$\varphi_{E|F} = \varphi_{L|F}|_E = \varphi_{L|F}\,\mathrm{Gal}(L|E) \in \mathrm{Gal}(E|F) \text{ and } \varphi_{L|F}^{[E\colon F]} = \varphi_{L|E}.$$

Proof. This follows directly from the definition. ∎

Sheet 2, Exercise 2: Let $\mathcal{O}$ be a discrete valuation ring with valuation v and unique maximal ideal $\mathfrak{p} \subseteq \mathcal{O}$ and field of fractions K. Suppose that the residual field is finite and write $q = \sharp\mathcal{O}/\mathfrak{p}$. Define the absolute value $|x| = q^{-v(x)}$ on K.

(1) Show that $|\cdot|$ is indeed an absolute value and that it satisfies the strong triangle inequality. (In other words show that $(K, |\cdot|)$ is a non-archimedean valued field.)
(2) Define the sequence of subgroups $\{H_r\}_{r\in\mathbb{N}}$ (of $(\mathcal{O}, +)$) by $H_r = \mathfrak{p}^r$. Show that for a sequence $(a_n)_{n\in\mathbb{N}}$ in $\mathcal{O}$ the following are equivalent:
   - (a_n) is a Cauchy sequence (resp. (a_n) converges to 0) with respect to $|\cdot|$ (in the usual sense);
   - (a_n) is a Cauchy sequence (resp. (a_n) is a Null sequence) with respect to the sequence of subgroups $\{H_r\}_{r\in\mathbb{N}}$ as defined on Sheet 1, Exercise 3.
(3) Write $\widehat{\mathcal{O}}$ for (any) completion of $\mathcal{O}$ and show that the field of fractions $K_v = \mathbb{Q}(\widehat{\mathcal{O}})$ is a non-archimedean local field.

Sheet 2, Exercise 3: Classify all absolute values of $\mathbb{Q}$ up to equivalence. The candidates are:

- The usual absolute value $|x|_\infty = \operatorname{sgn}(x) \cdot x$; and
- The p-adic absolute values defined by $|x|_p = p^{-v_p(x)}$, where v_p is the usual p-adic valuation.[4]

One can now proceed as follows

(1) Show that all the candidate absolute values are pairwise inequivalent.
(2) Show that each non-archimedean absolute value $|\cdot|$ is equivalent to $|\cdot|_p$ for some p. (Hint: Consider the ideal $\mathfrak{a} = \{a \in \mathbb{Z} \colon |a| < 1\}$ in $\mathbb{Z}$).
(3) Show that each archimedean absolute value $|\cdot|$ is equivalent to $|\cdot|_\infty$. (Hint: Show first, that for all $n, m \in \mathbb{N}$ one has $|m|^{\frac{1}{\log(m)}} = |n|^{\frac{1}{\log(n)}}$.)

(Bonus: What about the function field $K = \mathbb{F}_q(X)$?)

Sheet 2, Exercise 4: Let p be a prime.

(1) Show that $\mathbb{Q}_p$ contains the $(p-1)$th roots of unity. (Hint: Hensel's Lemma.)
(2) Determine all roots of unity in $\mathbb{Q}_p$.
(3) Show that $\mathbb{Q}_p$ contains infinitely many quadratic extensions $\mathbb{Q}(\sqrt{D})$ of $\mathbb{Q}$.

Sheet 3, Exercise 2: Recall the absolute values of $\mathbb{Q}$:

- The archimedean valuation: $|x|_\infty = \operatorname{sgn}(x) \cdot x$ with corresponding completion $\mathbb{Q}_\infty = \mathbb{R}$;
- The non-archimedean absolute values indexed by primes p: $|x|_p = p^{-v_p(x)}$ with corresponding completion $\mathbb{Q}_p$.

[4] On $\mathbb{Z}$ it is defined by $v_p(0) = -\infty$ and $v_p(m) = k$ if k is the largest integer so that $p^k \mid m$. One then extends v_p from $\mathbb{Z}$ to $\mathbb{Q}$ in the obvious way. Note that p is always prime in this context.

(It was shown in Exercise 3, Sheet 2 that these are all inequivalent and exhaust all possible absolute values up to equivalence.) Put $\mathcal{P} = \{p \text{ prime }\} \cup \{\infty\}$.

(1) Show that for each $x \in \mathbb{Q}$ we have
$$\prod_{v \in \mathcal{P}} |x|_v = 1.$$
(2) Use the Approximation Theorem (i.e. Theorem 3.5) and $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$ as topological groups (see Exercise 4 from Sheet 1) to show that $\mathbb{Z}$ is dense in $\widehat{\mathbb{Z}}$.
(3) Let
$$(y_v)_{v \in \mathcal{P}} \in \prod_{v \in \mathcal{P}} \mathbb{Q}_v^\times$$
and assume that for all but finitely many primes p we have $y_p \in \mathbb{Z}_p^\times$. Show that there are $q_y \in \mathbb{Q}^\times$ such that
$$y_p/q_y \in \mathbb{Z}_p^\times$$
for all primes p and $y_\infty/q_y \in \mathbb{R}_{\geq 0}$.

Sheet 3, Exercise 3: Let $(F, |\cdot|)$ be a non-archimedean valued field with discrete valuation v associated to $|\cdot|$. with completion $(\widehat{F}, |\cdot|)$. We write $\widehat{O}$ for the valuation ring in $\widehat{F}$ and $\widehat{\mathfrak{p}}$ for the unique maximal ideal in $\widehat{\mathcal{O}}$.

(1) Show that $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}}^n \cong \mathcal{O}/\mathfrak{p}^n$ and $\widehat{\mathcal{O}} \cong \varprojlim_n \mathcal{O}/\mathfrak{p}^n$.
(2) Show that $\widehat{\mathcal{O}}^\times/\widehat{U}^1 \cong (\mathcal{O}/\mathfrak{p})^\times$ and $\widehat{\mathcal{O}}^\times = \varprojlim_n \mathcal{O}^\times/U^n$.

This establishes most of Proposition 3.12. Note that all isomorphisms are to preserve topologies, where all finite sets carry the discrete topology. (The statement $\widehat{\mathcal{O}}/\widehat{\mathfrak{p}} \cong \mathcal{O}/\mathfrak{p}$ from Proposition 3.12 is implicit in Exercise 2.c) from Sheet 2.)

Sheet 3, Exercise 4: Let $E|F$ be an unramified extension of non-archimedean local fields of characteristic 0. The corresponding residue fields are denoted by $\mathfrak{k}_E$ and $\mathfrak{k}_F$. Given $x \in \mathcal{O}_E$ we write $\overline{x}$ for the image in $\mathfrak{k}_E$. Write $n = [E\colon F]$. Prove that the norm map $\mathrm{Nr}_{E|F}\colon \mathcal{O}_E^\times \to \mathcal{O}_F^\times$ is surjective. One can argue as follows:

(1) Take $x \in \mathcal{O}_F$ and show that for $\overline{x} \in \mathfrak{k}_F$ there is $\overline{\alpha} \in \mathfrak{k}_E$ such that $\mathrm{Nr}_{\mathfrak{k}_E|\mathfrak{k}_F}(\overline{\alpha}) = \overline{x}$ and $\mathfrak{k}_E = \mathfrak{k}_F(\overline{\alpha})$.
(2) Argue as in (the proof of) Proposition 3.23 of the lecture (notes) that $E = F(\alpha)$ for a lift $\alpha \in \mathcal{O}_E$ of $\overline{\alpha}$.
(3) Conclude the proof by playing with the lift α to find a preimage of x under the norm map $\mathrm{Nr}_{E|F}$.

Sheet 4, Exercise 1: Let F be a non-archimedean local field. Recall that an infinite extension $E|F$ is called unramified if it is a union of finite unramified subextensions. Let F_{ur} be the composite of all unramified extensions of F (in $\overline{F}$). We call F_{ur} the maximal unramified extension of F.

(1) Let ζ be a primitive p^m-th root of unity. Show that the extension $\mathbb{Q}_p(\zeta)$ is totally ramified, in other words $e(\mathbb{Q}_p|\mathbb{Q}_p) = [\mathbb{Q}_p(\zeta)\colon \mathbb{Q}_p]$. (Hint: Look at the element $1-\zeta \in \mathbb{Z}_p[\zeta]$.)
(2) Show that the maximal unramified extension of $\mathbb{Q}_p$ is obtained by adjoining all roots of unity of order prime to p.
(3) Show that the maximal unramified extension of $\mathbb{F}_p((T))$ is[5]

$$\bigcup_{s\in\mathbb{N}} \mathbb{F}_{p^s}((T)) \subseteq \overline{\mathbb{F}}_p((T)).$$

Sheet 9, Exercise 4: Set $F = \mathbb{Q}_p$, write μ_{p^n} for the group of p^nth roots of unity and put $E = F(\mu_{p^n})$. Show that

$$N_{E|F}E^\times = U_F^n \times \langle p\rangle.$$

It can be used that the map $\exp\colon p^k\mathbb{Z}_p \to 1+p^k\mathbb{Z}_p$ (defined by the usual power series) is an isomorphism for $n \geq 1$ if p is odd and $n \geq 2$ if p is even.

4. Cohomology of finite Groups

We will now introduce the basic Cohomology theory for finite groups. Note that parts of this material were already discussed in Algebra 1. We will closely follow [4].

4.1. G-modules, group rings and basic definitions.

Let G be a finite group (written multiplicatively). A **G-module** A is an abelian group on which G operates so that

$$1a = a,\ \sigma(a+b) = \sigma a + \sigma b \text{ and } (\sigma\tau)a = \sigma(\tau a),$$

for $a, b \in A$ and $\sigma, \tau \in G$.

The basic example of a G-module is the **group ring** $\mathbb{Z}[G]$. It comes with the map, called **augmentation**,

$$\epsilon\colon \mathbb{Z}[G] \to \mathbb{Z},\ \sum_{\sigma\in G} n_\sigma\sigma \mapsto \sum_{\sigma\in G} n_\sigma.$$

The **augmentation ideal** is $I_G = \ker(\epsilon)$.

We call the element

$$N_G = \sum_{\sigma\in G} \sigma \in \mathbb{Z}[G]$$

the **norm** (sometimes also trace) of $\mathbb{Z}[G]$. With this element we define the co-augmentation by

$$\mu\colon \mathbb{Z} \to \mathbb{Z}[G], n \mapsto n\cdot N_G.$$

[5]This is [3, Chapter II, Section 9, Exercise 3]. However it seems that in loc. cit. the formulation is slightly inaccurate.

The image of this map defines an ideal and we set $J_G = \mathbb{Z}[G]/\mathbb{Z}\cdot N_G$. We get the two exact sequences

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0, \tag{4}$$
$$0 \to \mathbb{Z} \xrightarrow{\mu} \mathbb{Z}[G] \to J_G \to 0.$$

of rings.

Lemma 4.1. *As group I_G is the free abelian group generated by $\{\sigma - 1 \colon \sigma \in G\backslash\{1\}\}$. Similarly J_G is the free abelian group generated by $\{\sigma \bmod \mathbb{Z}\cdot N_G \colon \sigma \neq 1\}$. We have*

$$\mathbb{Z}[G] \cong I_G \oplus \mathbb{Z} \cong J_G \oplus \mathbb{Z}.$$

Proof. The proof follows by observing that for $x = \sum_{\sigma\in G} n_\sigma\sigma \in \mathbb{Z}[G]$ we can write

$$x = \sum_{1\neq\sigma\in G} n_\sigma(\sigma - 1) + (\sum_{\sigma\in G} n_\sigma)1.$$

Similarly we have the unique decomposition

$$x = \sum_{1\neq\sigma\in G} (n_\sigma - n_1)\sigma + n_1 \cdot N_G.$$

□

Lemma 4.2. *We have $I_G = \mathrm{Ann}(\mathbb{Z}\cdot N_G)$ and $\mathbb{Z}\cdot N_G = \mathrm{Ann}(I_G)$.*

Proof. Let $x = \sum_{\sigma\in G} n_\sigma\sigma$. We compute

$$x \cdot N_G = \sum_{\sigma\in G} n_\sigma(\sigma \cdot N_G) = \left(\sum_{\sigma\in G} n_\sigma\right) \cdot N_G.$$

In particular, $x \cdot N_G = 0$ if and only if $\sum_{\sigma\in G} n_\sigma = 0$. This implies the first claim. The second claim is a similarly easy **exercise**. □

Definition 4.1. Let G be a finite group and A a G-module. We define the 4 submodules:

$$A^G = \{a \in A \colon \sigma a = a \text{ for all } \sigma \in G\},$$
$$N_G A = \{N_G a \colon a \in A\},$$
$${}_{N_G}A = \{a \in A \colon N_G a = 0\} \text{ and}$$
$$I_G A = \{\sum_{1\neq\sigma\in G} n_\sigma(\sigma a_\sigma - a_\sigma) \colon a_\sigma \in A\}.$$

We call A^G the **fixed group** of A and $N_G A$ the **norm group** of A.

Given G-modules A and B we turn $\mathrm{Hom}(A, B) = \mathrm{Hom}_{\mathbb{Z}}(A, B)$ into a G-module by setting

$$\sigma f = \sigma \circ f \circ \sigma^{-1} \text{ for } \sigma \in G \text{ and } f \in \mathrm{Hom}(A, B).$$

Note that $\mathrm{Hom}_G(A,B) = \mathrm{Hom}(A,B)^G$.

Similarly we turn $A \otimes B = A \otimes_{\mathbb{Z}} B$ into a G-module by setting

$$\sigma(a \otimes b) = \sigma a \otimes \sigma b \text{ for } a \in A,\ b \in B \text{ and } \sigma \in G.$$

Given two G-homomorphisms $A \xrightarrow{h} A'$ and $B \xrightarrow{g} B'$ we get

$$(h,g)\colon \mathrm{Hom}(A',B) \to \mathrm{Hom}(A,B'),\ f \mapsto g \circ f \circ h, \text{ and}$$
$$h \otimes g\colon A \otimes B \to A' \otimes B',\ a \otimes b \mapsto h(a) \otimes g(b).$$

Remark 4.3. Recall the definitions of **flat**, **injective** and **projective** G-modules. Note that in particular for free $\mathbb{Z}$-modules exactness of short exact sequences is preserved under taking Hom and tensor products: If

$$0 \to X \to Y \to Z \to 0$$

is a short exact sequence of free $\mathbb{Z}$-modules, then

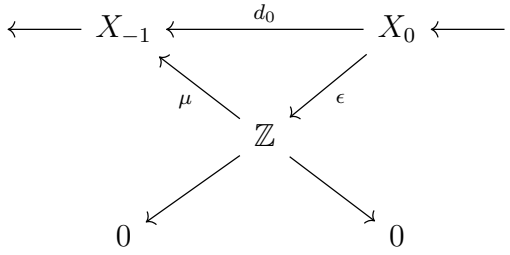
$$0 \to \mathrm{Hom}(A,X) \to \mathrm{Hom}(A,Y) \to \mathrm{Hom}(A,Z) \to 0,$$
$$0 \to \mathrm{Hom}(Z,A) \to \mathrm{Hom}(Y,A) \to \mathrm{Hom}(X,A) \to 0,$$
$$0 \to X \otimes A \to Y \otimes A \to Z \otimes A \to 0 \text{ and}$$
$$0 \to A \otimes X \to A \otimes Y \to A \otimes Z \to 0$$

are also exact.

Definition 4.2. Let G be a finite group. A **complete free resolution** of the (trivial) G-module $\mathbb{Z}$ is an exact sequence

$$\ldots \xleftarrow{d_{-2}} X_{-2} \xleftarrow{d_{-1}} X_{-1} \xleftarrow{d_0} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \xleftarrow{d_3} \ldots$$

of free G-modules X_q so that the diagram



commutes. (All the maps are G-homomorphisms.)

Remark 4.4. Note that a complete free resolution is indeed a combination of two free resolutions. Originally one serves for the definition of cohomology, while the other is used to define homology. However, connecting both makes the theory much more elegant.

Example 4.5. The following **standard resolution** is constructed based on ideas from algebraic topology.

We define $X_0 = X_{-1} = \mathbb{Z}[G]$ and

$$X_q = X_{-q-1} = \bigoplus_{(\sigma_1,\dots,\sigma_q)\in G^q} \mathbb{Z}[G]\cdot(\sigma_1,\dots,\sigma_q) \text{ for } q \geq 1.$$

These are by definition free. The G-homomorphisms ϵ and μ are now simply the previously introduced augmentation and co-augmentation maps. Furthermore, the G-homomorphisms d_q are defined on the (free) generators $(\sigma_1,\dots,\sigma_q)$ by setting

$d_0 1 = N_G$ and $d_1(\sigma) = \sigma - 1$,

$$d_q(\sigma_1,\dots,\sigma_q) = \sigma_1(\sigma_2,\dots,\sigma_q) + \sum_{i=1}^{q-1}(-1)^i(\sigma_1,\dots,\sigma_{i-1},\sigma_i\sigma_{i+1},\sigma_{i+2},\dots,\sigma_q) + (-1)^q(\sigma_1,\dots,\sigma_{q-1}) \text{ for } q > 1,$$

$$d_{-1}1 = \sum_{\sigma\in G}[\sigma^{-1}(\sigma) - (\sigma)] \text{ and}$$

$$d_{-q-1}(\sigma_1,\dots,\sigma_q) = \sum_{\sigma\in G}\sigma^{-1}(\sigma,\sigma_1,\dots,\sigma_q) + \sum_{\sigma\in G}\sum_{i=1}^{q}(-1)^i(\sigma_1,\dots,\sigma_{i-1},\sigma_i\sigma,\sigma^{-1},\sigma_{i+1},\dots,\sigma_q) + \sum_{\sigma\in G}(-1)^{q+1}(\sigma_1,\dots,\sigma_q,\sigma) \text{ for } -q-1 < -1.$$

Obviously we must have $d_0 = \mu\circ\epsilon$ ($\mu\circ\epsilon(1) = \mu(1) = N_G = d_0 1$). Thus we need to check exactness of the sequence $(X_q)_{q\in\mathbb{Z}}$. We first consider the right part

$$0 \longleftarrow \mathbb{Z} \xleftarrow{\epsilon} X_0 \xleftarrow{d_1} X_1 \xleftarrow{d_2} X_2 \xleftarrow{d_3} \dots$$

We define

$$E\colon \mathbb{Z}\to X_0,\ 1\mapsto 1,$$
$$D_0\colon X_0\to X_1,\ \sigma\mapsto(\sigma) \text{ and}$$
$$D_q\colon X_q\to X_{q+1},\ \sigma_0(\sigma_1,\dots,\sigma_q)\mapsto(\sigma_0,\dots,\sigma_q).$$

We check that

$$E\circ\epsilon + d_1\circ D_0 = \mathrm{Id} \text{ and } D_{q-1}\circ d_q + d_{q+1}\circ D_q = \mathrm{Id}.$$

This directly implies

$$\ker(\epsilon)\subseteq \mathrm{Im}(d_1) \text{ and } \ker(d_q)\subseteq \mathrm{Im}(d_{q+1}).$$

On the other hand one directly checks that $\epsilon\circ d_1 = 0$. This shows exactness at X_0. We continue by induction on q and show that $d_q\circ d_{q+1} = 0$. Note that

$$d_q = (D_{q-2}\circ d_{q-1} + d_q\circ D_{q-1})\circ d_q = d_q\circ D_{q-1}\circ d_q$$

by induction hypothesis ($d_{q-1}\circ d_q = 0$). On the other hand

$$d_q = d_q\circ(D_{q-1}\circ d_q + d_{q+1}\circ D_q) = d_q\circ D_{q-1}\circ d_q + d_q\circ d_{q+1}\circ D_q.$$

Substracting these two formulae gives

$$d_q \circ d_{q+1} \circ D_q = 0.$$

But each cell in X_{q+1} is in the image of D_q, so that $d_q \circ d_{q+1} = 0$ as claimed.

Note that we directly obtain the sequence

$$0 \longrightarrow \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \longrightarrow \mathrm{Hom}(X_0, \mathbb{Z}) \longrightarrow \mathrm{Hom}(X_1, \mathbb{Z}) \longrightarrow \dots$$

which is exact since we are dealing with free $\mathbb{Z}$-modules. Of course we have $\mathbb{Z} = \mathrm{Hom}(\mathbb{Z}, \mathbb{Z})$ and an elementary calculation shows that $X_{-q-1} = \mathrm{Hom}(X_q, \mathbb{Z})$ and that the maps d_{-q-1} arise naturally. Thus we get that the sequence

$$0 \to \mathbb{Z} \xrightarrow{\mu} X_{-1} \xrightarrow{d_{-1}} X_{-2} \xrightarrow{d_{-2}} X_{-3} \xrightarrow{d_{-3}} \dots$$

is exact. It remains to show the exactness at X_0, which is an elementary task.

We continue to work with the standard complex from the previous example. Let A be a G-module and define

$$A_q = \mathrm{Hom}_G(X_q, A).$$

The G-homomorphisms $x\colon X_q \to A$ are called q-**cochains** of A. We get the sequence

$$\dots \xrightarrow{\partial_{-2}} A_{-2} \xrightarrow{\partial_{-1}} A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \xrightarrow{\partial_2} A_2 \xrightarrow{\partial_3} \dots$$

Note that because $d_q \circ d_{q+1}$ we directly get $\partial_{q+1} \circ \partial_q = 0$ so that $\mathrm{Im}(\partial_q) \subseteq \ker(\partial_{q+1})$. We define

$$Z_q = \ker(\partial_{q+1}) \text{ and } R_q = \mathrm{Im}(\partial_q).$$

Elements in Z_q are called q-**cocycle**, while elements in R_q are q-**coboundaries**.

Definition 4.3. Let $q \in \mathbb{Z}$. We call

$$H^q(G, A) = Z_q / R_q$$

the q**th cohomology group** of the G-module A.

Remark 4.6. Note that the cohomology groups $H^{-q-1}(G, A)$ are precisely the classical homology groups usually denoted by $H_q(G, A)$. This unification of homology and cohomology goes back to J. Tate and will prove to be very useful.

We start by looking at the meaning of certain cohomology groups of small dimension. First observe that

$$A_0 = A_{-1} = \mathrm{Hom}_G(\mathbb{Z}[G], A) = A.$$

Furthermore

$$A_q = A_{-q-1} = \{x\colon G^q \to A\} \text{ for } q \geq 1.$$

Also the first couple of maps ∂_q of the standard complex are very simple:

$$\begin{aligned}\partial_{-1}(x) &= \sum_{\sigma\in G}(\sigma^{-1}x(\sigma) - x(\sigma)) \text{ for } x\colon G \to A,\\ \partial_0(x) &= N_G x \text{ for } x \in A \text{ and}\\ \partial_1(x) &= \sigma x - x \text{ for } x \in A.\end{aligned}$$

We obtain directly the following

- $Z_{-1} = \ker(\partial_0) = {}_{N_G}A$ and $R_{-1} = \mathrm{Im}(\partial_{-1}) = I_G A$. This gives
$$H^{-1}(G, A) = {}_{N_G}A/I_G A.$$
- $Z_0 = \ker(\partial_1) = A^G$ and $R_0 = \mathrm{Im}(\partial_0) = N_G A$. This gives
$$H^0(G, A) = A^G/N_G A,$$
which is the norm residue group of the G-module A.
- The 1-cocycles are functions $x\colon G \to A$ with $\partial_2 x = 0$ (i.e. $x(\sigma\tau) = \sigma x(\tau) + x(\sigma)$ for $\sigma, \tau \in G$). The 1-coboundaries are functions $x(\sigma) = \sigma a - a$ with fixed $a \in A$. Note that, if G operates trivially on A, then we have
$$H^1(G, A) = \mathrm{Hom}(G, A).$$

Remark 4.7. Let us consider the following situation. Given a short exact sequence

$$0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$$

of G-modules we obtain the related exact sequence

$$0 \to A^G \xrightarrow{i} B^G \xrightarrow{j} C^G.$$

Observe that by passing to the G-fixed modules we loose surjectivity of j. This can be explained as follows.

Take $x \in C^G$. Since j is surjective there is $b \in B$, so that $j(b) = c$. However, it is not clear that $b \in B^G$. The best we know is that

$$j(\sigma b - b) = \sigma(j(b)) - j(b) = \sigma c - c = 0.$$

In other words $\sigma b - b \in \ker(j)$ and by exactness $\sigma b - b \in \mathrm{Im}(i)$. Thus there is $a_\sigma \in A$ so that $i(a_\sigma) = \sigma b - b$. The map $\sigma \mapsto a_\sigma$ is a 1-cocycle with coefficients in A. Further note that the only choice we made was the choice of the pre-image b of c. Suppose there is another one: $j(b') = c$. Then we find another 1-cocycle a'_σ. The difference between a_σ and a'_σ is precisely a 1-coboundary. We conclude that we can associate to each $c \in C^G$ a unique cohomology class $\overline{a}_\sigma \in H^1(G, A)$. Note that $\overline{a}_\sigma = 0$ if we can choose $b \in B^G$ in the first place. In summary we have constructed a canonical homomorphism $C^G \xrightarrow{\delta} H^1(G, A)$ so that the sequence

$$0 \to A^G \xrightarrow{i} B^G \xrightarrow{j} C^G \xrightarrow{\delta} H^1(G, A).$$

is exact.

Remark 4.8. Let A be a (multiplicatively written) abelian group and let F be an arbitrary group. Our goal is to classify groups $\widehat{G}$ containing (up to isomorphism) A as a normal subgroup such that $G \cong \widehat{G}/A$.

First suppose there is such a $\widehat{G}$. For each $\sigma \in G$ take a pre-image $u_\sigma \in \widehat{G}$. In particular each element of $\widehat{G}$ can be written as

$$a \cdot u_\sigma \text{ with } a \in A,\ \sigma \in G.$$

By normality of A we have $u_\sigma \cdot a = a^\sigma u_\sigma$. This turns A into a G-module. (More precisely $a^\sigma = u_\sigma a u_\sigma^{-1}$.) We also write

$$u_\sigma u_\tau = x(\sigma,\tau) \cdot u_{\sigma\tau} \text{ for } x(\sigma,\tau) \in A.$$

We claim that $x(\sigma,\tau)$ is a 2-cocycle. To see this we first observe

$$\begin{aligned}(u_\sigma u_\tau)u_\rho &= x(\sigma,\tau)u_{\sigma\tau}u_\rho = x(\sigma,\tau)x(\sigma\tau,\rho)\cdot u_{\sigma\tau\rho}\\ &= u_\sigma(u_\tau u_\rho) = u_\sigma x(\tau,\rho)u_{\tau\rho} = x^\sigma(\tau,\rho)u_\sigma u_{\tau\rho} = x^\sigma(\tau,\rho)x(\sigma,\tau\rho)\cdot u_{\sigma\tau\rho}.\end{aligned}$$

Here we have only used associativity and the definitions. As a result we get

$$x(\sigma,\tau)x(\sigma\tau,\rho) = x^\sigma(\tau,\rho)x(\sigma,\tau\rho)$$

as desired.

Choosing different representatives u'_σ of $\widehat{G}/A$ we obtain a different system $x'(\sigma,\tau)$ of 2-cocycles. It is easy to check that these differ by the 2-coboundary $\partial_2(u'_\sigma u_\sigma^{-1})$.

In summary we have seen that an extension $\widehat{G}$ of G gives rise to a unique class in $H^2(G,A)$ given by $x(\sigma,\tau)$. Furthermore, the multiplication table of $\widehat{G}$ is uniquely determined by the system $x(\sigma,\tau)$.

On the contrary given an abelian group A and a homomorphism $h\colon G \to \mathrm{Aut}(A)$ we can turn A into a G-module by setting $\sigma a = h(\sigma)a$. (All G-module structures on A arise this way.) Taking $c \in H^2(G,A)$ will give us a solution $\widehat{G}$ to the extension problem as follows: We let $\widehat{G}$ be the group generated by elements u_σ for $\sigma \in G$ and $a \in A$ modulo the relations

$$a^\sigma = u_\sigma a u_\sigma^{-1} \text{ and } u_\sigma u_\tau = x(\sigma,\tau)u_{\sigma\tau},$$

where $x(\sigma,\tau)$ is a 2-cocycle in c. It is easy to verify that $\widehat{G}$ has the desired properties.

Sheet 4, Exercise 2: Let G be a pro-finite group and let A be a G-module. We endow A with the discrete topology. Show that the the following properties are equivalent:

(1) The action $G \times A \to A$ is continuous (where $G \times A$ carries the product topology);
(2) For every $a \in A$ the subgroup $G_a = \{g \in G\colon ga = a\}$ is open;
(3) We have $A = \bigcup_U A^U$ where U runs through open subgroups of G and $A^U = \{a \in A\colon ua = a \text{ for all } u \in U\}$.

(If G is a topological group, then one usually distinguishes abstract G-modules and topological G-modules. In the latter case A is a (Hausdorff) topological (abelian) group and the G-action is assumed to be continuous. The exercise characterizes those abstract G-modules which can be turned into topological G-modules by endowing them with the discrete topology.)

Sheet 4, Exercise 3: In this exercise we are trying to explain the genesis of the *standard complex*, which was introduced in the lecture in an ad-hoc way.

We start with the projections

$$d_i\colon G^{n+1} \to G^n,\ (\sigma_0, \dots, \hat{\sigma}_i, \dots, \sigma_n) \text{ for } i = 0, \dots, n.$$

Put $M^n(G, A) = \mathrm{Map}(G^{n+1}, A)$. This is a G-module with the action

$$[\sigma x](\sigma_0, \dots, \sigma_n) = \sigma[x(\sigma^{-1}\sigma_0, \dots, \sigma^{-1}\sigma_n)] \text{ where } x \in M^n(G, A).$$

We define the maps[6]

$$[\partial^n x](\sigma_0, \dots, \sigma_n) = \sum_{i=0}^{n} (-1)^i x(\sigma_0, \dots, \hat{\sigma}_i, \dots, \sigma_n).$$

from $M^{n-1}(G, A)$ to $M^n(G, A)$. One obtains an exact sequence

$$0 \to A \xrightarrow{\partial^0} M^0(G, A) \xrightarrow{\partial^1} M^1(G, A) \xrightarrow{\partial^2} M^2(G, A) \xrightarrow{\partial^3} \dots.$$

Passing to G-fixed maps we obtain the so called homogeneous cochains:

$$C^n(G, A) = M^n(G, A)^G = \{x\colon G^{n+1} \to A\colon \sigma x(\sigma_0, \dots, \sigma_n) = x(\sigma\sigma_0, \dots, \sigma\sigma_n)\}.$$

One obtains a complex

$$C^0(G, A) \xrightarrow{\partial^1} C^1(G, A) \xrightarrow{\partial^2} C^2(G, A) \xrightarrow{\partial^3} \dots$$

but exactness is lost in general. One attaches the cohomology groups

$$H^n(G, A) = \ker(\partial^{n+1})/\mathrm{Im}(\partial^n) \text{ for } n \geq 1.$$

These groups agree with the (Tate) cohomology groups defined in the lecture (for $n \geq 1$). To show this one executes the following exercises:

(1) Let $\mathcal{C}^0(G, A) = A$ and let $\mathcal{C}^n(G, A)$ be the abelian group of maps $G^n \to A$. Show that the map $r\colon C^n(G, A) \ni x \mapsto y \in \mathcal{C}^n(G, A)$ given by

$$y(\sigma_1, \dots, \sigma_n) = x(1, \sigma_1, \sigma_1\sigma_2, \dots, \sigma_1 \cdots \sigma_n)$$

is an isomorphism of abelian groups and compute its inverse.

(2) Write down the maps ∂_r^n that make the following diagram commute:

[6] This is a natural construction maybe familiar from algebraic topology. Indeed, the d_i's induce the maps $d_i^*\colon M^{n-1}(G, A) \to M^n(G, A)$. Then $\partial^n = \sum_{i=0}^{n} (-1)^i d_i^*$.

$$\begin{array}{ccc} C^{n-1}(G,A) & \xrightarrow{\partial^n} & C^n(G,A) \\ \downarrow{\scriptstyle r} & & \downarrow{\scriptstyle r} \\ \mathcal{C}^{n-1}(G,A) & \xrightarrow{\partial_r^n} & \mathcal{C}^n(G,A) \end{array}$$

(3) Use the computation from the exercise above to identify the complex

$$\mathcal{C}^0(G,A) \xrightarrow{\partial_r^1} \mathcal{C}^1(G,A) \xrightarrow{\partial_r^2} \mathcal{C}^2(G,A) \xrightarrow{\partial_r^3} \dots$$

with the complex $A_0 \to A_1 \to A_2 \to \dots$ from the lecture (notes).

Sheet 4, Exercise 4: A G-set X is simply a set with an G-action. (At the moment we do not include any topological considerations.) An A-Torsor is a G-set X with a simply transitive right-A-action,[7] which is compatible with the G-action.[8] We write $\mathrm{Tors}(A)$ for the set of all isomorphism classes of A torsors.

(1) Give an example of an A-torsor.
(2) Show that $H^1(G,A) \cong \mathrm{Tors}(A)$ as sets.

4.2. **The long exact sequence.** Let A and B be two G-modules together with a G-homomorphism $f\colon A \to B$. This canonically induces a homomorphism

$$\overline{f}_q\colon H^q(G,A) \to H^q(G,B)$$

constructed as follows. First,

$$x(\sigma_1,\dots,\sigma_q) \mapsto f(x(\sigma_1,\dots,\sigma_q)).$$

gives a homomorphism $f_q\colon A_q \to B_q$. Note that $\partial_{q+1} \circ f_q = f_{q+1} \circ \partial_{q+1}$ so that we get the commutative diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & A_q & \xrightarrow{\partial_{q+1}} & A_{q+1} & \longrightarrow & \cdots \\ & & \downarrow{\scriptstyle f_q} & & \downarrow{\scriptstyle f_{q+1}} & & \\ \cdots & \longrightarrow & B_q & \xrightarrow{\partial_{q+1}} & B_{q+1} & \longrightarrow & \cdots \end{array}$$

In particular, f_q induces the desired homomorphism $\overline{f}_q$.

Theorem 4.9. *Suppose $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules. Then there is a canonical homomorphism*

$$\delta_q\colon H^q(G,C) \to H^{q+1}(G,A)$$

called the connecting homomorphism (or also δ-homomorphism).

Proof. The construction is based on the snake lemma and was given in Algebra 1 (as an exercise). □

[7] A simply transitive right action is a map $X \times A \to X$, $(x,a) \mapsto xa$, such that for all $x,y \in X$ there is a unique $a \in A$ with $y = xa$.

[8] Compatibility means that $\sigma(xa) = \sigma(x)\sigma(a)$ holds for all $\sigma \in G$, $x \in X$ and all $a \in A$.

Theorem 4.10. *A short exact sequence*

$$0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$$

induces a long exact sequence

$$\ldots \to H^q(G,A) \xrightarrow{\bar{i}_q} H^q(G,B) \xrightarrow{\bar{j}_q} H^q(G,C) \xrightarrow{\delta_q} H^{q+1}(G,A) \to \ldots$$

Proof. Note that the relevant maps are given by

$$\begin{aligned}
&\bar{i}_q \colon [a_q] \mapsto [ia_q],\\
&\bar{j}_q \colon [b_q] \mapsto [jb_q] \text{ and}\\
&\delta_q \colon [c_q] \mapsto [a_{q+1}] \text{ with } [c_q] = [jb_q] \text{ and } [\partial b_q] = [ia_{q+1}].
\end{aligned}$$

We can directly read off that

$$\bar{j}_q \circ \bar{i}_q = \delta_q \circ \bar{j}_q = \bar{i}_{q+1} \circ \delta_q = 0.$$

This implies the inclusions

$$\mathrm{Im}(\bar{i}_q) \subseteq \ker(\bar{j}_q),\ \mathrm{Im}(\bar{j}_q) \subseteq \ker(\delta_q) \text{ and } \mathrm{Im}(\delta_q) \subseteq \ker(\bar{i}_{q+1}).$$

We compute the other inclusions by hand:

- Take $[b_q] \in \ker(\bar{j}_q)$. Thus we can write $jb_q = \partial c_{q-1}$ for some c_{q-1}. Choose b_{q-1} so that $jb_{q-1} = c_{q-1}$. Then $j(b_q - \partial b_{q-1}) = 0$. So we can assume that b_q is chosen so that $jb_q = 0$. But then there is a_q with $b_q = ia_q$. Since $i\partial a_q = \partial b_q = 0$ this a_q is a cocycle and we have $[b_q] = \bar{i}_q[a_q] \in \mathrm{Im}(\bar{i}_q)$. Thus we have $\mathrm{Im}(\bar{i}_q) \supseteq \ker(\bar{j}_q)$.
- Let $[c_q] \in \ker(\delta_q)$. Let a_{q+1} and b_q be so that $\delta_q[c_q] = [a_{q+1}] = 0$, $ia_{q+1} = \partial b_q$ and $c_q = jb_q$. Since $[a_{q+1}] = 0$ we have $a_{q+1} = \partial a_q$. One obtains $\partial(b_q - ia_q) = 0$ and $c_q = j(b_q - ia_q)$. This yields $[c_q] = \bar{j}_q[b_q - ia_q]$ so that $\mathrm{Im}(\bar{j}_q) \supseteq \ker(\delta_q)$.
- Let $[a_{q+1}] \in \ker(\bar{i}_{q+1})$, so that $ia_{q+1} = \partial b_q$ for some b_q. Put $c_q = jb_q$. Observe that $\partial c_q = \partial jb_q = j\partial b_q = jia_{q+1} = 0$. Thus c_q is a cocycle and $[a_{q+1}] = \delta_q[c_q] \in \mathrm{Im}(\delta_q)$. We have seen that $\mathrm{Im}(\delta_q) \supseteq \ker(\bar{i}_{q+1})$.

This completes the proof of exactness. ∎

Theorem 4.11. *Suppose* $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ *is exact then we obtain the exact sequence*

$$0 \to A^G \to B^G \to C^G \to H^1(G,A) \to H^1(G,B) \to \ldots.$$

Proof. Note that we have explicitly constructed the map $C^G \to H^1(G,A)$ in Remark 4.7.

The homomorphism $\delta \colon C^G \to H^1(G,A)$ is given by

$$C^G \to C^G/N_G C = H^0(G,C) \xrightarrow{\delta_0} H^1(G,A).$$

Obviously we only need to check exactness at C^G. Take $c \in \mathrm{Im}(j|_{B^G})$. Thus $c = j(b)$ with $b \in B^G$ and we get

$$\delta c = \delta_0(c + N_G C) = \delta_0(jb + N_G C) = \delta_0 \overline{j}_0(b + N_G B) = 0.$$

In particular, $\mathrm{Im}(j|_{B^G}) \subseteq \ker(\delta)$.

On the other hand if $c \in \ker(\delta)$, this means $c \in C^G$ and $\delta c = \delta_0(c + N_G C) = 0$. Then we have

$$c + N_G C = \overline{j}_0(b + N_G B) = jb + N_G C.$$

Thus $c = jb + N_G c'$. Choose $b' \in B$ with $jb' = c'$. Then we have $c = jb + N_G(jb') = jb + jN_G b' \in j(B^G)$. Thus $\mathrm{Im}(j) = \ker(\delta)$ and we are done. ∎

Theorem 4.12. *Let*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{j} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' & \longrightarrow & 0 \end{array}$$

be a commutative diagram of G-modules with exact rows. Then the diagram

$$\begin{array}{ccc} H^q(G, C) & \xrightarrow{\delta_q} & H^{q+1}(G, A) \\ \downarrow{\scriptstyle \overline{h}_q} & & \downarrow{\scriptstyle \overline{f}_{q+1}} \\ H^q(G, C') & \xrightarrow{\delta_q} & H^{q+1}(G, A') \end{array}$$

is commutative.

Proof. We need to show that $\overline{f}_{q+1} \circ \delta_q = \delta_q \circ \overline{h}_q$. To do so we only need to use the definition of δ_q. Take $[c_q] \in H^q(G, C)$. We pick g_q and a_{q+1} so that $c_q = jb_q$ and $ia_{q+1} = \partial b_q$. Then $\delta_q[c_q] = [a_{q+1}]$ and we have

$$(\overline{f}_{q+1} \circ \delta_q)[c_q] = \overline{f}_{q+1}[a_{q+1}] = [fa_{q+1}].$$

Next put $c'_q = hc_q$, $b'_q = gb_q$ and $a'_{q+1} = fa_{q+1}$. We deduce that $c'_q = j'b'_q$ and $\partial b'_q = i'a'_{q+1}$. As a result we have $(\delta_q \circ \overline{h}_q)[c_q] = \delta_q[c'_q] = [fa_{q+1}]$. This completes the proof. ∎

Theorem 4.13. *Given the commutative diagram*

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & C' & \longrightarrow & C & \longrightarrow & C'' & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

of G-modules with exact rows and columns, we have the corresponding commutative diagram

$$\begin{array}{ccc}
H^{q-1}(G, C'') & \xrightarrow{\delta} & H^q(G, C') \\
\downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle -\delta} \\
H^q(G, A'') & \xrightarrow{\delta} & H^{q+1}(G, A')
\end{array}$$

Proof. Let D be the kernel of the composition $B \to C \to C''$. We define

- $i\colon A' \to A \oplus B'$ by setting $ia' = (a, b')$ where $A' \ni a' \mapsto a \in A$ and $A' \ni a' \mapsto b' \in B'$.
- $j\colon A \oplus B' \to D$ by $d(a, b') = d_1 - d_2$ where $A \ni a \mapsto d_1 \in D \subseteq B$ and $B' \ni b' \mapsto d_2 \in D$.

We obtain the exact sequence

$$0 \to A' \xrightarrow{i} A \oplus B' \xrightarrow{j} D \to 0$$

and the commutative diagram

$$\begin{array}{ccccccccc}
A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & B'' & \longrightarrow & C'' \\
\uparrow{\scriptstyle \mathrm{Id}} & & \uparrow{\scriptstyle \mathrm{Id}\oplus 0} & & \vdots & & \uparrow & & \uparrow{\scriptstyle \mathrm{Id}} \\
A' & \xrightarrow{i} & A \oplus B' & \xrightarrow{j} & D & \longrightarrow & B & \longrightarrow & C'' \\
\downarrow{\scriptstyle -\mathrm{Id}} & & \downarrow{\scriptstyle 0\oplus(-\mathrm{Id})} & & \vdots & & \downarrow & & \downarrow{\scriptstyle \mathrm{Id}} \\
A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & C & \longrightarrow & C''
\end{array}$$

The dotted arrows stand for G-homomorphisms that can be added to the diagram without destroying its commutativity. Indeed $\mathrm{Im}(D \to B'') \subseteq \mathrm{Im}(A'' \to B'')$ and $A'' \to B''$ is injective (resp. $\mathrm{Im}(D \to C) \subseteq \mathrm{Im}(C' \to C)$ and $C' \to C$ is injective). By using the previous theorem we obtain

$$\begin{array}{ccccc}
H^{q-1}(G,C'') & \xrightarrow{\delta} & H^q(G,A'') & \xrightarrow{\delta} & H^{q+1}(G,A') \\
{\scriptstyle \mathrm{Id}}\uparrow & & \uparrow & & \uparrow{\scriptstyle \mathrm{Id}} \\
H^{q-1}(G,C'') & \xrightarrow{\delta} & H^q(G,D) & \xrightarrow{\delta} & H^{q+1}(G,A') \\
\downarrow{\scriptstyle \mathrm{Id}} & & \downarrow & & \downarrow{\scriptstyle -\mathrm{Id}} \\
H^{q-1}(G,C'') & \xrightarrow{\delta} & H^q(G,C') & \xrightarrow{\delta} & H^{q+1}(G,A')
\end{array}$$

and the proof is complete. □

Theorem 4.14. *Let $\{A_i : i \in I\}$ be a family of G-modules. Then we have*

$$H^q(G, \bigoplus_i A_i) \cong \bigoplus H^q(G, A_i) \text{ and}$$
$$H^q(G, \prod_i A_i) \cong \prod_i H^q(G, A_i).$$

Proof. We only proof the first statement, since the second one follows from essentially the same argument.

Put $A = \oplus_i A_i$. We have

$$A_q = \mathrm{Hom}_G(X_q, A) \cong \bigoplus \mathrm{Hom}_G(X_q, A_i) = \bigoplus_i (A_i)_q.$$

This leads to the diagram

$$\begin{array}{ccccccc}
\ldots & \longrightarrow & A_{q-1} & \xrightarrow{\partial} & A_q & \longrightarrow & \ldots \\
 & & \downarrow{\scriptstyle \cong} & & \downarrow{\scriptstyle \cong} & & \\
\ldots & \longrightarrow & \bigoplus_i (A_i)_{q-1} & \xrightarrow{\partial} & \bigoplus_i (A_i)_q & \longrightarrow & \ldots
\end{array}$$

which yields the desired isomorphisms. □

4.3. **Induced Modules and dimension shift.**

Definition 4.4. A G-module A is called G-induced, if it can be represented as $A = \sum_{\sigma \in G} \sigma D$ for a subgroup $D \subseteq A$.

The easiest example of an G-induced G-module is the group ring $\mathbb{Z}[G]$. In general G-induced G-modules are of the form $\mathbb{Z}[G] \otimes D$ for arbitrary abelian groups D.

Lemma 4.15. *Let A be a G-module and let X be a G-induced module. Suppose $H \subseteq G$ is a subgroup.*

1. *$X \otimes A$ is a G-induced module.*
2. *X is a H-induced H-module.*
3. *If H is normal in G, then X^H is a G/H-induced G/H-module.*

Proof. To verify (1) is straight forward. To see (2) we write $X = \oplus_{\sigma\in G}\sigma D$ and modify this to get

$$X = \bigoplus_{h\in H}\bigoplus_{\sigma} h\sigma D = \bigoplus_{h\in H} h\left[\bigoplus_{\sigma}\sigma D\right].$$

Finally we turn to (3). We claim that

$$X^H = \bigoplus_{\tau\in G/H} \tau N_H D.$$

Obviously this is a direct sum and contained in X^H (since $N_H D \subseteq X^H$). Now take $x \in X^H$. By assumption we have a unique representation

$$x = \sum_{\tau\in G}\tau d_\tau.$$

Applying $\sigma^{-1} \in H$ has the effect

$$x = \sigma^{-1}x = \sum_{\tau\in G}\sigma^{-1}\tau d_\tau = \sum_{\tau\in G}\tau d_{\sigma\tau}.$$

We obtain $d_\tau = d_{\sigma\tau}$. With this at hand we get

$$x = \sum_{\tau}\sum_{\sigma\in H}\tau\sigma d_{\tau\sigma} = \sum_{\tau}\tau\left(\sum_{\sigma\in H}\sigma d_\tau\right) = \sum_{\tau}\tau N_H(d_\tau),$$

as desired. ∎

Definition 4.5. We say that a G-module A has trivial cohomology if $H^q(H, A) = 0$ for all q and for all subgroups H of G.

The following theorem turns the notion of G-induced modules into a powerful tool.

Theorem 4.16. *Every G-induced module A has trivial cohomology.*

Proof. It suffices to show that $H^q(G, A) = 0$ for all q. In other words, we need to see that

$$\ldots \to \mathrm{Hom}_G(X_q, A) \xrightarrow{\partial} \mathrm{Hom}_G(X_{q+1}, A) \to \ldots$$

is exact. To see this we write $A = \oplus_\sigma \sigma D$ and let $\pi\colon A \to D$ be the natural projection. We get a bijection

$$\mathrm{Hom}_G(X_q, A) \to \mathrm{Hom}_{\mathbb{Z}}(X_q, D),\ f \mapsto \pi \circ f.$$

With this identification we obtain the sequence

$$\ldots \to \mathrm{Hom}_{\mathbb{Z}}(X_q, D) \to \mathrm{Hom}_{\mathbb{Z}}(X_{q+1}, D) \to \ldots$$

which we know to be exact, since the X_q's are free $\mathbb{Z}$-modules. ∎

Recall the exact sequences from (4). From these we obtain the exact sequences

$$0 \to I_G \otimes A \to \mathbb{Z}[G] \otimes A \to A \to 0,$$
$$0 \to A \to \mathbb{Z}[G] \otimes A \to J_G \otimes A \to 0.$$

for each G-module A. Note that $\mathbb{Z}[G] \otimes A$ is now G-induced and thus cohomologically trivial. Applying the lonng exact cohomological sequence yields isomorphisms

$$\delta \colon H^{q-1}(H, J_G \otimes A) \to H^q(H, A) \text{ and } \delta^{-1} \colon H^{q+1}(H, I_G \otimes A) \to H^q(H, A),$$

for each subgroup $H \subseteq G$. We will iterate this process as follows. Define

$$A^m = \underbrace{J_G \otimes \ldots \otimes J_G}_{m-\text{times}} \otimes A \text{ for } m \geq 0$$

and

$$A^m = \underbrace{I_G \otimes \ldots \otimes I_G}_{|m|-\text{times}} \otimes A \text{ for } m \leq 0.$$

Iteration of δ (or δ^{-1}) yields isomorphisms

$$\delta^m \colon H^{q-m}(H, A^m) \to H^q(H, A).$$

This method is known as dimension shifting. Due to its great importance we will reformulate it as a theorem.

Theorem 4.17. *For each q and each subgroup $H \subseteq G$ iteration of the connection homomorphism δ yields the isomorphism*

$$\delta^m \colon H^{q-m}(H, A^m) \to H^q(H, A).$$

We will end this section by deriving some very important applications of this theorem.

Theorem 4.18. *The groups $H^q(G, A)$ are torsion groups. More precisely, the orders of the elements of $H^q(G, A)$ divide the order of G.*

Proof. Let $n = \sharp G$. Since $H^0(G, A) = A^G / N_G A$ and $na = N_G a$ for all $a \in A^G$, we have $n \cdot H^0(G, A) = \{0\}$. This holds for any G-module A and the general case follows by dimension shifting since $H^q(G, A) \cong H^0(G, A^q)$. ∎

We say an abelian group A has unique unlimited division if the equation $nx = a$ has a unique solution for each $a \in A$ and each $n \in \mathbb{N}$.

Corollary 4.19. *If a G-module A has unique unlimited division (as abelian group), then it has trivial cohomology.*

Proof. This is Sheet 5, Exercise 1 stated below. ∎

We can now compute two important Cohomology groups.

Corollary 4.20. *We have*

$$H^2(G,\mathbb{Z}) \cong H^1(G,\mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}).$$

We write $\chi(G) = \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ *and call this the character group of* G.

Proof. This is Sheet 5, Exercise 1 stated below. ∎

Let G' be the commutator group of G. Then we set $G^{\mathrm{ab}} = G/G'$.

Theorem 4.21. *We have*

$$H^{-2}(G,\mathbb{Z}) \cong G^{\mathrm{ab}}.$$

Proof. Recall that $\mathbb{Z}[G]$ has trivial cohomology (since it is G-induced). Considering the exact sequence

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

we obtain the isomorphism

$$\delta\colon H^{-2}(G,\mathbb{Z}) \to H^{-1}(G,I_G).$$

We recognize $H^{-1}(G,I_G) = I_G/I_G^2$. Thus we need to find an isomorphism between G/G' and I_G/I_G^2.

We consider the map

$$G \to I_G/I_G^2,\ \sigma \mapsto (\sigma-1) + I_G^2.$$

To see that this is a homomorphism we compute

$$\sigma\tau - 1 = (\sigma-1) + (\tau-1) + \underbrace{(\sigma-1)\cdot(\tau-1)}_{\in I_G^2}.$$

Because I_G is abelian, the kernel of this map must contain the commutator subgroup G'. We therefore obtain the map

$$\log\colon G/G' \to I_G/I_G^2.$$

Since I_G has the free generators $(\sigma-1)$ for $\sigma \in G$ we can define a homomorphism $I_G \to G/G'$ by $(\sigma-1) \mapsto \sigma\cdot G'$. Compute

$$(\sigma-1)(\tau-1) = (\sigma\tau-1) - (\sigma-1) - (\tau-1) \mapsto \sigma\tau\sigma^{-1}\tau^{-1}G' = G'.$$

to see that the elements $(\sigma-1)(\tau-1)$ are contained in the kernel of this map. We obtain the homomorphism

$$\exp\colon I_G/I_G^2 \to G/G',\ (\sigma-1)+I_G^2 \mapsto \sigma G'.$$

Obviously we have $\log\circ\exp = \mathrm{Id} = \exp\circ\log$ giving the desired isomorphism. ∎

We have now computed the 5 cohomology groups

$$\begin{aligned} H^{-2}(G,\mathbb{Z}) &\cong G^{\mathrm{ab}}, \\ H^{-1}(G,\mathbb{Z}) &= 0, \\ H^{0}(G,\mathbb{Z}) &= \mathbb{Z}/n\mathbb{Z}, \\ H^{1}(G,\mathbb{Z}) &= 0 \text{ and} \\ H^{2}(G,\mathbb{Z}) &= \chi(G). \end{aligned}$$

Remark 4.22. In general we have the duality principle

$$H^{-q}(G,\mathbb{Z}) \cong \chi(H^q(G,\mathbb{Z})) \text{ for all } q > 0.$$

Since we will not need this we omit the proof.

Sheet 5, Exercise 1: An abelian group A is said to have unique unlimited division if the equation $nx = a$ has a unique solution $x \in A$ for each $a \in A$ and each $n \in \mathbb{N}$.

(1) Give an example of an abelian group A with unique unlimited division.
(2) Show that a G-module A which has unique unlimited division (as abelian group) has trivial cohomology.
(3) Show that $H^2(G,\mathbb{Z}) = \chi(G)$, where G acts trivially on $\mathbb{Z}$ and the character group $\chi(G)$ is defined as $\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$.

4.4. **Inflation, Restriction, Corestriction.** We start by considering $q > 0$. Recall that if $H \subseteq G$ is normal, then A^H is a G/H-module.

Suppose $H \subset G$ is normal, then we can take a q-cochain

$$x\colon G/H \times \cdots \times G/H \to A^H$$

and associate a q-cochain $y\colon G \times \cdots \times G \to A$ by

$$y(\sigma_1,\ldots,\sigma_q) = x(\sigma_1 \cdot H,\ldots,\sigma_q \cdot H).$$

We call this the inflation of x and write

$$y = \mathrm{Inf}x.$$

It is easy to see that $\partial_{q+1} \circ \mathrm{Inf} = \mathrm{Inf} \circ \partial_{q+1}$. This makes the following definition possible.

Definition 4.6. Let A be a G-module and $H \subseteq G$ be a normal subgroup of G. For $q \geq 1$, we call the homomorphism

$$\mathrm{Inf}_q\colon H^q(G/H, A^H) \to H^q(G,A)$$

inflation.

The other obvious operation on cochains is restriction. Taking $x\colon G \times \cdots \times G \to A$ we write $\mathrm{Res}x\colon H \times \cdots \times H \to A$. Again one observes that this operator commutes with the operator ∂.

Definition 4.7. Let A be a G-module and $H \subseteq G$ be a subgroup of G. For $q \geq 1$, we call the homomorphism

$$\mathrm{Res}_q \colon H^q(G, A) \to H^q(H, A)$$

restriction.

The following three theorems show that these two new maps are compatible with the canonical homomorphisms encountered previously. The proofs are omitted, since they are easy Exercises. (See Sheet 5, Exercise 2 below.)

Theorem 4.23. *Let A and B be two G-modules, $H \subseteq G$ be a normal subgroup of G and let $f \colon A \to B$ be a G-homomorphism. Then the diagrams*

$$\begin{array}{ccc} H^q(G/H, A^H) & \xrightarrow{\overline{f}} & H^q(G/H, B^H) \\ \downarrow{\scriptstyle \mathrm{Inf}_q} & & \downarrow{\scriptstyle \mathrm{Inf}_q} \\ H^q(G, A) & \xrightarrow{\overline{f}} & H^q(G, B) \end{array} \qquad \begin{array}{ccc} H^q(G, A) & \xrightarrow{\overline{f}} & H^q(G, B) \\ \downarrow{\scriptstyle \mathrm{Res}_q} & & \downarrow{\scriptstyle \mathrm{Res}_q} \\ H^q(H, A) & \xrightarrow{\overline{f}} & H^q(H, B) \end{array}$$

commute.

Theorem 4.24. *Consider a short exact sequence*

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

of G-modules and let $H \subseteq G$ be a normal subgroup. If

$$0 \to A^H \to B^H \to C^H \to 0$$

is also exact, then the diagram

$$\begin{array}{ccc} H^q(G/H, C^H) & \xrightarrow{\delta} & H^{q+1}(G/H, A^H) \\ \downarrow{\scriptstyle \mathrm{Inf}_q} & & \downarrow{\scriptstyle \mathrm{Inf}_{q+1}} \\ H^q(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \end{array}$$

commutes

Theorem 4.25. *Let*

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

be a short exact sequence of G-modules and let $H \subseteq G$ be a subgroup. Then the diagram

$$\begin{array}{ccc} H^q(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \\ \downarrow{\scriptstyle \mathrm{Res}_q} & & \downarrow{\scriptstyle \mathrm{Res}_{q+1}} \\ H^q(H, C) & \xrightarrow{\delta} & H^{q+1}(H, A) \end{array}$$

commutes.

Combining inflation and restriction yields the following result.

Theorem 4.26. *Let A be a G-module and $H \subseteq G$ be a normal subgroup. Then the sequence*

$$0 \to H^1(G/H, A^H) \overset{\mathrm{Inf}_1}{\to} H^1(G, A) \overset{\mathrm{Res}_1}{\to} H^1(H, A)$$

is exact.

Proof. We first show that inflation is injective. Take a 1-cocycle $x\colon G/H \to A^H$, so that $\mathrm{Inf}(x)$ is a 1-coboundary. Then we have

$$[\mathrm{Inf}(x)](\sigma) = x(\sigma \cdot H) = \sigma a - a$$

for $a \in A$. Thus for all $\tau \in H$ we must have $\sigma a - a = \sigma\tau a - a$ so that $a = \tau a$ and therefore $a \in A^H$. We conclude that x must have been a 1-coboundary.

We turn to exactness at $H^1(G, A)$. Take a 1-cocycle $x\colon G/H \to A^H$ of A^H. Then, for $\sigma \in H$, we have

$$[\mathrm{Res} \circ \mathrm{Inf}x](\sigma) = [\mathrm{Inf}x](\sigma) = x(\sigma \cdot H) = x(H) = x([1]).$$

Obviously we have $x([1]) = 0$. We have seen that

$$\mathrm{Im}(\mathrm{Inf}_1) \subseteq \ker(\mathrm{Res}_1).$$

On the other hand we take a 1-cocycle $x\colon G \to A$ of the G-module A, whose restriction to H is a 1-coboundary of A. This means

$$x(\tau) = \tau a - a$$

with $a \in A$ and for all $\tau \in H$. Let $\rho\colon G \to A$ be the 1-coboundary $\rho(\sigma) = \sigma a - a$. Then the difference $x' = x - \rho$ is a 1-cocycle in the same cohomology class as x. Furthermore $x'(\tau) = 0$ for all $\tau \in H$. We see that

$$x'(\sigma\tau) = x'(\sigma) + \sigma x'(\tau) = x'(\sigma) \text{ and } x'(\tau \cdot \sigma) = x'(\tau) + \tau x'(\sigma) = \tau x'(\sigma),$$

for all $\tau \in H$. Define $y\colon G/H \to A$ by $y(\sigma H) = x'(\sigma)$. By the observation above this is well defined 1-cocycle with image in A^H and $\mathrm{Inf}y = x'$. This implies $\ker \mathrm{Res} \subseteq \mathrm{Im}\mathrm{Inf}$ and we are done. ∎

This can be extended to $q > 1$ only under some conditions.

Theorem 4.27. *Let A be a G-module and $H \subseteq G$ be a normal subgroup of G. If $H^i(H, A) = 0$ for $i = 1, \ldots, q-1$ and $q \geq 1$, then*

$$0 \to H^q(G/H, A^H) \overset{\mathrm{Inf}}{\to} H^q(G, A) \overset{\mathrm{Res}}{\to} H^q(H, A)$$

is exact.

Proof. The proof is via induction and dimension shifting. The case $q = 1$ was treated above. Put $B = \mathbb{Z}[G] \otimes A$ and $C = J_G \otimes A$, so that we have the exact sequence

$$0 \to A \to B \to C \to 0.$$

Since $H^1(H, A) = 0$ also

$$0 \to A^H \to B^H \to C^H \to 0$$

is exact. This gives the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^{q-1}(G/H, C^H) & \xrightarrow{\text{Inf}} & H^{q-1}(G, C) & \xrightarrow{\text{Res}} & H^{q-1}(H, C) \\ & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} \\ 0 & \longrightarrow & H^{q}(G/H, A^H) & \xrightarrow{\text{Inf}} & H^{q}(G, A) & \xrightarrow{\text{Res}} & H^{q}(H, A) \end{array}$$

Note that B is G-induced and B^H is G/H-induced. This implies that the maps δ are isomorphisms. Furthermore we have

$$H^i(H, C) \cong H^{i+1}(H, A) = 0 \text{ for } i = 1, \dots, q-2.$$

With this additional information the diagram above makes the induction step work. □

Next we want to obtain a reasonable definition of inflation and restriction for $q \leq 0$. We start with the following simple observation.

The assignment

$$a + N_G A \mapsto a + N_H A,\ a \in A^G \subseteq A^H$$

yields a homomorphism

$$\text{Res}_0 \colon H^0(G, A) = A^G/N_G A \to H^0(H, A) = A^H/N_H A.$$

The next lemma establishes that this restriction has the desired properties.

Lemma 4.28. *Let $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ be an exact sequence of G-modules. Further let $H \subseteq G$ be a subgroup of G. Then*

$$\begin{array}{ccc} H^0(G, C) & \xrightarrow{\delta} & H^1(G, A) \\ \downarrow{\scriptstyle \text{Res}_0} & & \downarrow{\scriptstyle \text{Res}_1} \\ H^0(H, C) & \xrightarrow{\delta} & H^1(H, A) \end{array}$$

is commutative.

Proof. Let $c \in C^G$ be a 0-cocycle of the G-module C. Put $[c] = c + N_G C$. This is the corresponding homology class. Note that by definition $\text{Res}_0([c]) = c + N_H C$. Choose $b \in B$ such that $jb = c$, then there is a 1-cocylce $a_1 \colon G \to A$ so that $ia_1 = \partial b$. (This is because $j\partial b = \partial c = 0$ and exactness.) By definition we have $\delta([c]) = [a_1]$ and

$$\delta \text{Res}_0([c]) = [\text{Res}_1(a_1)] = \text{Res}_1([a_1]) = \text{Res}_1 \delta([c]).$$

□

In general there is not such a nice and elementary definition of the restriction maps. However, we have the following axiomatic definition:

Definition 4.8 (and Lemma)**.** Let G be a finite group with a subgroup $H \subseteq G$. Restriction is the uniquely determined family of homomorphisms

$$\mathrm{Res}_q \colon H^q(G, A) \to H^q(H, A) \text{ for } q \in \mathbb{Z},$$

with the properties

(1) $\mathrm{Res}_0 \colon H^0(G, A) \to H^0(H, A)$ is given by $a + N_G A \mapsto a + N_H A$ for $a \in A^G$.
(2) For every exact sequence $0 \to A \to B \to C \to 0$ of G-modules the diagram

$$\begin{array}{ccc} H^q(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \\ \downarrow{\scriptstyle \mathrm{Res}_q} & & \downarrow{\scriptstyle \mathrm{Res}_{q+1}} \\ H^q(H, C) & \xrightarrow{\delta} & H^{q+1}(H, A) \end{array}$$

is commutative.

Proof. We should show that restriction exists and that it is indeed unique.

The definition of restriction goes through the commutative diagram

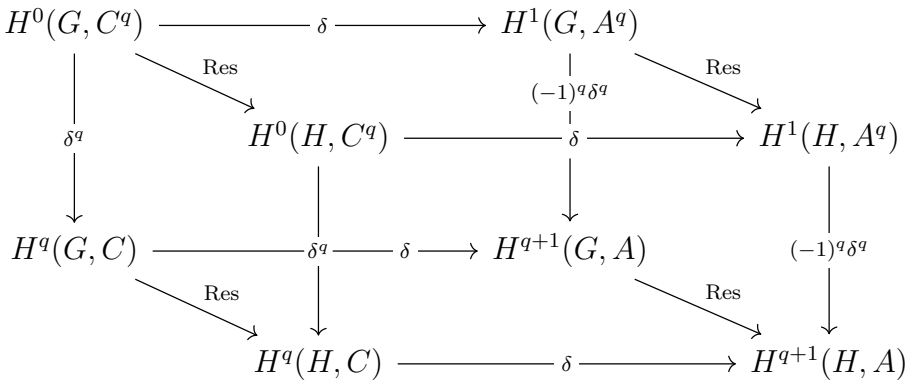
$$\begin{array}{ccc} H^0(G, A^q) & \xrightarrow{\delta^q} & H^q(G, A) \\ \downarrow{\scriptstyle \mathrm{Res}_0} & & \downarrow{\scriptstyle \mathrm{Res}_q} \\ H^0(H, A^q) & \xrightarrow{\delta^q} & H^q(H, A) \end{array}$$

where

$$\delta^q \colon H^0(G, A^q) \to H^q(G, A) \text{ and } \delta^q \colon H^0(H, A^q) \to H^q(H, A)$$

are isomorphisms defined by q applications of the connecting homomorphism δ. The same diagram shows uniqueness. In particular for $q \geq 0$ we get the maps introduced earlier.

We still need to check the second property. Consider the diagram



Here we use exactness of $0 \to A \to B \to C \to 0$ to deduce exactness of $0 \to A^q \to B^q \to C^q \to 0$ via induction. Earlier we shew that the upper square is commutative. The sides commute by definition of Restriction. The front and the

back square are also commutative. This forces the bottom square to be commutative, which is exactly what we want. ◻

Definition 4.9. The map $G^{\mathrm{ab}} \to H^{\mathrm{ab}}$ induced by

$$\mathrm{Res}_{-2}\colon H^{-2}(G,\mathbb{Z}) \to H^{-2}(H,\mathbb{Z})$$

is called *Verlagerung* (also transfer) and is denoted by Ver.

Next we define the co-restriction

$$\mathrm{CoRes}_q\colon H^q(H,A) \to H^q(G,A).$$

For $q=-1$ we define this map via

$$a + I_H A \mapsto a + I_G A \text{ for } a \in {}_{N_H}A \subseteq {}_{N_G}A.$$

For $q=0$ we have obtain it from[9]

$$a + N_H A \mapsto N_{G/H} a + N_G A \text{ for } a \in A^H.$$

From this direct definitions it is straight forward to verify

Lemma 4.29. *Let $0 \to A \to B \to C \to 0$ be an exact sequence of G-modules. Then*

$$\begin{array}{ccc} H^{-1}(H,C) & \xrightarrow{\delta} & H^0(H,A) \\ \downarrow{\scriptstyle \mathrm{CoRes}_{-1}} & & \downarrow{\scriptstyle \mathrm{CoRes}_0} \\ H^{-1}(G,C) & \xrightarrow{\delta} & H^0(G,A) \end{array}$$

is commutative.

Proof. **Exercise.** ◻

Definition 4.10 (and Lemma)**.** Let G be a finite group with subgroup $H \subseteq G$. The Co-Restriction is the uniquely determined family of homomorphisms

$$\mathrm{CoRes}_q\colon H^q(H,A) \to H^q(G,A) \text{ for } q \in \mathbb{Z}$$

satisfying

(1) CoRes_0 is defined by $a + N_H A \mapsto N_{G/H} a + N_G A$ for $a \in A^H$.
(2) For each exact sequence $0 \to A \to B \to C \to 0$ the diagram

$$\begin{array}{ccc} H^q(H,C) & \xrightarrow{\delta} & H^{q+1}(H,A) \\ \downarrow{\scriptstyle \mathrm{CoRes}_q} & & \downarrow{\scriptstyle \mathrm{CoRes}_{q+1}} \\ H^q(G,C) & \xrightarrow{\delta} & H^{q+1}(G,A) \end{array}$$

is commutative.

Proof. See Sheet 6, Exercise 2 below. ◻

[9] Even though G/H is not necessarily a group we define $N_{G/H}$ simply as the sum over a system of representatives for G/H. Since a is H-fixed the choice is irrelevant.

Theorem 4.30. *The map* $\kappa\colon H^{\mathrm{ab}} \to G^{\mathrm{ab}}$ *induced by*

$$\mathrm{CoRes}_{-2}\colon H^{-2}(H,\mathbb{Z}) \to H^{-2}(G,\mathbb{Z})$$

is the canonical homomorphism given by $\sigma H' \mapsto \sigma G'$.

Proof. This follows from the diagram

$$\begin{array}{ccccc} H^{-2}(H,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(H,I_H) & -\!=\!\to & I_H/I_H^2 \xleftarrow[\log]{} H^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{CoRes}_{-2}} & & \downarrow{\scriptstyle \mathrm{CoRes}_{-1}} & & \downarrow{\scriptstyle \kappa} \\ H^{-2}(G,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(G,I_G) & -\!=\!\to & I_G/I_G^2 \xleftarrow[\log]{} G^{\mathrm{ab}} \end{array}$$

□

Theorem 4.31. *The composition*

$$H^q(G,A) \overset{\mathrm{Res}}{\to} H^q(H,A) \overset{\mathrm{CoRes}}{\to} H^q(G,A)$$

gives the endomorphism

$$\mathrm{CoRes} \circ \mathrm{Res} = [G\colon H] \cdot \mathrm{Id}.$$

Proof. Write $[a] = a + N_G A \in H^0(G,A)$ for $a \in A^G$. We compute

$$\begin{aligned} \mathrm{CoRes}_0 \circ \mathrm{Res}_0([a]) = \mathrm{CoRes}_0(a + N_H A) &= N_{G/H} a + N_G A \\ &= [G\colon H] \cdot a + N_G A = [G\colon H] \cdot [a]. \end{aligned}$$

The general result follows by dimension shifting. □

Theorem 4.32. *Let* $f\colon A \to B$ *be a homomorphsim of* G*-modules and let* $H \subseteq G$ *be a subgroup. Then the diagram(s)*

$$\begin{array}{ccc} H^q(G,A) & \xrightarrow{\overline{f}} & H^q(G,B) \\ {\scriptstyle \mathrm{Res}_q}\downarrow\uparrow{\scriptstyle \mathrm{CoRes}_q} & & {\scriptstyle \mathrm{Res}_q}\downarrow\uparrow{\scriptstyle \mathrm{CoRes}_q} \\ H^q(H,A) & \xleftarrow[\overline{f}]{} & H^q(H,B) \end{array}$$

is/are commutative.

Proof. This can be checked directly for $q = 0$. The general case follows from a standard dimension shifting argument. □

Since the groups $H^q(G,A)$ are abelian torsion groups, they are the sum of their p-Sylow groups:

$$H^q(G,A) = \bigoplus_p H^q(G,A)_p.$$

We call $H^q(G,A)_p$ the p-primary part of $H^q(G,A)$. We have the following result.

Theorem 4.33. *Let A be a G-module and G_p a p-Sylow group of G. Then*

$$\mathrm{Res}_q\colon H^q(G,A)_p \to H^q(G_p,A)$$

is injecctive and

$$\mathrm{CoRes}_q\colon H^q(G_p,A) \to H^q(G,A)_p$$

is surjective.

Proof. Note that $[G\colon G_p]$ is co-prime to p. In particular, by Theorem 4.31, we find that

$$H^q(G,A)_p \overset{\mathrm{Res}}{\to} H^q(G_p,A) \overset{\mathrm{CoRes}}{\to} H^q(G,A)_p$$

is an automorphism. This directly implies that Res must be injective when restricted to $H^q(G,A)_p$.

Since the orders of elements in $H^q(G_p,A)$ are all powers of p we must have $\mathrm{CoRes}(H^q(G_p,A)) \subseteq H^q(G,A)_p$. Surjectivity follows again since the composition with Res is an automorphism. ∎

This theorem gives the following very useful vanishing criterion.

Corollary 4.34. *Suppose that for each prime p there is a p-Sylow group of G so that $H^q(G_p,A)=0$, then $H^q(G,A)=0$.*

Proof. This is clear since $\mathrm{Res}\colon H^q(G,A)_p \to H^q(G_p,A)=0$ is injective, so that $H^q(G,A)_p=0$ for all p. ∎

We end this subsection with a nice application of this criterion.

Definition 4.11. Let G be a finite group and H a subgroup of G. A G-module is called G/H-induced, if it has a representation

$$A = \oplus_{\sigma\in G/H}\sigma D,$$

where $D\subseteq A$ is a H-module.

Theorem 4.35 (Shapiro's Lemma)**.** *Suppose $A=\bigoplus_{\sigma\in G/H}\sigma D$ is a G/H induced G-module, then*

$$H^q(G,A)\cong H^q(H,D).$$

Furthermore, the isomorphism is given explicitly by Res *together with the homomorphism induced from the projection $\pi\colon A\to D$.*

Proof. We choose representatives $G/H=\{[\sigma_1],\dots,[\sigma_m]\}$ with $\sigma_1=1$. For $q=0$ we consider the map

$$A^G/N_GA \overset{\mathrm{Res}}{\to} A^H/N_HA \overset{\overline{\pi}}{\to} D^H/N_HD.$$

In the opposite direction we define

$$\nu\colon D^H/N_HD \to A^G/N_GA,\ d+N_HD \mapsto \sum_{i=1}^m \sigma_i d + N_GA.$$

We leave it as an exercise to verify that

$$(\overline{\pi} \circ \mathrm{Res}) \circ \nu = \mathrm{Id} = \nu \circ (\overline{\pi} \circ \mathrm{Res}).$$

This gives the result for $q = 0$.

For the general case we apply a dimension shifting argument. Define

$$A^q = \begin{cases} J_G \otimes \ldots \otimes J_G \otimes A & \text{if } q \geq 0, \\ I_G \otimes \ldots \otimes I_G \otimes A & \text{if } q < 0; \end{cases}$$

$$D^q_* = \begin{cases} J_G \otimes \ldots \otimes J_G \otimes D & \text{if } q \geq 0, \\ I_G \otimes \ldots \otimes I_G \otimes D & \text{if } q < 0; \text{ and} \end{cases}$$

$$D^q = \begin{cases} J_H \otimes \ldots \otimes J_H \otimes D & \text{if } q \geq 0, \\ I_H \otimes \ldots \otimes I_H \otimes D & \text{if } q < 0. \end{cases}$$

The decomposition $A = \bigoplus_{i=1}^m \sigma_i D$ implies $A^q = \bigoplus_{i=1}^m \sigma_i D^q_*$. In particular A^q is also G/H-induced. Further we have

$$J_G = J_H \oplus K_1 \text{ for } K_1 = \bigoplus_{\tau \in H} \tau \left(\sum_{i=2}^m \mathbb{Z} \cdot \overline{\sigma_i} \right).$$

Similarly

$$I_G = I_H \oplus K_{-1} \text{ for } K_{-1} = \bigoplus_{\tau \in H} \tau \left(\sum_{i=2}^m \mathbb{Z} \cdot (\sigma_i - 1) \right).$$

As a result we can (canonically) decompose $D^q_* = D^q \oplus C^q$ where C^q is a H-induced H-module. We obtain the diagram

$$\begin{array}{ccccccc} H^0(G, A^q) & \xrightarrow{\mathrm{Res}_0} & H^0(H, A^q) & \xrightarrow{\overline{\pi_*}} & H^0(H, D^q_*) & \xrightarrow{\overline{\rho}} & H^0(H, D^q) \\ \downarrow{\scriptstyle \delta^q} & & \downarrow{\scriptstyle \delta^q} & & & & \downarrow{\scriptstyle \delta^q} \\ H^q(G, A) & \xrightarrow{\mathrm{Res}_q} & G^q(H, A) & & \xrightarrow{\qquad\qquad \overline{\pi} \qquad\qquad} & & H^q(H, D) \end{array}$$

We have already seen above that $\overline{\pi_*} \circ \mathrm{Res}_0$ is bijective. Furthermore the map $\overline{\rho}$ is bijective since C^q has trivial cohomology. We conclude that the top row of the diagram is a bijection. Since $A^q \xrightarrow{\pi_*} D^q_* \xrightarrow{\rho} D^q$ comes from $\pi \colon A \to D$, the diagram is commutative and we are done. ∎

Sheet 5, Exercise 2: Prove the compatibility statements for the Inflation map Inf_q (with $q \geq 1$) from Theorem 4.23 and 4.24. More precisely:

(1) Let A and B be two G-modules, $H \subseteq G$ a normal subgroup and let $f \colon A \to B$ be a G-homomorphism. Show that $\mathrm{Inf}_q \circ \overline{f}_q = \overline{f}_q \circ \mathrm{Inf}_q$.

(2) Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules and let $H \subseteq G$ be a normal subgroup. Suppose that $0 \to A^H \to B^H \to C^H \to 0$ is also exact and show that $\delta \circ \mathrm{Inf}_{q+1} = \mathrm{Inf}_q \circ \delta$.

Sheet 5, Exercise 3: Let $H \subseteq G$ be a subgroup and let D be a H-module. Then we define

$$\mathrm{Ind}_H^G(D) = \{f\colon G \to D\colon f(hg) = hf(g) \text{ for all } h \in H,\, g \in G\}.$$

We turn this into a G-module by setting $[gf](x) = f(xg)$ for $f \in \mathrm{Ind}_H^G(D)$ and $g, x \in G$.

(1) Show that for $H = \{1_G\}$ (*trivial*) we have $\mathrm{Ind}_H^G(D) \cong \mathbb{Z}[G] \otimes D$. (In other words the G-induced G-modules are precisely given by $\mathrm{Ind}_{\{1_G\}}^G(D)$ for abelian groups D.)

(2) Show that $\mathrm{Hom}_G(\mathrm{Ind}_H^G(D), B) = \mathrm{Hom}(D, \mathrm{Res}_H^G(B))$. (This is called Frobenius reciprocity.) Here $\mathrm{Res}_H^G(B)$ is the H-module obtained by restricting the action of G on B to H.

Sheet 6, Exercise 2: Verify the claims from *Definition and Lemma* 4.10 of the lecture (notes): Let G be a finite group with subgroup H. Then there is a uniquely determined family of homomorphisms (called Co-Restriction)

$$\mathrm{CoRes}_q\colon H^q(H, A) \to H^q(G, A) \text{ for } q \in \mathbb{Z}$$

satisfying

- CoRes_0 is defined by $a + N_H A \mapsto N_{G/H} a + N_G A$ for $a \in A^H$;
- For each exact sequence $0 \to A \to B \to C \to 0$ the diagram

$$\begin{array}{ccc} H^q(H, C) & \xrightarrow{\delta} & H^{q+1}(H, A) \\ {\scriptstyle \mathrm{CoRes}_q}\downarrow & & \downarrow{\scriptstyle \mathrm{CoRes}_{q+1}} \\ H^{q+1}(G, C) & \xrightarrow{\delta} & H^{q+1}(G, A) \end{array}$$

commutes.

Sheet 6, Exercise 3: Let G be a finite group with subgroup H. Write $G = g_1 H \cup \ldots \cup g_r H$ where $r = [G\colon H]$. We define

$$\phi(g) = g_i \text{ if } g \in g_i H.$$

We set $V(g) = \prod_{i=1}^r \phi(gg_i)^{-1} \cdot (gg_i)$.

(1) Show that V induces a homomorphism $\overline{V}\colon G^{\mathrm{ab}} \to H^{\mathrm{ab}}$, which is independent of the representatives g_i.

(2) Find an isomorphism $\widetilde{\log}\colon H^{\mathrm{ab}} \to (I_H \to I_G I_H)/I_G I_H$ such that the diagram

$$\begin{array}{ccc} G^{\mathrm{ab}} & \xrightarrow{\overline{V}} & H^{\mathrm{ab}} \\ {\scriptstyle \log}\downarrow & & \downarrow{\scriptstyle \widetilde{\log}} \\ I_G/I_G^2 & \xrightarrow{\overline{v}} & (I_H + I_G I_H)/I_G I_H \end{array}$$

commutes, where $\overline{v}(x + I_G^2) = x \cdot (g_1 + \ldots + g_r) + I_G I_H$.

(3) Does the map $\overline{V}$ agree with the map Ver defined using cohomolgy groups (i.e. Definition 4.9)?

Sheet 7, Exercise 1: We continue Sheet 6, Exercise 3 using the same notation. Our goal is to show that, if G is a finite group with commutator subgroup G', then $\mathrm{Ver}\colon G^{\mathrm{ab}} \to (G')^{\mathrm{ab}}$ is trivial.
This can be done by completing the following sketch:

- Reduce to the case where G' is abelian. Further, show that $I_{G'}\mathbb{Z}[G]$ is a two-sided ideal of $\mathbb{Z}[G]$ and that the quotient by it is a commutative ring.
- Use the classification of finite abelian groups to write $G^{\mathrm{ab}} = G/G' \cong \mathbb{Z}/e_1\mathbb{Z} \times \ldots \times \mathbb{Z}/e_s\mathbb{Z}$ and choose elements in $\sigma_1, \ldots, \sigma_n$ such that $\sigma_i \cdot G'$ generates $\{1\} \times \ldots \mathbb{Z}/e_i\mathbb{Z} \times \ldots \times \{1\}$.
- Find elements $\mu_i \in \mathbb{Z}[G]$ such that $\sigma_i^{e_i} - 1 = (\sigma_i - 1)\mu_i$.
- Check that $\mu_1 \cdots \mu_s + I_{G'}\mathbb{Z}[G] = g_1 + \ldots + g_r + I_{G'}\mathbb{Z}[G]$.

4.5. **The cup-product.** Let A and B be two G-modules. Obviously $A \otimes B$ is also a G-module and we have a canonical bilinear map

$$A^G \times B^G \to (A \otimes B)^G,\ (a, b) \mapsto a \otimes b.$$

Of course $N_G A \times N_G B$ is mapped to $N_G(A \otimes B)$. This induces a bilinear map

$$H^0(G, A) \times H^0(G, B) \to H^0(G, A \otimes B),\ ([a], [b]) \mapsto [a \otimes b].$$

We write $[a] \cup [b] = [a \otimes b]$ and call it the cup-product. As in the case of restriction and co-restriction we can extend the definition of the cup-product to arbitrary dimension by dimension shifting.

Definition 4.12 (and Lemma)**.** There is a family of bilinear maps

$$\cup\colon H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

called the cup-product. It is uniquely determined by the following properties

(1) For $p = q = 0$ the cup-product is given by

$$(\overline{a}, \overline{b}) \mapsto \overline{a} \cup \overline{b} = \overline{a \otimes b}.$$

(2) Suppose $0 \to A \to A' \to A'' \to 0$ and $0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$ are both exact, then the diagram

$$\begin{array}{ccc} H^p(G, A'') \times H^q(G, B) & \xrightarrow{\cup} & H^{p+q}(G, A'' \otimes B) \\ \downarrow{\scriptstyle \delta \times 1} & & \downarrow{\scriptstyle \delta} \\ H^{p+1}(G, A) \times H^q(G, B) & \xrightarrow{\cup} & H^{p+q+1}(G, A \otimes B) \end{array}$$

commutes.

(3) Suppose $0 \to B \to B' \to B'' \to 0$ and $0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$ are both exact, then the diagram

$$\begin{array}{ccc} H^p(G,A)\times H^q(G,B'') & \xrightarrow{\cup} & H^{p+q}(G,A\otimes B'') \\ \downarrow{\scriptstyle 1\times\delta} & & \downarrow{\scriptstyle (-1)^p\delta} \\ H^p(G,A)\times H^{q+1}(G,B) & \xrightarrow{\cup} & H^{p+q+1}(G,A\otimes B) \end{array}$$

commutes.

Proof. This is the usual dimension shifting argument and we omit it. ∎

Theorem 4.36. *Let a_p (resp. b_q) be a p-cocycle (resp. a q-cocycle) of A (resp. B). Then we have*

$$\overline{a}_0 \cup \overline{b}_q = \overline{a_0 \otimes b_q} \text{ and } \overline{a}_p \cup \overline{b}_0 = \overline{a_p \otimes b_0} \tag{5}$$

Proof. This is a direct consequence of the proof (that we omitted) of the lemma part of the definition above. ∎

For the usefulness of the cup-product it is important, that it behaves well with other cohomological operations. This is the content of the following theorems.

Theorem 4.37. *Let $f\colon A \to A'$ and $g\colon B \to B'$ be two G-homomorphisms. Then we have*

$$\overline{f}(\overline{a}) \cup \overline{g}(\overline{b}) = \overline{f \otimes g}(\overline{a} \cup \overline{b}).$$

Proof. This is obvious in (diagonal) dimension 0 and the general case is derived using dimension shifting. ∎

Theorem 4.38. *Let A, B be G-modules and let $H \subseteq G$ be a subgroup. Then we have*

(1) *For $\overline{a} \in H^p(G,A)$ and $\overline{b} \in H^q(G,B)$ we have*

$$\mathrm{Res}_{p+q}(\overline{a} \cup \overline{b}) = \mathrm{Res}_p(\overline{a}) \cup \mathrm{Res}_q(\overline{b}) \in H^{p+q}(H, A\otimes B).$$

(2) *For $\overline{a} \in H^p(G,A)$ and $\overline{b} \in H^q(H,B)$ we have*

$$\mathrm{CoRes}_{p+q}(\mathrm{Res}_p(\overline{a}) \cup \overline{b}) = \overline{a} \cup \mathrm{CoRes}_q(\overline{b}) \in H^{p+q}(G, A\otimes B).$$

Proof. We only sketch the $p = q = 0$ case for (2) (since (1) is trivial):

$$\mathrm{CoRes}_0(\mathrm{Res}_0(\overline{a}) \cup \overline{b}) = \mathrm{CoRes}_0(a\otimes b + N_H(A\otimes B)) = \sum_{\sigma\in G/H} \sigma(a\otimes b) + N_G(A\otimes B)$$

$$= \sum_{\sigma\in G/H} a\otimes \sigma b + N_G(A\otimes B) = a\otimes\left(\sum_{\sigma\in G/H}\sigma b\right) + N_G(A\otimes B) = \overline{a}\cup \mathrm{CoRes}_0(\overline{b}),$$

where we used that $a \in A^G$ and $b \in B^H$. As usual the rest of the proof proceeds by dimension shifting. ∎

Theorem 4.39. *We have*

$$\overline{a} \cup \overline{b} = (-1)^{pq}(\overline{b} \cup \overline{a}) \text{ and } (\overline{a} \cup \overline{b}) \cup \overline{c} = \overline{a} \cup (\overline{b} \cup \overline{c}).$$

Proof. The proof relies on the canonical identifications $A \otimes B = B \otimes A$ and $(A \otimes B) \otimes C = A \otimes (B \otimes C)$. (Actually these were already used above in the dimension shifting arguments that we omitted.) ∎

Finally we derive some explicit formulae for the cup-product in small dimensions.

Lemma 4.40. *The cup product $\overline{a}_1 \cup \overline{b}_{-1} \in H^0(G, A \otimes B)$ is given by*

$$x_0 = \sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}.$$

Proof. Let $A' = \mathbb{Z}[G] \otimes A$. This is a G-induced G-module and we have the exact sequences

$$0 \to A \to A' \to A'' \to 0 \text{ and}$$
$$0 \to A \otimes B \to A' \times B \to A'' \otimes B \to 0.$$

Since $H^1(G, A') = 0$ we have a 0-cochain $a'_0 \in A'$ with $a_1 = \partial a'_0$. Thus

$$a_1(\tau) = \tau a'_0 - a'_0 \text{ for all } \tau \in G.$$

Let $a''_0 \in (A'')^G$ be the image of a'_0 in A''. By definition of δ we have $\delta(\overline{a''_0}) = \overline{a}_1$. Since $N_G b_{-1} = 0$ we can compute:

$$\begin{aligned}
\overline{a}_1 \cup \overline{b}_{-1} &= \delta(\overline{a''_0}) \cup \overline{b}_{-1} = \delta(\overline{a''_0} \cup \overline{b}_{-1}) = \delta(\overline{a''_0 \otimes b_{-1}}) = \overline{\partial_0(a'_0 \otimes b_{-1})} \\
&= \overline{N_G(a'_0 \otimes b_{-1})} = \overline{\sum_{\tau \in G} \tau a'_0 \otimes \tau b_{-1}} = \overline{\sum_{\tau \in G} (a_1(\tau) + a'_0) \otimes \tau b_{-1}} \\
&= \overline{\sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}} + \overline{a'_0 \otimes N_G b_{-1}} = \overline{\sum_{\tau \in G} a_1(\tau) \otimes \tau b_{-1}}.
\end{aligned}$$

∎

Now we take $B = \mathbb{Z}$ and use the identification $A \otimes \mathbb{Z} = A$ given by $a \otimes n \mapsto n \cdot a$. Recall the canonical isomorphism

$$H^{-2}(G, \mathbb{Z}) \cong G^{\mathrm{ab}}.$$

Thus we can view the class $\overline{\sigma} = \sigma G' \in G^{\mathrm{ab}}$ of $\sigma \in G$ as an element in $H^{-2}(G, \mathbb{Z})$.

Lemma 4.41. *We have $\overline{a}_1 \cup \overline{\sigma} = \overline{a_1(\sigma)} \in H^{-1}(G, A)$.*

Proof. Look at the exact sequence $0 \to A \otimes I_G \to A \otimes \mathbb{Z}[G] \to A \to 0$ to obtain the isomorphism

$$H^{-1}(G, A) \xrightarrow{\delta} H^0(G, A \otimes I_G).$$

Obviously it suffices to show that $\delta(\overline{a}_1 \cup \overline{\sigma}) = \delta(\overline{a_1(\sigma)})$.

To so we recall the definition of δ and find

$$\delta(\overline{a_1(\sigma)}) = \overline{x}_0 \text{ with } x_0 = \sum_{\tau \in G} \tau a_1(\sigma) \otimes \tau.$$

On the other hand we remember that $\delta\colon H^{-2}(G,\mathbb{Z}) \to H^{-1}(G,I_G)$ is given by $\delta\overline{\sigma} = \overline{\sigma - 1}$. We obtain

$$\delta(\overline{a}_1 \cup \overline{\sigma}) = -(\overline{a}_1 \cup \delta(\overline{\sigma}) = -\overline{a}_1 \cup (\overline{\sigma - 1}) = \overline{y}_0.$$

We can rewrite y_0 as

$$y_0 = -\sum_{\tau\in G} a_1(\tau)\otimes\tau(\sigma-1) = \sum_{\tau\in G} a_1(\tau)\otimes\tau - \sum_{\tau\in G} a_1(\tau)\otimes\tau\sigma = \sum_{\tau\in G}\tau a_1(\sigma)\otimes\tau\sigma.$$

In the last step we used the 1-cocycle property $a_1(\tau) = a_1(\tau\sigma) - \tau a_1(\sigma)$ and a change of variables in one of the resulting sums. Now we can check

$$y_0 - x_0 = \sum_{\tau\in G}\tau a_1(\sigma)\otimes\tau(\sigma-1) = N_G(a_1(\sigma)\otimes(\sigma-1)).$$

In particular $\overline{x}_0 = \overline{y}_0$ and we are done. ∎

The final theorem will turn out to be of great interest for class field theory.

Theorem 4.42. *We have*

$$\overline{a}_2 \cup \overline{\sigma} = \overline{\sum_{\tau\in G} a_2(\tau,\sigma)} \in H^0(G,A).$$

Proof. Again we consider $A' = \mathbb{Z}[G]\otimes A$ and $A'' = J_G\otimes A$ so that $0\to A\to A'\to A''\to 0$ is exact. Recall that $H^2(G,A') = 0$. Therefore we find a 1-cochain $a_1'\in A_1'$ with $a_2 = \partial a_1'$. In particular

$$a_2(\tau,\sigma) = \tau a_1'(\sigma) - a_1'(\tau\cdot\sigma) + a_1'(\tau).$$

The image a_1'' of a_1' is a 1-cocycle of A'' with $\overline{a}_2 = \delta(\overline{a_1''})$. This allows us to compute

$$\overline{a}_2\cup\overline{\sigma} = \delta(\overline{a_1''})\cup\overline{\sigma} = \delta(\overline{a_1''}\cup\overline{\sigma}) = \delta(\overline{a_1''}(\sigma)) = \overline{\partial(a_1'(\sigma))} = \overline{\sum_{\tau\in G}\tau a_1'(\sigma)}$$

$$= \overline{\sum_{\tau\in G} a_2(\tau,\sigma)} + \overline{\sum_{\tau\in G} a_1'(\tau\cdot\sigma) - \sum_{\tau\in G} a_1'(\tau)} = \overline{\sum_{\tau\in G} a_2(\tau,\sigma)}.$$

∎

Sheet 7, Exercise 3: For $p\geq -1$ and $q\geq 1$ let $[a_p]\in H^p(G,A)$ and $[b_q]\in H^q(G,B)$ be two classes in the corresponding cohomology groups. Write $[a_p]\cup[b_q] = [x]\in H^{p+q}(G,A\otimes B)$.

(1) Show that for $p\geq 1$ we can take

$$x(\sigma_1,\dots,\sigma_{p+q}) = a_p(\sigma_1,\dots,\sigma_q)\otimes[\sigma_1\cdots\sigma_p b_q(\sigma_{p+1},\dots,\sigma_{p+q})].$$

(This generalizes the case $p=0$ stated in Theorem 4.36.)

(2) Show that for $p=-1$ we can take x to be the co-cycle:

$$x = \sum_{\sigma\in G}\sigma a_p\otimes\sigma b_q(\sigma^{-1},\sigma_1,\dots,\sigma_{q-1}).$$

(Convince yourself that this is consistent with Lemma 4.40.)

4.6. **The Herbrand quotient.** Let $G = \langle\sigma\rangle$ be a finite cyclic group of order n. We have

$$\mathbb{Z}[G] = \bigoplus_{i=0}^{n-1} \mathbb{Z}\sigma^i \text{ and } N_G = 1 + \sigma + \ldots + \sigma^{n-1}.$$

Note that $\sigma^k - 1 = (\sigma - 1)(\sigma^{k-1} + \ldots + \sigma + 1)$. This means that

$$I_G = \mathbb{Z}[G](\sigma - 1).$$

Theorem 4.43. *Let G be a (finite) cyclic group and let A be a G-module. Then*

$$H^q(G, A) \cong H^{q-2}(G, A) \text{ for all } q \in \mathbb{Z}.$$

Proof. Note that it suffices to proof $H^{-1}(G, A) \cong H^1(G, A)$, since the general case follows from dimension shifting:

$$H^q(G, A) \cong H^{-1}(G, A^{q+1}) \cong H^1(G, A^{q+1}) \cong H^{q+2}(G, A).$$

Recall that the group Z_1 of 1-cocycles consists of crossed homomorphisms $x\colon G \to A$. Thus, for $x \in Z_1$ we have

$$x(\sigma^k) = \sigma x(\sigma^{k-1}) + x(\sigma) = \sum_{i=0}^{k-1} \sigma^i x(\sigma).$$

Obviously we also have $x(1) = 0$. We conclude that

$$N_G x(\sigma) = \sum_{i=0}^{n-1} \sigma^i x(\sigma) = x(\sigma^n) = x(1) = 0.$$

This implies $x(\sigma) \in {}_{N_G}A$.

On the other hand, we can take a (-1)-cocycle $a \in Z_{-1}$ and define $x \in Z_1$ by $x(\sigma) = a$ and $x(\sigma^k) = \sum_{i=0}^{k-1} \sigma^i a$. Thus we have an isomorphism

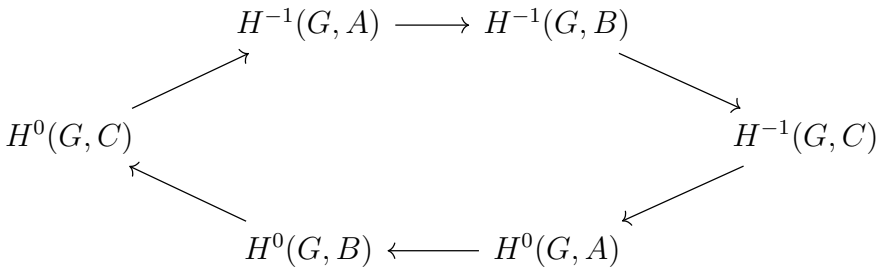
$$Z_1 \ni x \mapsto x(\sigma) \in Z_{-1}.$$

This isomorphism maps 1-coboundaries to (-1)-coboundaries and we are done. ∎

We have just seen that for cyclic groups

$$H^{2q}(G, A) \cong H^0(G, A) \text{ and } H^{2q+1}(G, A) \cong H^q(G, A).$$

If we now take a short exact sequence $0 \to A \to B \to C \to 0$ we can write the long exact sequence as



It is not completely obvious that this is exact. Indeed at $H^{-1}(G,A)$ one needs to check that the isomorphism $H^1(G,A) \cong H^{-1}(G,A)$ respects the kernel, but this is easy to see.

Definition 4.13. Let A be an abelian group and f, g endomorphisms so that $f \circ g = 0 = g \circ f$. Then we define the **Herbrand quotient** by

$$q_{f,g}(A) = \frac{[\ker(f)\colon \mathrm{Im}(g)]}{[\ker(g)\colon \mathrm{Im}(f)]},$$

as soon as both indices are finite.

An important special case is the following. Let G be a cyclic group of order n and let A be a G-module. We consider

$$f = D = \sigma - 1 \text{ and } g = N = 1 + \ldots + \sigma^{n-1}.$$

We have $D \circ N = N \circ D = 0$. Even more,

$$\ker(D) = A^G,\ \mathrm{Im}(N) = N_G A,\ \ker(N) = {}_{N_G}A \text{ and } \mathrm{Im}(D) = I_G A.$$

This implies

$$q_{D,N}(A) = \frac{\sharp H^0(G,A)}{\sharp H^{-1}(G,A)} = \frac{\sharp H^2(G,A)}{\sharp H^1(G,A)}$$

as soon as the relevant cohomology groups are finite. If this is the case we call A a Herbrand module.

Definition 4.14. Let G be a cyclic group of finite order and let A be a G-module. We set

$$h(A) = q_{D,N}(A).$$

Theorem 4.44. *If G is a cyclic group of finite order and $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules, then*

$$h(B) = h(A) \cdot h(C).$$

This equality includes the statement, that if two of the quotients are defined, then so is the third.

Proof. Exactness of (4.6) directly yields

$$\sharp H^{-1}(G,A) \cdot \sharp H^{-1}(G,C) \cdot \sharp H^0(G,B) = \sharp H^{-1}(G,B) \cdot \sharp H^0(G,A) \cdot \sharp H^0(G,C).$$

This implies the result. ∎

Another interesting case is given by $f = 0$ and $g = n$. Here $n\colon a \mapsto n \cdot a$. We obviously have

$$q_{0,n}(A) = \frac{[A\colon n \cdot A]}{\sharp_n A}$$

(Recall that ${}_nA = \{a \in A\colon n \cdot a = 0\}$.)

Theorem 4.45. *Suppose the cyclic group G of order n operates trivially on A, then we have $h(A) = q_{0,n}(A)$. In particular, given a short exact sequence $0 \to A \to B \to C \to 0$ of abelian groups, we get*

$$q_{0,n}(B) = q_{0,n}(A)q_{0,n}(C).$$

Proof. Clear. ∎

Theorem 4.46. *If A is a finite group, then $q_{f,g}(A) = 1$.*

Proof. We clearly have

$$\sharp A = \sharp \ker(f) \cdot \sharp \mathrm{Im}(f) = \sharp \ker(g) \cdot \sharp \mathrm{Im}(g).$$

This implies the result. ∎

This implies the following important fact. Suppose $A \subseteq B$ is a submodule of finite index, then $h(B) = h(A)$.

Lemma 4.47. *Let f and g be commuting endomorphisms of an abelian group A. Then*

$$q_{0,gf}(A) = q_{0,g}(A) \cdot q_{0,f}(A).$$

Proof. We start with the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & g(A) \cap \ker(f) & \longrightarrow & g(A) & \longrightarrow & fg(A) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker(f) & \longrightarrow & A & \longrightarrow & f(A) & \longrightarrow & 0 \end{array}$$

We obtain the exact sequence

$$0 \to \ker(f)/[g(A) \cap \ker(f)] \to A/g(A) \to f(A)/[fg](A) \to 0.$$

This yields

$$\frac{[A\colon [fg](A)]}{[A\colon f(A)]} = \frac{[A\colon g(A)] \cdot \sharp g(A) \cap \ker(f)}{\sharp \ker(f)}.$$

The result follows after observing that

$$\ker(fg)/\ker(g) = g^{-1}[g(A) \cap \ker(f)]/g^{-1}(0) \cong g(A) \cap \ker(f).$$

∎

With this at hand we can prove the following important theorem:

Theorem 4.48. *Let G be a cyclic group of prime order p and let A be a G-module. If $q_{0,p}(A)$ is defined, thenn $q_{0,p}(A^G)$ and $h(A)$ are defined. Even more, we have*

$$h(A)^{p-1} = q_{0,p}(A^G)^p/q_{0,p}(A).$$

Proof. Suppose σ generated G and put $D = \sigma - 1$. We have the usual exact sequence

$$0 \to A^G \to A \xrightarrow{D} I_G A \to 0.$$

Clearly if $q_{0,p}(A)$ is defined also $q_{0,p}(I_G A)$ is defined (since $I_G A$ is a subgroup and a factor of $G(A)$). By multiplicativity we get

$$q_{0,p}(A) = q_{0,p}(A^G) \cdot q_{0,p}(I_G A).$$

In particular $q_{0,p}(A^G)$ is defined. Furthermore, since G acts trivially on A^G we get $h(A^G) = q_{0,p}(A^G)$.

We need to compute $q_{0,p}(I_G A)$. To do so we observe that the ideal

$$\mathbb{Z} \cdot N_G = \mathbb{Z}\left(\sum_{i=0}^{p-1} \sigma^i\right)$$

kills the module $I_G A$. Thus, we can view $I_G A$ as a $\mathbb{Z}[G]/\mathbb{Z} \cdot N_G$-module. We have the ring isomorphism

$$\mathbb{Z}[G]/\mathbb{Z} \cdot N_G \cong \mathbb{Z}[X]/(1 + X + \ldots + X^{p-1}) \cong \mathbb{Z}[\zeta],$$

where ζ is a primitive pth root of unity. (Recall that $\mathbb{Z}[\zeta]$ is the ring of integers of thy cyclotomic field $\mathbb{Q}[\zeta]$). The isomorphism is given by $\sigma \mapsto \zeta$. We have the factorisation

$$p = e \cdot (\zeta - 1)^{p-1}$$

for some unit e. Translating this back gives

$$p = \epsilon \cdot (\sigma - 1)^{p-1},$$

for some unit ϵ in $\mathbb{Z}[G]/\mathbb{Z} \cdot N_G$. The unit ϵ defines an automorphism on $I_G A$, so that $q_{0,\epsilon}(I_G A) = 1$. We compute that

$$q_{0,p}(I_G A) = q_{0,D^{p-1}}(I_G A) \cdot q_{0,\epsilon}(I_G A) = q_{0,D}(I_G A)^{p-1} = \frac{1}{q_{D,0}(I_G A)^{p-1}}.$$

As observed above $N = N_G$ annihilates $I_G A$ and we can write

$$q_{0,p}(I_G A) = \frac{1}{q_{D,0}(I_G A)^{p-1}} = \frac{1}{q_{D,N}(I_G A)^{p-1}} = \frac{1}{h(I_G A)^{p-1}}.$$

Using the exact sequence $0 \to A^G \to A \to I_G A \to 0$ yields

$$h(A)^{p-1} = h(A^G)^{p-1} h(I_G A)^{p-1}.$$

We have now all the information we need and compute

$$h(A)^{p-1} = h(A^G)^{p-1} h(I_G A)^{p-1} = \frac{q_{0,p}(A^G)^{p-1}}{q_{0,p}(I_G A)} = \frac{q_{0,p}(A^G)^p}{q_{0,p}(A)}.$$

□

We complete this subsection with the following nice application.

Theorem 4.49 (Chevalley)**.** *Let G be a cyclic group of prime order p and let A be a finitely generated G-module. Suppose α is the rank of A and that β is the rank of A^G. We have*

$$h(A) = p^{(p\cdot\beta-\alpha)/(p-1)}.$$

Proof. Write $A = A_0 \oplus A_1$, where A_0 is a torsion module and A_1 is torsion free. We obtain $A^G = A_0^G \oplus A_1^G$. The finite generation of A tells us that A_0 is a finite group, so that the rank of A is the rank of A_1. Similarly the rank of A^G is the rank of A_1^G. Applying our last theorem yields

$$h(A)^{p-1} = h(A_1)^{p-1} = \frac{q_{0,p}(A_1^G)^p}{q_{0,p}(A_1)}.$$

Finally $q_{0,p}(A_1^G) = [A_1^G \colon pA_1^G] = p^\beta$ and $q_{0,p}(A_1) = [A_1 \colon pA_1] = p^\alpha$. ∎

Sheet 7, Exercise 2: Use the Herbrand quotient $q_{0,m}(F^\times)$, where m denotes the map $x \mapsto x^m$, to proof Theorem 3.20. More precisely, show that

$$[F^\times \colon (F^\times)^m] = mq^{v(m)} \cdot \sharp F_m,$$

for a non-archimedean local field F. Recall that $F_m = F \cap \mu_m$ where μ_m is the group of mth roots of unity. Further, q is the residue characteristic and v is the normalized valuation on F.

4.7. **A theorem of Tate.** We begin with the **Theorem of Cohomological Triviality**:

Theorem 4.50. *A G-module A is cohomological trivial if the is q_0 so that $H^{q_0}(H, A) = H^{q_0+1}(H, A) = 0$ for all subgroups $H \subseteq G$.*

Proof. For the cyclic group this is obvious. Indeed we will reduce the case of general G to the cyclic one. Either way it suffices to show that $H^{q_0}(H, A) = H^{q_0+1}(H, A) = 0$ for all subgroups $H \subseteq G$ implies that $H^{q_0-1}(H, A) = H^{q_0+2}(H, A) = 0$ for all subgroups $H \subseteq G$. By dimension shifting we can further assume that $q_0 = 1$. We do so by induction over the order $n = \sharp G$ of G. The case $n = 1$ is trivial.

Thus we suppose that $H^1(H, A) = H^2(H, A) = 0$ for all subgroups $H \subseteq G$ and (by induction hypothesis) we also suppose that $H^0(H, A) = H^3(H, A) = 0$ for all proper subgroups $H \subseteq G$.

If G is not a p-group, then all Sylow subgroups are proper subgroups and the result is clear (see Corollary 4.34).

The critical case we need to consider is the one where G is a p-group. In this case there is a normal subgroup $H \subseteq G$, so that G/H is cyclic of prime order. By assumption we have $H^i(H, A) = 0$ for $i = 0, 1, 2, 3$. We consider the map

$$\mathrm{Inf}_i \colon H^i(G/H, A^H) \to H^i(G, A).$$

For $i = 1, 2, 3$ this is an isomorphism. We use this in two ways. First we obtain $H^i(G/H, A^H) = 0$ for $i = 1, 2$. In particular, since G/H is cyclic we find

that $H^3(G/H, A^H) = 0$, which then implies $H^3(G, A) = 0$. But we also have $H^0(G/H, A^H) = 0$. Note that since $H^0(H, A) = 0$ we have $A^H = N_H A$. This allows us to compute

$$A^G = N_{G/H} A^H = N_{G/H}(N_H A) = N_G A.$$

This implies $H^0(G, A) = 0$ and we are done. ∎

Given a fixed element $a \in H^p(G, A)$ we look at the canonical map

$$a\cup\colon H^q(G, B) \to H^{p+q}(G, A \otimes B),\ b \mapsto a \cup b.$$

Theorem 4.51. *Let A be a G-module such that for each subgroup $H \subseteq G$ we have*

(1) *$H^{-1}(H, A) = 0$;*
(2) *$H^0(H, A)$ is cyclic of order $\sharp H$.*

Let a be the generator of $H^0(G, A)$. Then the map

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

is an isomorphism for every $q \in \mathbb{Z}$.

Proof. Instead of working with A directly we use the module $B = A \oplus \mathbb{Z}[G]$. We can do so without changing the cohomology groups. Indeed, if $i\colon A \to B$ is the canonical injection, the $\overline{i}\colon H^q(H, A) \to H^q(H, B)$ is an isomorphism. (This is because $\mathbb{Z}[G]$ is cohomological trivial.)

We can now take $a_0 \in A^G$ so that $a = a_0 + N_G A$ is the generator of $H^0(G, A)$. We consider the map

$$f\colon \mathbb{Z} \to B,\ n \mapsto a_0 \cdot n + N_G n \tag{6}$$

Due to the presence of the second term this map is injective. (This was the hole point of passing from A to B.) We obtain the induced homomorphism

$$\overline{f}\colon H^q(H, \mathbb{Z}) \to H^q(H, B).$$

This leads to the commuting diagram

$$\begin{array}{ccc} H^q(G, \mathbb{Z}) & \xrightarrow{a\cup} & H^q(G, A) \\ & \searrow^{\overline{f}} & \downarrow{\scriptstyle \overline{i}} \\ & & H^q(G, B) \end{array}$$

It remains to show that $\overline{f}$ is bijective. To see this we look at the exact sequence

$$0 \to \mathbb{Z} \xrightarrow{f} B \to C \to 0$$

of G-modules. Since $H^{-1}(H, B) = H^{-1}(H, A) = 0$ and $H^1(H, \mathbb{Z}) = 0$ for all $H \subseteq G$ we get an exact sequence

$$0 \to H^{-1}(H, C) \to H^0(H, \mathbb{Z}) \xrightarrow{\overline{f}} H^0(H, B) \to H^0(H, C) \to 0.$$

Since for $q = 0$ the map $\overline{f}$ is obviously an isomorphism we get $H^{-1}(H, C) = H^0(H, C) = 0$ for all subgroups $H \subseteq G$. Applying the Theorem of Cohomological Triviality we get $H^q(H, C) = 0$ for all q and all subgroups $H \subseteq G$. By looking at the long exact sequence of cohomology we see that this implies that $\overline{f}\colon H^q(G, \mathbb{Z}) \to H^q(G, B)$ is an isomorphism for all q. ∎

This brings us to the following major theorem:

Theorem 4.52 (Tate)**.** *Let A be a G-module such that for all subgroups $H \subseteq G$ we have*

(1) $H^1(H, A) = 0$*;*
(2) $H^2(H, A)$ *is cyclic of order $\sharp H$.*

Let a be the generator of $H^2(G, A)$. Then

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

is an isomorphism. Furthermore, $\mathrm{Res}(a)$ *generates $H^2(H, A)$ and we obtain isomorphisms*

$$\mathrm{Res}(a)\cup\colon H^q(H, \mathbb{Z}) \to H^{q+2}(H, A)$$

for all subgroups $H \subseteq G$.

This theorem has several generalisations. However, the version given here is enough for our purposes.

Proof. We consider the dimension shift $\delta^2\colon H^q(H, A^2) \to H^{q+2}(H, A)$. We know that $H^{-1}(H, A^2) = 0$ and that $H^0(H, A^2)$ is cyclic of order $\sharp H$. We get the commutative diagram

$$\begin{array}{ccc} H^q(G, \mathbb{Z}) & \xrightarrow{\delta^{-2}a\cup} & H^q(G, A^2) \\ \| & & \downarrow{\scriptstyle \delta^2} \\ H^q(G, \mathbb{Z}) & \xrightarrow{a\cup} & H^{q+2}(G, A) \end{array}$$

According to our previous theorem $\delta^{-2}a\cup$ is bijective. In particular $a\cup$ must be bijective.

The remaining statement follows directly as soon as we can show that $\mathrm{Res}(a)$ generates $H^2(H, A)$. But this is true since $\mathrm{CoRes} \circ \mathrm{Res}(a) = [G\colon H] \cdot a$ so that the order of $\mathrm{Res}(a)$ must divide $\sharp H$. ∎

Sheet 8, Exercise 2: Let G be a finite group and let A and B be G-modules. Suppose that A has trivial Cohomology and that B is without p-torsion for all primes p dividing $\sharp G$. Show that $A \otimes B$ has trivial Cohomology. (It can be used that every module with trivial cohomology can be written as a quotient of a free $\mathbb{Z}[G]$-module.)

4.8. **Examples from Galois theory.** We end this section by considering some important examples of trivial cohomology groups arising from Galois theory.

Theorem 4.53. *Let $G = \mathrm{Gal}(L|K)$ be the Galois group of a finite Galois extension. Then*

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

for all q.

Proof. This was an exercise in Algebra 1 based on the fact that $H^q(G, \mathbb{Z}[G]\otimes_{\mathbb{Z}} K) = 0$ for all q. The latter fact has been established above. ∎

Theorem 4.54 (Hilbert-Noether-Speiser)**.** *Let $G = \mathrm{Gal}(L|K)$ be the Galois group of a finite Galois extension. Then*

$$H^1(G, L^\times) = 1.$$

Proof. This was proven in Algebra 1. ∎

Theorem 4.55. *Let $L|K$ be an extension of finite fields with Galois group $G = \mathrm{Gal}(L|K)$, then*

$$H^q(G, L^\times) = 1 \text{ for all } q.$$

Proof. **Exercise**. ∎

Sheet 5, Exercise 4: Let $L|K$ be a finite Galois extension with Galois group G. We let $\sigma \in G$ act on L^n component wise and write $v_\sigma \colon L^n \to L^n$ for the corresponding map. Further, for $X \in \mathrm{GL}_n(L)$ set

$$X^\sigma = v_\sigma X v_\sigma^{-1} \in \mathrm{GL}_n(L).$$

We call $f \colon G \to \mathrm{GL}_n(L)$ a 1-cocycle (with values in $\mathrm{GL}_n(L)$, if

$$f(gh) = f(g) \cdot f(h)^g \text{ for all } g, h \in G.$$

(1) Show that if $X = (X_{ij})_{1\le i,j\le n}$, then $X^\sigma = (\sigma X_{ij})_{1\le i,j\le n}$.
(2) Let f be a 1-cocyle a defined above and set $u_\sigma = f(\sigma)v_\sigma$. Check that $u_\sigma u_\tau = u(\sigma\tau)$ and $\sigma(l) \cdot u_\sigma = u_\sigma \cdot l$ for $\sigma, \tau \in G$ and $l \in L^\times$. (Note that here we view $L^\times$ as the center of $\mathrm{GL}_n(L)$.)
(3) Let $\mathfrak{A} = \sum_{\sigma\in G} L u_\sigma$ be the K-subalgebra of $\mathrm{End}_K(L^n)$. Show that $\mathfrak{A}$ is isomorphic to $\mathrm{End}_K(L)$.
(4) Use the Skolem-Noether Theorem[10] to find $a \in \mathrm{GL}_n(L)$ such that $f(\sigma) = a \cdot a^{-\sigma}$. (In some sense this says that $H^1(G, \mathrm{GL}_n(L)) = \{1\}$, even if the latter is not appropriately defined for $n > 1$.)

[10]This theorem states the following: Let B be a finite dimensional central simple K-algebra, and let A be a central simple K-algebra. Further let $f, g \colon A \to B$ be two K-algebra homomorphisms, then there exists a unit $b \in B^\times$ such that for all $a \in A$ we have $g(a) = bf(a)b^{-1}$. It can also be used that $\mathrm{End}_K(L)$ is a finite dimensional central simple K-algebra.

Sheet 7, Exercise 1: Let K be a field containing the n-th roots of unity and suppose that n is co-prime to the characteristic of K. A (not necessarily finite) abelian Galois extension $L|K$ is called kummerian if $G(L|K)$ has exponent n (i.e. $\sigma^n = 1$ for all $\sigma \in G(L|K)$). If $L|K$ is a kummerian extension, then we call L a kummerian field over K. The exercise is to proof the following result:

Theorem (Kummer Theory): There is an inclusion preserving isomorphism between the collection of kummerian fields L over K and the collection of subgroups $\Delta \subseteq K^\times$ containing $(K^\times)^n$. It is given by the assignment

$$L \mapsto \Delta = (L^\times)^n \cap K^\times,$$
$$\Delta \mapsto L = K(\Delta^{\frac{1}{n}}).$$

Furthermore, the factor group $\Delta/(K^\times)^n$ is isomorphic to the character group $\chi(G(L|K))$.

Note that in the current multiplicative setting it is convenient to define the character group by

$$\chi(G(L|K)) = \{\xi \colon G(L|K) \to \mu_\infty\}, \text{ where } \mu_\infty = \bigcup_{k\geq 0} \mu_k = \{e^{2\pi i x} \colon x \in \mathbb{Q}/\mathbb{Z}\},$$

where μ_k is the group of kth roots of unity. Note that if $L|K$ is an infinite extension, then $G(L|K)$ is a pro-finite group and we additionally require that $\xi \in \chi(G(L|K))$ is continuous (where μ_∞ is equipped with the discrete topology).
One can proceed as follows:

(1) Construct maps such that the sequence

$$1 \to \mu_n \to K^\times \xrightarrow{(\cdot)^n} (L^\times)^n \cap K^\times \to \chi(G(L|K)) \to 1$$

is exact. Conclude that this gives the isomorphism

$$(L^\times)^n \cap K^\times/(K^\times)^n \cong \chi(G(L|K)),$$

where the class $a\cdot(K^\times)^n \in (L^\times)^n \cap K^\times/(K^\times)^n$ corresponds to the character χ_a given by $\chi_a(\sigma) = \sigma(a^{\frac{1}{n}})/a^{\frac{1}{n}}$.

(2) Determine the largest kummerian field over K and its Galois group.

(3) Conclude the proof of the theorem using Galois theory. (If needed it can be used that for pro-finite groups G the map $\mathrm{ev} \colon G \to \chi(\chi(G))$, $g \mapsto [\chi \mapsto \chi(g)]$ is a topological isomorphism.)

Sheet 7, Exercise 4: Let F be a non-archimedean local field with residual characteristic q. Let $E|F$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(E|F)$ and degree $n = ef$. (Recall that e is the ramification index and f is the inertia degree.) Further suppose that $(n, q) = 1$ and put $\kappa = (q-1, e)$. Show that

$$H^{-1}(G, \mathcal{O}_E^\times) = \mathbb{Z}/\kappa\mathbb{Z}.$$

We can proceed as follows:

(1) Use the assumption $(q, n) = 1$ to see that $H^{-1}(G, \mathcal{O}_E^\times) \cong H^{-1}(G, \mathfrak{k}_E^\times)$.
(2) Let T be the kernel of the reduction map $G \to \mathrm{Gal}(\mathfrak{k}_E|\mathfrak{k}_F)$. Show that the map $H^{-1}(G, \mathfrak{k}_E^\times) \to H^{-1}(T, \mathfrak{k}_F^\times)$ induced from the norm is an isomorphism.
(3) Conclude the proof by computing $H^{-1}(T, \mathfrak{k}_F^\times)$.

(This can be found as a result in the very nice article [2].)

5. Abstract Class Field Theory

We start with some abstract definitions and observations. The notation is on purpose very suggestive. Indeed we will set up a formal Galois theory for arbitrary pro-finite groups.

Let G be a pro-finite group and let $\{G_K \colon K \in X\}$ denote the family of all open subgroups of G. (Recall that these are precisely closed subgroups with finite index.) We call the index K of G_K field. We write $G = G_{K_0}$ and call K_0 ground field. Formally we write $K \subseteq L$ when $G_K \supseteq G_L$ and set

$$[L \colon K] = [G_K \colon G_L].$$

This is said to be the degree of the extension $L|K$. Further we call $L|K$ normal if G_L is normal in G_K. In this case the factor group $G_{L|K} = G_K/G_L$ is the Galois group of the extension $L|K$. We say $L|K$ is cyclic (resp. abelian or solvable) if $G_{L|K}$ is cyclic (resp. abelian or solvable). If $G_K = \bigcap_{i=1}^n G_{K_i}$, then we write $K = \prod_{i=1}^n K_i$ and call K the composite. Similarly we write $K = \bigcap_{i=1}^n K_i$ if G_K is (topologically) generated by the G_{K_i} in G.

Definition 5.1. Let G be a pro-finite group and A a G-module so that one of the following equivalent conditions holds:

(1) The map
$$G \times A \to A,\ (\sigma, a) \mapsto \sigma a$$
is continuous when A is equipped with the discrete topology;
(2) For every $a \in A$ the group $\{\sigma \in G \colon \sigma a = a\}$ is open in G;
(3) $A = \bigcup_U A^U$, where U runs through all open subgroups of G.

Then we call the pair (G, A) a formation.

Given a formation (G, A) we write

$$A_K = A^{G_K} = \{a \in A \colon \sigma a = a \text{ for all } \sigma \in G_K\},$$

for each $K \in X$. If $L|K$ is normal, then A_L is a $G_{L|K}$-module. Further write

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

Given a tower $N \supseteq L \supseteq K$ of normal extensions we obtain the homomorphism

$$H^q(G_{L|K}, A_L) = H^q(G_{L|K}, A_N^{G_{N|L}}) \xrightarrow{\mathrm{Inf}} H^q(G_{N|K}, A_N),$$

for $q \geq 1$. In our notation this reads

$$H^q(L|K) \overset{\text{Inf}}{\to} H^q(N|K).$$

Similarly we obtain

$$H^q(N|K) = H^q(G_{N|K}, A_N) \overset{\text{Res}}{\to} H^q(G_{N|L}, A_N) = H^q(N|L) \text{ and}$$
$$H^q(N|L) = H^q(G_{N|L}, A_N) \overset{\text{CoRes}}{\to} H^q(G_{N|K}, A_N) = H^q(N|K).$$

The resulting maps will be denoted by Res_L and CoRes_K. Note that if N and L are both normal, then the sequence

$$1 \to H^q(L|K) \overset{\text{Inf}_N}{\to} H^q(N|K) \overset{\text{Res}_L}{\to} H^q(N|L)$$

is exact for $q = 1$. The exactness persists for $q > 1$, if $H^i(N|L) = 1$ for $i = 1, \ldots, q-1$.

If $L|K$ is normal and $\sigma \in G$, then we look at the map

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

This induces an isomorphism $G_{L|K} \to G_{\sigma L|\sigma K}$. Further, $a \mapsto \sigma a$ gives an isomorphism $A_L \to A_{\sigma L}$. Both isomorphisms are compatible and we get an equivalence between the $G_{L|K}$-module A_L and the $G_{\sigma L|\sigma K}$-module $A_{\sigma L}$. We conclude that each $\sigma \in G$ induces an isomorphism

$$H^q(L|K) \overset{\sigma^*}{\to} H^q(\sigma L|\sigma K).$$

Furthermore, the isomorphism σ^* commutes with inflation, restriction and corestriction.

Definition 5.2. A formation (G, A) is called a field formation if for every normal extension we have

$$H^1(L|K) = 1.$$

In view of the Hilbert-Noether theorem this definition is reasonable. Further, note that for field formations we always have that the sequence

$$1 \mapsto H^2(L|K) \overset{\text{Inf}_N}{\to} H^2(N|K) \overset{\text{Res}_L}{\to} H^2(N|L)$$

is exact for a normal tower $N \supseteq L \supseteq K$. Therefore, if the extensions $N \supseteq L \supseteq K$ are normal, then we can view $H^2(L|K)$ as a subset of the group $H^2(N|K)$. This is because inflation

$$H^2(L|K) \overset{\text{Inf}_N}{\to} H^2(N|K)$$

is injective. Taking this to an extreme we observe that the groups $H^2(L|K)$ form a direct group system with respect to inflation. Thus we define the direct limit

$$H^2(\,|K) = \varinjlim_L H^2(L|K)$$

running through all normal extensions of K. We will interpret inflation as an inclusion and abuse notation to write

$$H^2(\,|K) = \bigcup_L H^2(L|K) \text{ and } H^2(L|K) \subseteq H^2(N|K).$$

For an arbitrary extension $K'|K$ we obtain the canonical homomorphism

$$H^2(\,|K) \overset{\text{Res}_{K'}}{\to} H^2(\,|K').$$

This homomorphism is constructed so that the restriction to $H^2(L|K)$ yields the usual homomorphism

$$H^2(L|K) \overset{\text{Res}_{K'}}{\to} H^2(L|K').$$

(To see this is well defined one recalls that Res and Inf behave nicely together.) We get the following theorem:

Theorem 5.1. *Let (G, A) be a field formation and $K'|K$ normal. Then we have the exact sequence*

$$1 \to H^2(K'|K) \overset{\text{Incl}}{\to} H^2(\,|K) \overset{\text{Res}_{K'}}{\to} H^2(\,|K').$$

We will now define the notion of a class formation. This definition might seem ad-hoc right now, but later we will see that it is exactly what we need. Right now let us just say that the axioms are TaylorMade for an application of Tate's Theorem.

Definition 5.3. A formation (G, A) is called a class formation if it satisfies the following axioms:

- **Axiom I:** $H^1(L|K) = 1$ for every normal extension $L|K$. (I.e. we have a field formation.)
- **Axiom II:** For every normal extension $L|K$ there is an isomorphism

  $$\text{inv}_{L|K} \colon H^2(L|K) \to \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z},$$

  called invariance map, with the following properties:
  (1) For a tower of normal extensions $N \supseteq L \supseteq K$ we have

  $$\text{inv}_{L|K} = \text{inv}_{N|K}|_{H^2(L|K)}.$$

  (2) For a tower $N \supseteq L \supseteq K$ where $N|K$ is normal we have

  $$\text{inv}_{N|L} \circ \text{Res}_L = [L\colon K] \cdot \text{inv}_{N|K}.$$

  In other words the diagram

  $$\begin{array}{ccc} H^2(N|K) & \xrightarrow{\text{inv}_{N|K}} & \frac{1}{[N\colon K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow{\scriptstyle \text{Res}_L} & & \downarrow{\scriptstyle \cdot[L\colon K]} \\ H^2(N|L) & \xrightarrow{\text{inv}_{N|L}} & \frac{1}{[N\colon L]}\mathbb{Z}/\mathbb{Z} \end{array}$$

commutes.

The compatibility condition II (1) allows us to obtain an injective homomorphism

$$\mathrm{inv}_K\colon H^2(\,|K) \to \mathbb{Q}/\mathbb{Z}.$$

For this homomorphism we get

$$\mathrm{inv}_L \circ \mathrm{Res}_L = [L\colon K] \cdot \mathrm{inv}_K$$

from II (2).

Theorem 5.2. *Let $N \supseteq L \supseteq K$ be extensions such that $N|K$ is normal. Then we have*

(1) $\mathrm{inv}_{N|K}(c) = \mathrm{inv}_{L|K}(c)$ *if $L|K$ is normal and $c \in H^2(L|K) \subseteq H^2(N|K)$;*
(2) $\mathrm{inv}_{N|L}(\mathrm{Res}_L(c)) = [L\colon K] \cdot \mathrm{inv}_{N|K}(c)$ *for $c \in H^2(N|K)$;*
(3) $\mathrm{inv}_{N|K}(\mathrm{CoRes}_K(c)) = \mathrm{inv}_{N|L}(c)$ *for $c \in H^2(N|L)$ and*
(4) $\mathrm{inv}_{\sigma N|\sigma K}(\sigma^* c) = \mathrm{inv}_{N|K}(c)$ *for $c \in H^2(N|K)$ and $\sigma \in G$.*

Proof. We have observed that (1) and (2) hold above.

To see (3) we first observe that Axiom II implies that $H^2(N|K) \overset{\mathrm{Res}_L}{\to} H^2(N|L)$ is surjective. Thus we choose $\tilde{c}$ so that $\mathrm{Res}_L(\tilde{c}) = c$. With this we get

$$\mathrm{CoRes}_K(c) = \mathrm{CoRes}_K(\mathrm{Res}_L(\tilde{c})) = \tilde{c}^{[L\colon K]}.$$

On the other hand we have

$$\mathrm{inv}_{N|K}(\mathrm{CoRes}_K(c)) = [L\colon K] \cdot \mathrm{inv}_{N|K}(\tilde{c}) = \mathrm{inv}_{N|L}(\mathrm{Res}_L(\tilde{c})) = \mathrm{inv}_{N|L}(c).$$

Finally we need to show (4). Let $\tilde{N}|K_0$ be a normal extension such that $N \subseteq \tilde{N}$. (Here K_0 is the base field of G.) We have $\sigma\tilde{N} = \tilde{N}$, so that the map $a \mapsto \sigma a$ defines a $G_{\tilde{N}|K_0}$-automorphism of the $G_{\tilde{N}|K_0}$-module $A_{\tilde{N}}$. Obviously

$$\sigma^*\colon H^2(\tilde{N}|K_0) \to H^2(\tilde{N}|K_0)$$

is the identity. We can compute

$$\begin{aligned}\mathrm{inv}_{\sigma N|\sigma K}(\sigma^* c) &= \mathrm{inv}_{\tilde{N}|\sigma K}(\sigma^* c) = \mathrm{inv}_{\tilde{N}|K_0}(\mathrm{CoRes}_{K_0}(\sigma^* c)) \\ &= \mathrm{inv}_{\tilde{N}|K_0}(\sigma^* \mathrm{CoRes}_{K_0}(c)) = \mathrm{inv}_{\tilde{N}|K_0}(\mathrm{CoRes}_{K_0} c) = \mathrm{inv}_{\tilde{N}|K}(c) = \mathrm{inv}_{N|K}(c).\end{aligned}$$

□

Definition 5.4. The unique element $u_{L|K} \in H^2(L|K)$ defined by

$$\mathrm{inv}_{L|K}(u_{L|K}) = \frac{1}{[L\colon K]} + \mathbb{Z}$$

is called fundamental class of the normal extension $L|K$.

We record the following compatibility properties of the fundamental classes.

Theorem 5.3. *Let $N \supseteq L \supseteq K$ be two extensions with $N|K$ normal. Then*

(1) *If $L|K$ is also normal, then $u_{L|K} = (u_{N|K})^{[N\colon L]}$;*
(2) $\mathrm{Res}_L(u_{N|K}) = u_{N|L}$*;*
(3) $\mathrm{CoRes}_K(u_{N|L}) = (u_{N|K})^{[L\colon K]}$ *and*
(4) $\sigma^*(u_{N|K}) = u_{\sigma N|\sigma K}$ *for $\sigma \in G$.*

Proof. Exercise. ∎

Applying Tate's Theorem we directly obtain the following crucial theorem.

Theorem 5.4. *For every normal extension $L|K$ and every dimension q the cup-product with the fundamental class $u_{L|K} \in H^2(L|K)$ gives an isomorphism*

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

Applying this to $q = -2$ together with the canonical identifications

$$G_{L|K}^{\mathrm{ab}} \cong H^{-2}(G_{L|K}, \mathbb{Z}) \text{ and } H^0(L|K) = A_K/N_{L|K}A_L$$

gives the general law of reciprocity. We record this in the following theorem.

Theorem 5.5. *For every normal extension $L|K$ we get a canonical isomorphism*

$$\theta_{L|K}\colon G_{L|K}^{\mathrm{ab}} \cong H^{-2}(G_{L|K}, \mathbb{Z}) \overset{u_{L|K}\cup}{\to} H^0(L|K) = A_K/N_{L|K}A_L.$$

This isomorphism is called Nakayama map.

We can give the following explicit description of the Nakayama map:

$$\theta_{L|K}(\sigma G'_{L|K}) = \left[\prod_{\tau\in G_{L|K}} u(\tau,\sigma)\right] \cdot N_{L|K}A_L,$$

where u is a 2-cocycle from the fundamental class $u_{L|K}$ and $\sigma G'_{L|K} \in G_{L|K}^{\mathrm{ab}}$.

The inverse isomorphism

$$\theta_{L|K}^{-1}\colon A_K/N_{L|K}A_L \to G_{L|K}^{\mathrm{ab}}$$

is called the reciprocity isomorphism. Lifting it to A_K gives the norm residue symbol denoted by $(\,, L|K)$. More precisely we have an exact sequence

$$1 \to N_{L|K}A_L \to A_K \overset{(\,,L|K)}{\to} G_{L|K}^{\mathrm{ab}} \to 1.$$

In particular $a \in A_K$ is a norm (from L) if and only if $(a, L|K) = 1$.

Lemma 5.6. *Let $L|K$ be a normal extension. Further, take $a \in A_K$ and $\overline{a} = a \cdot N_{L|K}A_L \in H^0(L|K)$. Then we have*

$$\chi((a, L|K)) = \mathrm{inv}_{L|K}(\overline{a} \cup \delta\chi) \in \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z},$$

for every character $\chi \in \chi(G_{L|K}^{\mathrm{ab}}) = H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$.

Proof. To save chalk we write $\sigma_a = (a, L|K) \in G_{L|K}^{\mathrm{ab}}$ and $\overline{\sigma}_a$ for the corresponding class in $H^{-2}(G_{L|K}, \mathbb{Z})$. By definition we have

$$\overline{a} = u_{L|K} \cup \overline{\sigma_a} \in H^0(G_{L|K}, A_L).$$

Using compatibility with δ and the cup-product we get

$$\overline{a} \cup \delta\chi = (u_{L|K} \cup \overline{\sigma_a}) \cup \delta\chi = u_{L|K} \cup (\overline{\sigma_a} \cup \delta\chi) = u_{L|K} \cup \delta(\overline{\sigma_a} \cup \chi).$$

Further we compute

$$\overline{\sigma_a} \cup \chi = \chi(\sigma_a) = \frac{r}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} = H^{-1}(G_{L|K}, \mathbb{Q}/\mathbb{Z})$$

with $n = [L\colon K]$. Applying δ yields

$$\delta(\chi(\sigma_a)) = n(\frac{r}{n} + \mathbb{Z}) = r + n\mathbb{Z} \in H^0(G_{L|K}, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}.$$

Finally we obtain

$$\overline{a} \cup \delta\chi = u_{L|K} \cup (r + n\mathbb{Z}) = u_{L|K}^r,$$

so that

$$\mathrm{inv}_{L|K}(\overline{a} \cup \delta\chi) = r \cdot \mathrm{inv}_{L|K}(u_{L|K}) = \frac{r}{n} + \mathbb{Z} = \chi(\sigma_a).$$

□

Theorem 5.7. *Let $N \supseteq L \supseteq K$ be extensions of K such that $N|K$ is normal. Then the following diagrams commute:*

(1) *For the canonical projection $\pi\colon G_{N|K}^{\mathrm{ab}} \to G_{L|K}^{\mathrm{ab}}$ we have*

$$\begin{array}{ccc} A_K & \xrightarrow{(\,,N|K)} & G_{N|K}^{\mathrm{ab}} \\ \| & & \downarrow{\scriptstyle \pi} \\ A_K & \xrightarrow{(\,,L|K)} & G_{L|K}^{\mathrm{ab}} \end{array}$$

(2) *For the Verlagerung (i.e.* Ver*) we have*

$$\begin{array}{ccc} A_K & \xrightarrow{(\,,N|K)} & G_{N|K}^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{Incl}} & & \downarrow{\scriptstyle \mathrm{Ver}} \\ A_L & \xrightarrow{(\,,N|L)} & G_{N|L}^{\mathrm{ab}} \end{array}$$

(3) *For the canonical homomorphism $\kappa\colon G_{N|L}^{\mathrm{ab}} \to G_{N|K}^{\mathrm{ab}}$ we have*

$$\begin{array}{ccc} A_L & \xrightarrow{(\,,N|L)} & G_{N|L}^{\mathrm{ab}} \\ \downarrow{\scriptstyle N_{L|K}} & & \downarrow{\scriptstyle \kappa} \\ A_K & \xrightarrow{(\,,N|K)} & G_{N|K}^{\mathrm{ab}} \end{array}$$

(4) *For the maps $\sigma\colon a \mapsto \sigma a$ and $\sigma^*\colon \tau \mapsto \sigma\tau\sigma^{-1}$ we have*

$$\begin{array}{ccc} A_K & \xrightarrow{(\,,N|K)} & G^{\mathrm{ab}}_{N|K} \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma^*} \\ A_{\sigma K} & \xrightarrow{(\,,\sigma N|\sigma K)} & G^{\mathrm{ab}}_{\sigma N|\sigma K} \end{array}$$

Proof. We heavily use compatibility properties of the fundamental classes. And other basic properties of cohomological operators developed earlier.

To see (1) we take $\chi \in \chi(G^{\mathrm{ab}}_{L|K})$. Then we have

$$\begin{aligned}\chi(\pi(a, N|K)) = \mathrm{Inf}\chi((a, N|K)) = \mathrm{inv}_{N|K}(\overline{a} \cup \delta(\mathrm{Inf}\chi)) = \mathrm{inv}_{N|K}(\overline{a} \cup \mathrm{Inf}(\delta\chi)) \\ = \mathrm{inv}_{N|K}(\mathrm{Inf}(\overline{a} \cup (\delta\chi))) = \mathrm{inv}_{N|K}(\overline{a} \cup \delta\chi) = \chi(a, L|K).\end{aligned}$$

Since the inequality holds for all characters χ the arguments must agree.

We turn to (2) and (3). The results will follow from commutativity of the diagrams

$$\begin{array}{ccccccc} A_K & \longrightarrow & H^0(N|K) & \xleftarrow{u_{N|K}\cup} & H^{-2}(G_{N|K}, \mathbb{Z}) & \longrightarrow & G^{\mathrm{ab}}_{N|K} \\ {\scriptstyle\mathrm{Incl}}\downarrow & & \downarrow{\scriptstyle\mathrm{Res}} & & \downarrow{\scriptstyle\mathrm{Res}} & & \downarrow{\scriptstyle\mathrm{Ver}} \\ A_L & \longrightarrow & H^0(N|L) & \xleftarrow{u_{N|L}\cup} & H^{-2}(G_{N|L}, \mathbb{Z}) & \longrightarrow & G^{\mathrm{ab}}_{N|L} \end{array}$$

$$\begin{array}{ccccccc} A_L & \longrightarrow & H^0(N|L) & \xleftarrow{u_{N|L}\cup} & H^{-2}(G_{N|L}, \mathbb{Z}) & \longrightarrow & G^{\mathrm{ab}}_{N|L} \\ \downarrow{\scriptstyle N_{L|K}} & & \downarrow{\scriptstyle\mathrm{CoRes}} & & \downarrow{\scriptstyle\mathrm{CoRes}} & & \downarrow{\scriptstyle\kappa} \\ A_K & \longrightarrow & H^0(N|K) & \xleftarrow[u_{N|K}\cup]{} & H^{-2}(G_{N|K}, \mathbb{Z}) & \longrightarrow & G^{\mathrm{ab}}_{N|K} \end{array}$$

We leave the verification of this as well as the proof of (4) as an exercise. ∎

With these results we already established the key properties of class formations. We can go even further in this abstract setting.

Definition 5.5. A subgroup I of A_K is called norm group if there is a normal extension $L|K$ so that $I = N_{L|K}A_L$.

Theorem 5.8. *Let $L|K$ be a normal extension and let L^{ab} be the maximal abelian extension of K contained in L. Then*

$$N_{L|K}A_L = N_{L^{\mathrm{ab}}|K}A_{L^{\mathrm{ab}}} \subseteq A_K.$$

Proof. We apply the reciprocity law twice:

$$A_K/N_{L|K}A_L \cong G^{\mathrm{ab}}_{L|K} = G_{L^{\mathrm{ab}}|K} \cong A_K/N_{L^{\mathrm{ab}}|K}A_{L^{\mathrm{ab}}}.$$

This suffices since the inclusion $N_{L|K}A_L \subseteq N_{L^{\mathrm{ab}}|K}A_{L^{\mathrm{ab}}}$ is obvious. ∎

Corollary 5.9. *The index* $[A_K\colon N_{L|K}A_L]$ *divides the degree* $[L\colon K]$. *Equality holds if and only if* $L|K$ *is abelian.*

Theorem 5.10. *The map*

$$L \mapsto I_L = N_{L|K}A_L$$

gives an inclusion reversing isomorphism between abelian extensions L *of* K *and norm groups* I *in* A_K. *Indeed we have*

$$I_{L_1} \supseteq I_{L_2} \Leftrightarrow L_1 \subseteq L_2;\ I_{L_1\cdot L_2} = I_{L_1} \cap I_{L_2} \text{ and } I_{L_1\cap L_2} = I_{L_1}\cdot I_{L_2}.$$

Furthermore, every group containing a norm group $I \subseteq A_K$ *is itself a norm group.*

Proof. Let L_1 and L_2 be two abelian extensions. Multiplicativity of the norm implies $I_{L_1\cdot L_2} \subseteq I_{L_1} \cap I_{L_2}$ On the other hand, if $a \in I_{L_1} \cap I_{L_2}$, then $(a, L_1L_2|K)$ has trivial projections $(a, L_1|K) = 1$ and $(a, L_2|K) = 1$. Thus $(a, L_1L_2|K) = 1$. Therefore $a \in I_{L_1\cdot L_2}$. We have seen that $I_{L_1\cdot L_2} = I_{L_1} \cap I_{L_2}$. Combining these observations gives

$$I_{L_1} \supseteq I_{L_2} \Leftrightarrow I_{L_1} \cap I_{L_2} = I_{L_2} = I_{L_1\cdot L_2} \Leftrightarrow [L_1\cdot L_2\colon K] = [L_2\colon K] \Leftrightarrow L_1 \subseteq L_2.$$

Note that we have observed above that every norm group is obtained by norms of an abelian extension. This implies bijectivity. The rest of the result follows at once. ∎

We conclude this section by briefly adding some topological considerations. Note that the groups $G^{\mathrm{ab}}_{L|K}$ form a projective group system. (We can think of this as the group system of all Galois groups of all abelian extensions of K.) We set

$$G^{\mathrm{ab}}_K = \varprojlim G^{\mathrm{ab}}_{L|K}.$$

(This can be thought of as the Galois group of the maximal abelian field over K.) By our compatibility conditions we get the universal norm residue symbol by setting

$$(a, K) = \varprojlim (a, L|K) \in G^{\mathrm{ab}}_K.$$

Note that this element is uniquely determined by $\pi_L(a, K) = (a, L|K)$. It gives a map

$$A_K \overset{(\,,K)}{\to} G^{\mathrm{ab}}_K.$$

Theorem 5.11. *The kernel of* $(\,,K)\colon A_K \to G^{\mathrm{ab}}_K$ *is given by the intersection*

$$D_K = \bigcap_L N_{L|K}A_L.$$

Further, the image is dense in G^{ab}_K *(with respect to the pro-finite topology).*

Proof. We observe that $(a, K) = 1$ if and only if $(a, L|K) = 1$ for all normal extensions $L|K$. But this precisely says $a \in D_K$. To see density of the image we recall that for $\sigma \in G^{\mathrm{ab}}_K$ the sets σH form a basis of neighborhoods of σ, when H runs through all open subgroups of G^{ab}_K. But for H open we know that $G^{\mathrm{ab}}_K/H = G_{L|K}$ is

the Galois group of an abelian extension $L|K$. By surjectivity of the norm residue symbol $(\ , L|K)\colon A_K \to G_{L|K}$ we find $a \in A_K$ with $\pi_L(a,K) = (a, L|K) = \pi_L\sigma$. In other words $(a,K) \in \sigma \cdot H$. ∎

Sheet 8, Exercise 3: Prove Theorem 5.2. More precisely, let (G,A) be a class formation. Let $N \supseteq L \supseteq K$ be normal extensions. Show that

(1) $\mathrm{inv}_{N|K}(c) = \mathrm{inv}_{L|L}(c)$ for $c \in H^2(L|K) \subseteq H^2(N|K)$;
(2) $\mathrm{inv}_{N|L}(\mathrm{Res}_l(c)) = [L\colon K] \cdot \mathrm{inv}_{N|K}(c)$ for $c \in H^2(N|K)$;
(3) $\mathrm{inv}_{N|K}(\mathrm{CoRes}_K(c)) = \mathrm{inv}_{N|L}(c)$ for $c \in H^2(N|L)$ and
(4) $\mathrm{inv}_{\sigma N|\sigma K}(\sigma^* c) = \mathrm{inv}_{N|K}(c)$ for $c \in H^2(N|K)$ and $\sigma \in G$.

Sheet 8, Exercise 4: Show that $(\mathrm{Gal}(\mathbb{C}|\mathbb{R}), \mathbb{C}^\times)$ is a class formation. Write down the invariance map and determine the norm residue symbol.
Sheet 9, Exercise 1: Complete the proof of Theorem 5.10: Suppose that (G,A) is a class formation. Given an abelian extension L of K we set $I_L = N_{L|K}A_L$. Show the following:

(1) Carefully explain why the map $L \mapsto I_L$ is a bijection between (finite) abelian extensions of K and norm groups I in A_K.
(2) $I_{L_1} \cap I_{L_2} = I_{L_1} \cdot I_{L_2}$.
(3) Every group containing a norm group is itself norm group.

6. Local Class Field Theory

We start by investigating the class formation of unramified extensions.

Theorem 6.1. *Let $E|F$ be an unramified extension of non-archimedean local fields. Then*

$$H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times) = 1$$

for all $q \in \mathbb{Z}$.

Proof. We consider the exact sequence

$$1 \to 1 + \mathfrak{p}_E \to \mathcal{O}_E^\times \to \mathfrak{k}_E^\times \to 1$$

of $\mathrm{Gal}(E|F)$-modules. Recall that by Theorem 4.55 we have $H^q(\mathrm{Gal}(E|F), \mathfrak{k}_E^\times) = 1$ for all q. Considering the long exact sequence of cohomology yields

$$H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times) \cong H^q(\mathrm{Gal}(E|F), 1 + \mathfrak{p}_E).$$

Similarly, considering

$$1 \to U_E^n \to U_E^{n-1} \to \mathfrak{k}_E \to 0$$

yields

$$H^q(\mathrm{Gal}(E|F), U_E^n) \cong H^q(\mathrm{Gal}(E|F), U_E^{n-1}).$$

Inductively we obtain $H^q(\mathrm{Gal}(E|F), U_E^n) \cong H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times)$ for all n.

By Lemma 3.18 we have the isomorphism $(\cdot)^m \colon U_E^n \to U_E^{n+v(m)}$ for n sufficiently large.[11] On the level of cohomology this gives us the commutative diagram

$$\begin{array}{ccc} H^q(\mathrm{Gal}(E|F), U_E^n) & \xrightarrow{\cong} & H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times) \\ \downarrow \cong & & \downarrow \\ H^q(\mathrm{Gal}(E|F), U_E^{n+v(m)}) & \xrightarrow{\cong} & H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times) \end{array}$$

Thus we found that for all $m \in \mathbb{N}$ the homomorphism

$$(\cdot)^m \colon H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times) \to H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times)$$

is bijective. However, the elements of $H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times)$ have finite order. This implies the result. ∎

Corollary 6.2. *Let $E|F$ be an unramified extension of local fields, then*

$$\mathcal{O}_F^\times = N_{E|F}\mathcal{O}_E^\times.$$

I.e. every unit is a norm element.

Proof. This follows from the theorem above by considering $q = 0$. ∎

Alternative argument for Theorem 6.1: If F has positive characteristic the proof of Theorem 6.1 has a gap. In this case one can argue for example as follows. First we observe that, since $E|F$ is unramified, the Galois group $\mathrm{Gal}(E|F)$ is cyclic. In particular, it suffices to show that $H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times)$ is trivial for $q = 0, 1$. The case $q = 0$ is easily derived from the fact that the norm map is surjective. (The latter fact can be shown without using Theorem 6.1, so that the argument is not circular!) For $q = 1$ we observe that $E^\times = \mathcal{O}_E^\times \times \varpi^{\mathbb{Z}}$. Since $\mathrm{Gal}(E|F)$ operates trivially on $\varpi^{\mathbb{Z}}$, the cohomology group $H^1(\mathrm{Gal}(E|F), \mathcal{O}_E^\times)$ is a direct summand of $H^1(\mathrm{Gal}(E|F), E^\times)$. One concludes by applying Hilbert 90. ∎

Our goal is to show that the unramified extensions $E|F$ together with the multiplicative groups $E^\times$ form a class formation. To see this we need to define the map inv. We start with the exact sequence

$$1 \to \mathcal{O}_E^\times \to E^\times \xrightarrow{v_E} \mathbb{Z} \to 1.$$

We have already seen that $H^q(\mathrm{Gal}(E|F), \mathcal{O}_E^\times) = 1$, so that by the long cohomological sequence we get an isomorphism

$$H^2(\mathrm{Gal}(E|F), E^\times) \xrightarrow{\overline{v}} H^2(\mathrm{Gal}(E|F), \mathbb{Z}).$$

Further we recall that $\mathbb{Q}$ was cohomologically trivial, so that from $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ we obtain an isomorphism

$$H^2(\mathrm{Gal}(E|F), \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(\mathrm{Gal}(E|F), \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(E|F), \mathbb{Q}/\mathbb{Z}) = \chi(\mathrm{Gal}(E|F)).$$

[11] This technically uses that E and F have characteristic zero. We sketch an alternative argument below.

For every character $\chi \in \chi(\mathrm{Gal}(E|F))$ we have $\chi(\varphi_{E|F}) \in \frac{1}{[E\colon F]}\mathbb{Z}/\mathbb{Z}$. Recall that $\varphi_{E|F}$ is the Frobenius automorphism which generates $\mathrm{Gal}(E|F)$. Thus we get an isomorphism

$$H^1(\mathrm{Gal}(E|F), \mathbb{Q}/\mathbb{Z}) = \chi(\mathrm{Gal}(E|F)) \xrightarrow{\varphi} \frac{1}{[E\colon F]}\mathbb{Z}/\mathbb{Z}.$$

We combine these isomorphisms:

$$H^2(\mathrm{Gal}(E|F), E^\times) \xrightarrow{\overline{v}} H^2(\mathrm{Gal}(E|F), \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(\mathrm{Gal}(E|F), \mathbb{Q}/\mathbb{Z}) \xrightarrow{\varphi} \frac{1}{[E\colon F]}\mathbb{Z}/\mathbb{Z}.$$

Definition 6.1. Let $E|F$ be an unramified extension we define

$$\mathrm{inv}_{E|F}\colon H^2(\mathrm{Gal}(E|F), E^\times) \to \frac{1}{[E\colon F]}\mathbb{Z}/\mathbb{Z}$$

by $\mathrm{inv}_{E|F} = \varphi \circ \delta^{-1} \circ \overline{v}$.

We now set

$$H^q(E|F) = H^q(\mathrm{Gal}(E|F), E^\times).$$

Let K_0 be a fixed underlying local field and let T be the maximal unramified extension of K_0.

Theorem 6.3. *The formation* $(\mathrm{Gal}(T|K_0), T^\times)$ *is a class formation.*

Proof. Axiom I is true due to the Hilbert-Noether theorem. To see both parts of Axiom II we need to verify that the following diagrams commute:

$$\begin{array}{ccccccc}
H^2(E|F) & \xrightarrow{\overline{v}} & H^2(\mathrm{Gal}(E|F), \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(\mathrm{Gal}(E|F), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[E\colon F]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{Incl}} & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Incl}} \\
H^2(N|F) & \xrightarrow{\overline{v}} & H^2(\mathrm{Gal}(N|F), \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(\mathrm{Gal}(N|F), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N\colon F]}\mathbb{Z}/\mathbb{Z}
\end{array}$$

$$\begin{array}{ccccccc}
H^2(N|F) & \xrightarrow{\overline{v}} & H^2(\mathrm{Gal}(N|F), \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(\mathrm{Gal}(N|F), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N\colon F]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \cdot[E\colon F]} \\
H^2(N|E) & \xrightarrow{\overline{v}} & H^2(\mathrm{Gal}(N|E), \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(\mathrm{Gal}(N|E), \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N\colon E]}\mathbb{Z}/\mathbb{Z}
\end{array}$$

where $N \supseteq E \supseteq F$ are two unramified extensions of F. We have already gathered all the necessary properties to see commutativity. We leave it to the reader to collect them together. ∎

This theorem allows us to apply all the results from abstract class field theory. We will give a precise interpretation of these later when also ramified extensions can be included.

As in the abstract setting we write

$$H^2(T|K) = \bigcup_L H^2(L|K),$$

where L runs through all finite unramified extensions of K and obtain an injective homomorphism

$$\mathrm{inv}_K \colon H^2(T|K) \to \mathbb{Q}/\mathbb{Z}.$$

Note that $\mathbb{Q}/\mathbb{Z} = \bigcup_n \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Furthermore, there is precisely one unramified extension $E|F$ of degree n for each natural number n. Since for this extension we have an isomorphism $\mathrm{inv}_{E|F} \colon H^2(E|F) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ we see that

$$H^2(T|K) \equiv \mathbb{Q}/\mathbb{Z}.$$

Furthermore, for each unramified extension $E|F$ we get the exact sequence

$$1 \to N_{E|F}E^\times \to F^\times \overset{(\,,E|F)}{\to} \mathrm{Gal}(E|F) \to 1.$$

(Here we use that $\mathrm{Gal}(E|F)$ is cyclic and in particular abelian.)

Theorem 6.4. *For $E|F$ unramified we have*

$$(a, E|F) = \varphi_{E|F}^{v_F(a)}$$

for all $a \in F^\times$.

Proof. Recall that

$$\chi(a, E|F) = \mathrm{inv}_{E|F}(\overline{a} \cup \delta\chi).$$

For all characters χ we compute

$$\begin{aligned}\chi(a, E|F) = \varphi \circ \delta^{-1} \circ \overline{v}(\overline{a} \cup \delta\chi) &= \varphi \circ \delta^{-1}(v_F(a) \cdot \delta\chi) \\ &= \varphi(v_F(a) \cdot \chi) = v_F(a)\chi(\varphi_{E|F}) = \chi(\varphi_{E|K}^{v_F(a)}).\end{aligned}$$

This gives the desired identity. ∎

This is the natural definition of the norm residue symbol.

Theorem 6.5. *Let F be a local field with uniformizer ϖ. Then the norm group of the unramified extension $E|F$ of degree f is precisely*

$$\mathcal{O}_F^\times \times (\varpi^f).$$

Proof. Note that f is the order of $\varphi_{E|F}$ in $\mathrm{Gal}(E|F)$. An element $a \in F^\times$ is a norm from E if and only if $(a, E|F) = \varphi_{E|F}^{v_F(a)} = 1$. This gives the result. ∎

We now introduce the so called universal norm residue symbol. To do so recall that

$$\mathrm{Gal}(T|F) = \varprojlim_E \mathrm{Gal}(E|F).$$

Thus we can set

$$(a, T|F) = \varprojlim_E (a, E|F).$$

This defines a homomorphism

$$F^\times \overset{(\,,T|F)}{\to} \mathrm{Gal}(T|F).$$

Since the Frobenius elements form a compatible system we can also define the universal Frobenius element

$$\varphi_F = \varprojlim_E \varphi_{E|F} \in \mathrm{Gal}(T|F).$$

(Note that φ_F has infinite order.) The universal symbol is described by the following theorem:

Theorem 6.6. *We have*

$$(a, T|F) = \varphi_F^{v_F(a)}$$

for all $a \in F^\times$. The kernel of $(\,, T|F)\colon F^\times \to \mathrm{Gal}(T|F)$ is the unit group $\mathcal{O}_F^\times$.

Proof. This is Sheet 9, Exercise 2 below. □

We now turn towards more general extensions. Let K_0 be a fixed non-archimedean local field with algebraic closure $\overline{K_0}$. We write $G = \mathrm{Gal}(\overline{K_0}|K_0)$ for the absolute Galois group of K_0. Then $(G, \overline{K_0}^\times)$ is a field formation since by Hilbert 90 we have $H^1(E|F) = 1$. We will need to show that this is a class formation.

Lemma 6.7. *For every finite normal extension $E|F$ we have*

$$(\sharp H^2(E|F)) \mid [E\colon F].$$

Proof. We start by considering the case when $E|F$ is cyclic and of prime degree $p = [E\colon F]$. In this case we need to show that the Herbrand quotient is

$$h(E^\times) = \frac{\sharp H^2(E|F)}{\sharp H^1(E|F)} = \sharp H^2(E|F) = p.$$

Note that we have

$$h(E^\times)^{p-1} = \frac{q_{0,p}(F^\times)^p}{q_{0,p}(E^\times)}.$$

But we have seen in Theorem 3.20 that for local fields[12]

$$q_{0,p}(F^\times) = (F^\times\colon (F^\times)^p)/\sharp F_p = p \cdot q_F^{v_F(p)} \text{ and}$$
$$q_{0,p}(E^\times) = (E^\times\colon (E^\times)^p)/\sharp E_p = p \cdot q_E^{v_E(p)}.$$

[12]For fields F of positive characteristic this holds only if p is co-prime to it. To fix the proof one can consider the exact sequence $1 \to \mathcal{O}_E^\times \to E^\times \to \mathbb{Z} \to 0$ to get $h(E^\times) = h(\mathbb{Z}) \cdot h(\mathcal{O}_E^\times) = p \cdot h(\mathcal{O}_E^\times)$ by multiplicativity of the Herbrand quotient. It remains to show that $h(\mathcal{O}_E^\times) = 1$ for completely ramified $E|F$, which we leave as an exercise.

Note that we have $p = ef$ with $q_E = q_F^f$ and $v_E(p) = e \cdot v_F(p)$. In particular we have $q_E^{v_E(p)} = q_F^{p \cdot v_F(p)}$. Inserting this above gives $h(E^\times)^{p-1} = p^{p-1}$ as claimed.

The general case can be derived as follows. First note that $G_{E|F}$ is solvable. Thus there is a field F' with $F \subseteq F' \subseteq E$ so that the extension $F'|F$ is cyclic of prime order. We have the exact sequence

$$1 \to H^2(F'|F) \to H^2(E|F) \stackrel{\mathrm{Res}}{\to} H^2(E|F').$$

This yields

$$(\sharp H^2(E|F)) \mid (\sharp H^2(E|F')) \cdot (\underbrace{\sharp H^2(F'|F)}_{=[F'\colon F]}).$$

The result follows by induction on the degree of the extension. ∎

Lemma 6.8. *Let $M|F$ be a normal extension containing two extensions $E|F$ and $E'|F$. We assume that $E'|F$ is unramified. In particular $N = E \cdot E'$ is unramified over E. Suppose $[c] \in H^2(E'|F) \subseteq H^2(M|F)$, then $\mathrm{Res}_E([c]) \in H^2(N|E) \subseteq H^2(M|E)$ and we have*

$$\mathrm{inv}_{N|E}(\mathrm{Res}_E([c])) = [E\colon F] \cdot \mathrm{inv}_{E'|F}([c]).$$

Proof. Let f be the inertia degree and e the ramification index of $E|F$, so that $[E\colon F] = ef$. When we view the valuations v_F and v_E extended to M then we have $v_E = e \cdot v_F$. Recalling the definition of the invariant map we obtain the diagram

$$\begin{array}{ccccccc}
H^2(E'|F) & \xrightarrow{\overline{v}_F} & H^2(G_{E'|F}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{E'|F}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[E'\colon F]}\mathbb{Z}/\mathbb{Z} \\
\uparrow{\scriptstyle Incl} & & \downarrow{\scriptstyle \mathrm{Inf}} & & \downarrow{\scriptstyle \mathrm{Inf}} & & \uparrow{\scriptstyle Incl} \\
H^2(M|F) & & H^2(G_{M|F}, \mathbb{Z}) & & H^1(G_{M|F}, \mathbb{Q}/\mathbb{Z}) & & \frac{1}{[M\colon F]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{Res}_L} & & \downarrow{\scriptstyle e\cdot\mathrm{Res}} & & \downarrow{\scriptstyle e\cdot\mathrm{Res}} & & \downarrow{\scriptstyle \cdot[E\colon F]} \\
H^2(N|E) & \xrightarrow[\overline{v}_E]{} & H^2(G_{N|E}, \mathbb{Z}) & \xrightarrow[\delta^{-1}]{} & H^1(G_{N|E}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow[\varphi]{} & \frac{1}{[N\colon E]}\mathbb{Z}/\mathbb{Z}
\end{array}$$

The commutativity of the two left blocks of the diagrams follows directly from the properties of the underlying cohomological constructions. To see that the right hand side commutes we need to see that

$$\varphi_{N|E}|_{E'} = \varphi_{E'|F}^f.$$

To see this we take an integer a in E' and check that

$$\varphi_{N|E}(a) \equiv a^{q_E} \bmod \mathfrak{p}_N = a^{q_F^f} \bmod \mathfrak{p}_N = a^{q_F^f} \bmod \mathfrak{p}_{E'} = \varphi_{E'|F}^f(a).$$

Further, for $\chi \in H^1(G_{E'|F}, \mathbb{Q}/\mathbb{Z})$ we have

$$\begin{aligned}
[E\colon F] \cdot \chi(\varphi_{E'|F}) = e \cdot f \cdot \chi(\varphi_{E'|F}) = e \cdot \chi(\varphi_{E'|F}^f) = e \cdot \chi(\varphi_{N|E}|_{E'}) \\
= e \cdot \mathrm{Inf}\chi(\varphi_{N|E}) = e \cdot (\mathrm{Res} \circ \mathrm{Inf})\chi(\varphi_{N|E}).
\end{aligned}$$

The required identity follows directly. ∎

Theorem 6.9. *Let $E|F$ be a normal extension and let $E'|F$ be the unramified extension of the same degree. Then*

$$H^2(E|F) = H^2(E'|F) \subseteq H^2(\,|F).$$

Proof. Note that it suffices to show

$$H^2(E'|F) \subseteq H^2(E|F).$$

This is because we already know that $[E\colon F] = [E'\colon F] = \sharp H^2(E'|F)$ and $(\sharp H^2(E|F)) \mid [E\colon F]$.

Put $N = E \cdot E'$ so that $N|E$ is an unramified extension. Let $c \in H^2(E'|F) \subseteq H^2(N|F)$. We look at the exact sequence

$$1 \to H^2(E|F) \to H^2(N|F) \overset{\mathrm{Res}_E}{\to} H^2(N|E).$$

We conclude that $c \in H^2(E|F)$ if and only if $\mathrm{Res}_E c = 1$. But the latter is the case if and only if $\mathrm{inv}_{N|E}(\mathrm{Res}_E(c)) = 0$. Thus, since $\mathrm{inv}_{E'|F}(c) \in \frac{1}{[E\colon F]}\mathbb{Z}/\mathbb{Z}$, we need to show that

$$\mathrm{inv}_{N|E}(\mathrm{Res}_E(c)) = [E\colon F] \cdot \mathrm{inv}_{E'|F}(c).$$

But this follows from the more general lemma that we shew before. ∎

The Brauer group is defined by

$$\mathrm{Br}(F) = H^2(\,|F) = \bigcup_E H^2(E|F)$$

where the union is taken over all finite normal extensions L of K. By the theorem the union can be restricted to all unramified extensions. The following theorem is now immediate:

Theorem 6.10. *The Brauer group* $\mathrm{Br}(F)$ *of a non-archimedean field of characteristic* 0 *is canonically isomorphic to* $\mathbb{Q}/\mathbb{Z}$.

Definition 6.2. Let $E|F$ be a normal extension and let $E'|F$ be the unramified extension of equal degree (i.e. $[E\colon F] = [E'\colon F]$), so that $H^2(E|F) = H^2(E'|F)$. Then we define

$$\mathrm{inv}_{E|F}\colon H^2(E|F) \to \frac{1}{[E\colon F]}\mathbb{Z}/\mathbb{Z}$$

by $\mathrm{inv}_{E|F}(c) = \mathrm{inv}_{E'|F}(c)$.

The following central theorem will allow us to use the key theorems from abstract class field theory.

Theorem 6.11. *The formation* $(G, \overline{K_0}^{\times})$ *is a class formation.*

Proof. This follows from the construction. ∎

For each normal extension $E|F$ we obtain a fundamental class

$$u_{E|F} \in H^2(E|F) \text{ so that } \operatorname{inv}_{E|F} u_{E|F} = \frac{1}{[E\colon F]} + \mathbb{Z}.$$

Theorem 6.12 (Main Theorem of Local CFT)**.** *For every normal extension $E|F$ and every q the homomorphism*

$$u_{E|F} \cup \colon H^q(G_{E|F}, \mathbb{Z}) \to H^{q+2}(E|F)$$

is bijective.

Proof. This is a restatement of Theorem 5.4, which in turn is a direct application of Tate's theorem. □

Corollary 6.13. *We have $H^3(E|F) = 1$ and $H^4(E|F) = \chi(G_{E|F})$.*

Proof. Apply the main theorem for $q = 1, 2$. □

Theorem 6.14 (Local Reciprocity Law)**.** *For each normal extension $E|F$ we have the isomorphism*

$$G_{E|F}^{\mathrm{ab}} \cong H^{-2}(G_{E|F}, \mathbb{Z}) \overset{u_{E|F}\cup}{\to} H^0(E|F) = F^\times / N_{E|F} E^\times.$$

The inverse isomorphism gives the exact sequence

$$1 \to N_{E|F} E^\times \to F^\times \overset{(\,,E|F)}{\to} G_{E|F}^{\mathrm{ab}} \to 1.$$

Proof. This is a restatement of Theorem 5.5. □

Recall that $(\,, E|F)$ is the all important norm residue symbol. Unfortunately we don't have an explicit formula for it. But the following compatibility properties will turn out helpful.

Theorem 6.15. *Let $N \supseteq E \supseteq F$ be two extensions of F. Suppose that $N|F$ and $E|F$ are normal then*

$$\begin{array}{ccc} F^\times & \xrightarrow{(\,,N|F)} & G_{N|F}^{\mathrm{ab}} \\ \| & & \downarrow \pi \\ F^\times & \xrightarrow{(\,,E|F)} & G_{E|F}^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} F^\times & \xrightarrow{(\,,N|F)} & G_{N|F}^{\mathrm{ab}} \\ \downarrow & & \downarrow \mathrm{Ver} \\ E^\times & \xrightarrow{(\,,N|E)} & G_{N|E}^{\mathrm{ab}} \end{array}$$

$$\begin{array}{ccc} E^\times & \xrightarrow{(\,,N|E)} & G_{N|E}^{\mathrm{ab}} \\ {\scriptstyle N_{E|F}}\downarrow & & \downarrow \kappa \\ F^\times & \xrightarrow{(\,,N|F)} & G_{N|F}^{\mathrm{ab}} \end{array} \qquad \begin{array}{ccc} F^\times & \xrightarrow{(\,,N|F)} & G_{N|F}^{\mathrm{ab}} \\ {\scriptstyle \sigma}\downarrow & & \downarrow \sigma^* \\ \sigma F^\times & \xrightarrow{(\,,\sigma N|\sigma F)} & G_{\sigma N|\sigma F}^{\mathrm{ab}} \end{array}$$

are commutative for $\sigma \in G$.

Proof. This is a restatement of Theorem 5.7. ∎

Lemma 6.16. *Let $E|F$ be a normal extension, $a \in F^\times$ and $\overline{a} = a \cdot N_{E|F}E^\times \in H^0(E|F)$. Then, for every character $\chi \in \chi(G^{\mathrm{ab}}_{E|F}) = \chi(G_{E|F}) = H^1(G_{E|F}, \mathbb{Q}/\mathbb{Z})$, we have*

$$\chi(a, E|F) = \mathrm{inv}_{E|F}(\overline{a} \cup \delta\chi) \in \frac{1}{[E\colon F]}\mathbb{Z}/\mathbb{Z},$$

where $\delta\chi$ is the image of χ under $\delta\colon H^1(G_{E|F}, \mathbb{Q}/\mathbb{Z}) \to H^2(G_{E|F}, \mathbb{Z})$.

Proof. This dual characterisation of the norm residue map already appeared in Lemma 5.6. ∎

Theorem 6.17. *Let $E|F$ be an abelian extension of non-archimedean local fields. Then the norm residue symbol $(\,, E|F)$ maps the unit group $\mathcal{O}_F^\times$ on the inertia group and U_F^1 is mapped on the ramification group.*

Proof. Let E_T be the maximal unramified subextension between E and F, $f = [E_T\colon F]$ and G_T the inertia group in $G_{E|F}$. For $u \in \mathcal{O}_F^\times$ we have

$$\pi(u, E|F) = (u, E|F) \cdot G_T = (u, E_T|F) = \varphi_{E_T|F}^{v_F(u)} = 1.$$

Thus $(u, E|F) \in G_T$. Suppose now $\tau \in G_T$ and $a \in F^\times$ with $(a, E|F) = \tau$. Then

$$\pi(a, E|F) = (a, E|F) \cdot G_T = 1.$$

Thus $1 = (a, E_T|F) = \varphi_{E_T|F}^{v_F(a)}$. We conclude that $v_F(a) \equiv 0 \bmod f$. Choose $b \in E^\times$ so that $v_E(b) = \frac{1}{f}v_F(a)$, then

$$v_E(N_{E|F}b) = e \cdot v_F(N_{E|F}b) = n \cdot v_E(b) = e \cdot v_F(a).$$

We have seen that $v_F(a) = v_F(N_{E|F}b)$ and we can write $a = u \cdot N_{E|F}(b)$ with $u \in \mathcal{O}_F^\times$. We are done since $(a, E|F) = (u, E|F) = \tau$.

To see the second point we observe that $(U_F^n, E|F) = 1$ for sufficiently large n. Since G_v is the only p-Sylow group of G_T it must be the image of the p-Sylow subgroup U_F^1/U_F^n of $\mathcal{O}_F^\times/U_F^n$. ∎

We can also pass through the usual limiting procedure. Indeed we have

$$G_F^{\mathrm{ab}} = \varprojlim G_{E|F} \text{ for } E|F \text{ abelian}$$

The universal norm residue symbol is then simply

$$(a, F) = \varprojlim (a, E|F) \in G_F^{\mathrm{ab}} \text{ where } a \in F^\times.$$

The so obtained map $F^\times \overset{(\,,F)}{\to} G_F^{\mathrm{ab}}$ is injective.[13] If T is the maximal unramified extension of F, then we obtain

$$(a, F)|_T = (a, T|F) = \varphi_F^{v_F(a)} \in G_{T|F}.$$

[13] This requires a little proof left as an exercise.

Theorem 6.18. *Let F be a non-archimedean local field. Then we get a correspondence*

$$E \mapsto I_E = N_{E|F}E^\times \subseteq F^\times \tag{7}$$

between finite abelian extensions $E|F$ and norm groups in $F^\times$. This correspondence is inclusion reversing and each group containing a norm group is itself a norm group.

Proof. This is Theorem 5.10. ∎

Theorem 6.19 (Existence Theorem)**.** *The norm groups of $F^\times$ are the open subgroups of finite index.*

Proof. First, by the reciprocity law, each norm group I_E has finite index in $F^\times$. Let m be this index, then $(F^\times)^m \subseteq I_E$. But $(F^\times)^m$ is open. In particular we can write I_E as union of translates of $(F^\times)^m$, which are open.

Now we take $I \subseteq F^\times$ open of finite index. Then $(F^\times)^m$ is contained in I for some m. Thus it suffices to show that $(F^\times)^m$ is a norm group. We will do this for the case when the characteristic of F does not divide m using Kummer theory. The remaining case requires a separate argument, which we omit.

We do so first assuming that F contains the mth roots of unity. For every $a \in F^\times$ we write $L_a = F(\sqrt[m]{a})$ and define

$$L = \bigcup_{a\in F^\times} L_a.$$

The so obtained extension of F is finite and abelian. We claim that

$$(F^\times)^m = I_L = \bigcap_{a\in F^\times} I_{L_a}.$$

The degree $[L_a\colon F] = d$ obviously divides m. In particular $(F^\times)^d \subseteq I_{L_a}$. This gives the inclusion $(F^\times)^m \subseteq I_{L_a}$ and thus $(F^\times)^m \subseteq I_L$. Now we use Kummer theory. Indeed we have

$$[F^\times\colon (F^\times)^m] = \sharp G_{L|F} = [F^\times\colon I_L].$$

This gives the desired equality.

Finally, if F does not contain the mth roots of unity, then adjoining them gives a new field F_1. The extension $L|F_1$ constructed above gives $(F_1^\times)^m = N_{L|F_1}L^\times$. Let $\tilde{L}$ be the smallest normal extension of F containing L. Then we get

$$\begin{aligned} N_{\tilde{L}|F}\tilde{L}^\times = N_{F_1|F}(N_{\tilde{L}|F_1}\tilde{L}^\times) \subseteq N_{F_1|F}(N_{L|F_1}L^\times) = N_{F_1|F}((F_1^\times)^m) \\ = (N_{F_1|F}F_1^\times)^m \subseteq (F^\times)^m. \end{aligned}$$

This concludes the proof. ∎

This theorem tells us that for each open subgroup I of finite index in $F^\times$ there is an abelian extension $E|F$ so that $N_{E|F}E^\times = I$. We call E the class field associated to I.

Theorem 6.20. *Let I be a subgroup of $F^\times$. Then the following are equivalent*

(1) *I is a norm group;*
(2) *I is open and of finite index;*
(3) *I is closed and of finite index;*
(4) *I is of finite index.*

Proof. This is Sheet 9, Exercise 3 below. ∎

Theorem 6.21. *Each norm group contains a group of the form*

$$U_F^n \times \langle \varpi^f \rangle$$

for $n \in \mathbb{Z}_{\geq 0}$ and $f \in \mathbb{N}$.

Proof. This follows directly from the topological description of the norm groups and the structure of the multiplicative group $F^\times$. ∎

We now discuss some applications of local class field theory.

Corollary 6.22 (Local Kronecker-Weber Theorem)**.** *Every finite abelian extension of $L|\mathbb{Q}_p$ is contained in a field $\mathbb{Q}_p(\zeta)$, where ζ is a root of unity. (I.e. the maximal abelian extension $\mathbb{Q}_p^{\mathrm{ab}}|\mathbb{Q}_p$ is generated by adjoining all roots of unity.)*

Proof. We find $f, n \in \mathbb{N}$ such that

$$U_{\mathbb{Q}_p}^n \times \langle p^f \rangle \subseteq N_{L|\mathbb{Q}_p} L^\times.$$

Thus by the existence theorem L is contained in the class field of

$$I = U_{\mathbb{Q}_p}^n \times \langle p^f \rangle = [U_{\mathbb{Q}_p}^n \times \langle p \rangle] \cap [\mathcal{O}_{\mathbb{Q}_p}^\times \times \langle p^f \rangle].$$

But to $\mathcal{O}_{\mathbb{Q}_p}^\times \times \langle p^f \rangle$ belongs the unique unramified extension of degree f and $[U_{\mathbb{Q}_p}^n \times \langle p \rangle$ belongs to $\mathbb{Q}_p(\mu_{p^n})$. (The latter was computed in an exercise.) This completes the proof. ∎

This already implies the classical Kronecker-Weber Theorem:

Theorem 6.23 (Kronecker-Weber)**.** *Every finite abelian extension $L|\mathbb{Q}$ is contained in a cyclotomic field $\mathbb{Q}(\mu_n)$. (Here μ_n is the group of nth roots of unity.)*

Proof. Let S be the set of all primes p that are ramified in L. (By Minkowski's theorem this set is non-empty as there are no unramified extensions of $\mathbb{Q}$.) For each p we fix a prime $\mathfrak{P} \subseteq \mathcal{O}_L$ lying over p and consider the completion $L_{\mathfrak{P}}$ with respect to the non-archimedean absolute value obtained from $\mathfrak{P}$.

Since the extension $L_{\mathfrak{P}}|\mathbb{Q}_p$ is abelian we find n_p such that

$$\mathbb{Q}_p \subseteq L_{\mathfrak{P}} \subseteq \mathbb{Q}_p(\mu_{n_p}).$$

Let p^{e_p} be the precise power of p dividing n_p and put

$$n = \prod_{p \in S} p^{e_p}.$$

Put $M = L(\mu_n)$. We claim that $L \subseteq \mathbb{Q}(\mu_n)$. To see this it suffices to show that $M = \mathbb{Q}(\mu_n)$.

Note that $M|\mathbb{Q}$ is abelian and observe that the primes that ramify in $M|\mathbb{Q}$ must lie in S. Consider $\tilde{\mathfrak{P}} \subseteq \mathcal{O}_M$ lying above $\mathfrak{P}$ and thus over p. The completion $M_{\tilde{\mathfrak{P}}}$ of M with respect to the absolute value associated to $\tilde{\mathfrak{P}}$ contains $L_{\mathfrak{P}}$. We have

$$M_{\tilde{\mathfrak{P}}} = L_{\mathfrak{P}}(\mu_n) = \mathbb{Q}_p(\mu_{p^{e_p}n'}) = \mathbb{Q}_p(\mu_{p^{e_p}})\mathbb{Q}_p(\mu_{n'})$$

with $(n', p) = 1$. Since $\mathbb{Q}_p(\mu_{n'})|\mathbb{Q}_p$ is the maximal unramified subextension of $\mathbb{Q}_p(\mu_{p^{e_p}n'})|\mathbb{Q}_p$ we find that the inertia group I_p of $M_{\tilde{\mathfrak{P}}}|\mathbb{Q}_p$ is isomorphic to

$$\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^{e_p}})|\mathbb{Q}_p).$$

In particular $\sharp I_p = \varphi(p^{e_p})$. Put

$$I = \langle I_p \colon p \in S \rangle \subseteq \mathrm{Gal}(M|\mathbb{Q}).$$

The fixed field of I must be unramified and thus equals $\mathbb{Q}$. We conclude that $I = \mathrm{Gal}(M|\mathbb{Q})$. We can therefore compute

$$[M \colon \mathbb{Q}] = \sharp I = \prod_{p \in S} \sharp I_p = \prod_{p \in S} \varphi(p^{e_p}) = \varphi(n) = [\mathbb{Q}(\mu_n) \colon \mathbb{Q}].$$

Since $\mathbb{Q}(\mu_n) \subseteq M$ this establishes the claim and completes the proof. ∎

Theorem 6.24. *Let p be odd, then there are exactly $p + 1$ extensions of $\mathbb{Q}_p$ with degree p.*

Proof. The existence theorem transforms this into the problem of computing index p subgroups of $\mathbb{Q}_p^\times$. Each of these subgroups contains $(\mathbb{Q}_p^\times)^p$, so that we further reduce the problem to computing index p subgroups of $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p$.

Structurally we have

$$\mathbb{Q}_p^\times \cong \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z}.$$

Thus

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^p \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Subgroups are now easily found. Indeed any tuple $(x, y) \neq (0, 0)$ generates a subgroup of order p and (x', y') generates the same subgroup exactly when $(x, y) = z(x', y')$ for $z \in (\mathbb{Z}/p\mathbb{Z})^\times$. We conclude that the number of index p subgroups is precisely

$$(p^2 - 1)/(p - 1) = p + 1.$$

∎

Suppose that F is a non-archimedean local field containing the group of nth roots of unity μ_n. We assume that n is co-prime to the characteristic of F. Let L be the maximal abelian extension of exponent n. This is the class field of the norm group

$$I = (F^\times)^n = N_{L|F}L^\times.$$

In this situation we write the characters multiplicatively so that

$$\chi(\mathrm{Gal}(L|F)) = \mathrm{Hom}(\mathrm{Gal}(L|F), \mu_n).$$

We have the natural pairing

$$\mathrm{Gal}(L|F) \times \chi(\mathrm{Gal}(L|F)) \to \mu_n,\ (\sigma, \chi) \mapsto \chi(\sigma).$$

Recall that using the local reciprocity law we identify $\mathrm{Gal}(L|F) \cong F^\times/(F^\times)^n$. On the other hand Kummer Theory gives an identification $\chi(\mathrm{Gal}(L|F)) = F^\times/(F^\times)^n$. Thus we obtain a natural pairing

$$\left(\frac{\cdot,\cdot}{\mathfrak{p}_F}\right) : F^\times/(F^\times)^n \times F^\times/(F^\times)^n \to \mu_n$$

called the Hilbert symbol.

Lemma 6.25. *Let F be as above. Then for $a, b \in F^\times$ we have*

$$(a, F(\sqrt[n]{b})|F)\sqrt[n]{b} = \left(\frac{a,b}{\mathfrak{p}_F}\right) \cdot \sqrt[n]{b}.$$

Proof. By definition the image of $a \in F^\times/(F^\times)^n$ in $\mathrm{Gal}(L|F)$ is the norm residue symbol

$$\sigma_a = (a, L|K).$$

Similarly the identification from Kummer Theory is given by $b \mapsto \chi_b$ where

$$\chi_b(\tau) = \tau(\sqrt[n]{b})/\sqrt[n]{b}.$$

By definition we have

$$\left(\frac{a,b}{\mathfrak{p}_F}\right) = \chi_b(\sigma_a) = \sigma_a(\sqrt[n]{b})/\sqrt[n]{b}.$$

This gives the desired result. ∎

Example 6.26. For $n = 2$ it can be shown that

$$\left(\frac{a,b}{\mathfrak{p}_F}\right) = 1$$

if and only if

$$ax^2 + by^2 = z^2 \tag{8}$$

has a non-trivial solution $x, y, z \in F$. Because $\mu_2 = \{\pm 1\}$ this determines the Hilbert symbol completely.

This brings us to the end of our discussion of local class field theory. A major flaw is that we did not describe the norm residue symbol explicitly. This can be done but would take us too far afield. For later use we only write down some pieces of the full picture without proof:

- **Theorem:** Let $a = u \cdot p^m \in \mathbb{Q}_p^\times$, where u is a unit. Further let ζ be a primitive p^nth root of unity. Then
$$(a, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p)\zeta = \zeta^r \tag{9}$$
where r is determined modulo p^n by $r \equiv u^{-1} \bmod p^n$.
- **Theorem:** The norm groups of purely ramified (abelian) extensions $E|F$ contain $U_F^n \times \langle \varpi \rangle$ for some $n \in \mathbb{Z}_{\geq 0}$.
- **Definition:** Let $E|F$ be an abelian extension and let n be the smallest non-negative integer so that $U_F^n \subseteq N_{E|F}E^\times$. The conductor $\mathfrak{f}$ of $E|F$ is $\mathfrak{p}^n$.
- **Theorem:** An abelian extension $E|F$ is unramified if and only if $\mathfrak{f} = 1$.

Sheet 8, Exercise 1: Let $E|F$ be a finite Galois extension of non-archimedean local fields and write $G = \mathrm{Gal}(E|F)$. Let n be the degree of the extension and q the residue charcteristic. We assume $(q, n) = 1$.

(1) Suppose that E is the bi-quadratic extension of F and assume that the residue characteristic is odd. Show that $H^{-1}(G, E^\times) = \mathbb{Z}/2\mathbb{Z}$. (Why is there only one bi-quadratic extension?)
(2) Show that in general $H^{-1}(G, E^\times)$ depends only on the (isomorphism class of the) Galois group G and not on the extension E.
(3) Show that G is abelian but not cyclic, then $H^{-1}(G, E^\times)$ is non-trivial.

To solve this exercise one can use Sheet 7,Exercise 4 above as well as the general reciprocity theorem (i.e. Theorem 6.14).

Sheet 9, Exercise 2:

(1) Prove Theorem 6.6 from the lecture (notes): Let F be a non-archimedean local field and let T be its maximal unramified extension. We have
$$(a, T|F) = \varphi_F^{v_F(a)}$$
for all $a \in F^\times$. The kernel of $(\,, T|F)\colon F^\times \to \mathrm{Gal}(T|F)$ is the unit group $\mathcal{O}_F^\times$.
(2) Show that the universal norm residue symbol
$$(\,, F)\colon F^\times \to G_F^{\mathrm{ab}}$$
is injective.[14]

Sheet 9, Exercise 3: Prove Theorem 6.20: Let F be a non-archimedean local field. Let I be a subgroup of $F^\times$ then the following are equivalent

(1) I is a norm group;
(2) I is open and of finite index;
(3) I is closed and of finite index;
(4) I is of finite index.

Sheet 10, Exercise 1: Show that there are 7 abelian extensions of $\mathbb{Q}_2$ of degree 2.

[14]It can be assumed that F has characteristic 0 for convenience.

7. Adeles and Ideles

Throughout let K be a number field with ring of integers $\mathcal{O}_K$. (Function fields can be treated similarly.)

We start by introducing some notation:

- Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be a prime ideal of $\mathcal{O}_K$. We write $v_\mathfrak{p}$ for the corresponding (normalised) non-archimedean valuation on K and we define the absolute value by $|x|_\mathfrak{p} = \mathrm{Nr}_{K|\mathbb{Q}}(\mathfrak{p})^{-v_\mathfrak{p}(x)}$. The completion of K with respect to $|\cdot|_\mathfrak{p}$ will be denoted by $K_\mathfrak{p}$. We call $v_\mathfrak{p}$ a finite place of K.
- Let $v\colon K \to \mathbb{R}$ be a real embedding of K, then we associate the absolute value $|x|_v = |v(x)|$. The corresponding completion is $K_v = \mathbb{R}$. We call v a real infinite place of K.
- Let $v\colon K \to \mathbb{C}$ be a complex embedding of K, then we associate the absolute value $|x|_v = |v(x)|^2$. The corresponding completion is $K_v = \mathbb{C}$. We call v a complex infinite place of K. (We encounter them always in pairs v and $\overline{v}$ and we do not distinguish these two!)

Together these make up all the *places of* K, which we usually denote by v. We have the following result:

Lemma 7.1. *For $x \in K^\times$ we have*

$$\prod_v |x|_v = 1,$$

where the product is taken over all places of K.

Proof. After observing that the product is actually finite (and therefore well defined), we arrange it as

$$\prod_v |x|_v = \underbrace{\prod_{v|\infty} |x|_v}_{=|N_{K|\mathbb{Q}}(x)|_\infty} \cdot \prod_p \underbrace{\prod_{\mathfrak{p}|p} |x|_\mathfrak{p}}_{=|N_{K|\mathbb{Q}}(x)|_p}$$

The claim is thus reduced to the case where $K = \mathbb{Q}$, which is easily verified. (Note that we have crucially used that the absolute values are appropriately normalized!) ∎

Let S be a set of places containing all infinite (or archimedean) ones. The S-units of K are defined by

$$K^S = \{a \in K^\times \colon |a|_v = 1 \text{ for all } v \notin S\}.$$

The name comes from the fact that $a \in K^S$ is a unit in the ring of integers of K_v for all $v \notin S$. Note that if $S = S_\infty$ contains precisely the infinite places, then we have

$$K^{S_\infty} = \mathcal{O}_K^\times.$$

To unify notation we set

$$\mathcal{O}_v = \begin{cases} \mathcal{O}_{\mathfrak{p}} & \text{if } v = v_{\mathfrak{p}} \text{ is finite,} \\ K_v & \text{else} \end{cases} \quad \text{and } U_v^n = \begin{cases} U_{K_{\mathfrak{p}}}^n & \text{if } v = v_{\mathfrak{p}} \text{ is finite,} \\ \mathbb{R}^+ & \text{if } v \mid \infty \text{ is real,,} \\ \mathbb{C}^\times & \text{if } v \mid \infty \text{ is compex.} \end{cases}$$

As usual we will put $U_v^0 = \mathcal{O}_v^\times$.

We recall two important facts from algebraic number theory:

(1) The ideal class group $\mathcal{C}_K = \mathcal{J}_K/\mathcal{P}_K$ is finite. (Here $\mathcal{J}_K$ is the group of fractional ideals of K and $\mathcal{P}_K$ is the group of principal ideals.)
(2) The group of S-units K^S is finitely generated and has rank $\sharp S - 1$. (This is a slight generalization of Dirichlet's unit theorem.)

Consider now a finite extension $L|K$. We usually write $\mathfrak{P}$ for ideals in $\mathcal{O}_L$. We write $\mathfrak{P} \mid \mathfrak{p}$, if $\mathfrak{P}$ lies above $\mathfrak{p}$. We get a corresponding extension of completions:

$$L_{\mathfrak{P}} \supseteq K_{\mathfrak{p}}.$$

(Places of L will be denoted by w and as in the finite place we write $w \mid v$ if w lies above v. Of course we have $L_w \supseteq K_v$ as above.)

We have the classical decomposition

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$$

satisfying

$$\sum_{i=1}^{r} [L_{\mathfrak{P}_i} \colon K_{\mathfrak{p}}] = [L \colon K] \text{ and } [L_{\mathfrak{P}_i} \colon K_{\mathfrak{p}}] = e_i \cdot f_i.$$

In the completed fields we have the identity $\widehat{\mathfrak{P}_i}^e = \widehat{\mathfrak{p}}$.

Assuming that $L|K$ is a Galois extension with Galois group $\mathrm{Gal}(L|K)$ allows us to observe that for $\sigma \in \mathrm{Gal}(L|K)$ we have $\sigma\mathfrak{P}_i = \mathfrak{P}_{i_\sigma}$ for some $1 \leq i_\sigma \leq r$. Therefore σ induces a $K_{\mathfrak{p}}$-isomorphism

$$\sigma^* \colon L_{\mathfrak{P}_i} \to L_{\sigma\mathfrak{P}_i} = L_{\mathfrak{P}_{i_\sigma}}.$$

In the special case, when $\sigma\mathfrak{P}_i = \mathfrak{P}_i$ (i.e $i = i_\sigma$), we obtain an automorphism, so that $\sigma^* \in \mathrm{Gal}(L_{\mathfrak{P}_i}|K_{\mathfrak{p}})$. This way we can identify the Galois group $\mathrm{Gal}(L_{\mathfrak{P}_i}|K_{\mathfrak{p}})$ with the decomposition group $G_{\mathfrak{P}_i}$. We thus have

$$\mathrm{Gal}(L_{\mathfrak{P}_i}|K_{\mathfrak{p}}) = G_{\mathfrak{P}_i} = \{\sigma \in \mathrm{Gal}(L|K) \colon \sigma\mathfrak{P}_i = \mathfrak{P}_i\} \subseteq \mathrm{Gal}(L|K).$$

We now introduce the adeles and ideles. In particular the ideles will be of great importance to us, because they will serve as the correct module to set up the global class formation.

Definition 7.1. Let S be a finite set of places of K. Then we define

$$\mathbb{A}_K^S = \prod_{v \in S} K_v \times \prod_{v \notin S} \mathcal{O}_v \subseteq \prod_v K_v.$$

This is called the group of S-adeles. The adele group is given by

$$\mathbb{A}_K = \bigcup_S \mathbb{A}_K^S.$$

We write $K \subseteq \mathbb{A}_K$ for the diagonal embedding $x \mapsto (x)_v$.

Remark 7.2. Note that the S-adeles naturally carry the product topology, turning them into locally compact groups (with respect to componentwise addition). We make $\mathbb{A}_K$ a locally compact topological group by declaring that the S-adeles are open subgroups. One can show that

$$K + \mathbb{A}_K^{S_\infty} = \mathbb{A}_K.$$

(This is nothing more than the chinese remainder theorem.) It follows immediately that $\mathbb{A}_K/K$ is compact.

Definition 7.2. Let S be a finite set of places of K. Then we define

$$\mathbb{A}_K^{\times,S} = \prod_{v\in S} K_v^\times \times \prod_{v\notin S} \mathcal{O}_v^\times \subseteq \prod_v K_v^\times.$$

This is called the group of S-ideles. These are locally compact topological groups with respect to pointwise multiplication and the product topology. The idele group is given by

$$\mathbb{A}_K^\times = \bigcup_S \mathbb{A}_K^{\times,S}.$$

This is a locally compact topological group containing the S-ideles as open subgroups. We write $K^\times \subseteq \mathbb{A}_K^\times$ for the diagonal embedding $x \mapsto (x)_v$ and we call $\mathbb{C}_K = \mathbb{A}_K^\times/K^\times$ the idele class group of K.[15]

For each place v of K we have the embedding $\iota_v \colon K_v^\times \to \mathbb{A}_K^\times$ given by

$$[\iota_v(x)]_w = \begin{cases} x & \text{if } v = w, \\ 1 & \text{else.} \end{cases}$$

The induced map $\overline{\iota_v} \colon K_v^\times \to \mathbb{C}_K$ sending $x \in K_v^\times$ to $\iota_v(x)\cdot K^\times \in \mathbb{C}_K$ is a topological embedding.

Note that we recover the S-units of K by taking the intersection of $K^\times$ (embedded diagonally as always) with the S-ideles:

$$K^S = K^\times \cap \mathbb{A}_K^{\times,S} \subseteq \mathbb{A}_K^\times.$$

[15]It is easy to see that $K^\times$ (embedded diagonally) is discrete in $\mathbb{A}_K^\times$. Indeed this is clear because the neighbourhood

$$\{a \in \mathbb{A}_K^\times \colon |a_v - 1|_v < 1 \text{ for } v \in S,\ |a_v|_v = 1 \text{ for } v \notin S\}$$

of 1 does not contain any other element of $K^\times$. Thus $\mathbb{C}_K$ equipped with the quotient topology is itself a locally compact (i.p. Hausdorff) topological group. The projection $\mathbb{A}_K^\times \to \mathbb{C}_K$ is continuous and maps open sets to open sets.

Recall that the non-zero fractional ideals of $\mathcal{O}_K \subseteq K$ form a group denoted by $\mathcal{J}_K$. The subgroup of principal (fractional) ideals is denoted by $\mathcal{P}_K$ and we obtain the class group

$$\mathcal{C}_K = \mathcal{J}_K/\mathcal{P}_K.$$

In contrast to the idele class group $\mathbb{C}_K$, the class group $\mathcal{C}_K$ is finite. The following results will show that they are still closely related.

Theorem 7.3. *We have the isomorphisms*

$$\mathbb{A}_K^\times/\mathbb{A}_K^{\times,S_\infty} \cong \mathcal{J}_K \text{ and } \mathbb{A}_K^\times/\mathbb{A}_K^{\times,S_\infty}K^\times \cong \mathcal{C}_K.$$

Proof. Given an idele $a \in \mathbb{A}_K^\times$ we define the corresponding ideal

$$\prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}.$$

(Note that this product is actually finite.) We obtain a homomorphism $\iota\colon \mathbb{A}_K^\times \to \mathcal{J}_K$ with kernel $\mathbb{A}_K^{\times,S_\infty}$. This gives the first isomorphism.

The second isomorphism is easily obtained by computing the kernel of

$$\mathbb{A}_K^\times \to \mathcal{C}_K,\ a \mapsto \iota(a)\cdot\mathcal{P}_K.$$

Indeed we observe that $\iota(a) \in \mathcal{P}_K$ precisely when $\iota(a) = (x)$ for $x \in K^\times$. This implies that

$$\prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_\mathfrak{p}(x)}.$$

We obtain that $v_\mathfrak{p}(a_\mathfrak{p}x^{-1}) = 0$ for all $\mathfrak{p} \nmid \infty$. This can be rewritten as

$$a \in x\cdot\mathbb{A}_K^{\times,S_\infty} \subseteq \mathbb{A}_K^{\times,S_\infty}K^\times.$$

□

Theorem 7.4. *We have*

$$\mathbb{A}_K^\times = \mathbb{A}_K^{\times,S}\cdot K^\times \text{ and } \mathbb{C}_K = \mathbb{A}_K^{\times,S}\cdot K^\times/K^\times,$$

where $S \supset S_\infty$ is a finite but sufficiently large set of places.

Proof. Take class group representatives $\mathfrak{a}_1, \ldots, \mathfrak{a}_{h_K} \in \mathcal{J}_K$. We can take

$$S = \{\mathfrak{p} \mid \prod_{i=1}^{h_K} \mathfrak{a}_i\} \cup S_\infty.$$

Indeed we morally write

$$\mathbb{A}_K^\times = \mathcal{J}_K\cdot\mathbb{A}_K^{\times,S_\infty} = \mathcal{C}_K\mathbb{A}_K^{\times,S_\infty}\cdot K^\times \subseteq \mathbb{A}_K^\times\cdot K^\times.$$

It is not hard to make this rigorous. □

Remark 7.5. We can equip $\mathbb{A}_K^\times$ with the modulus

$$|a|_{\mathbb{A}} = \prod_v |a_v|_v.$$

By construction all these products are actually finite and thus well defined. We define

$$\mathbb{A}_K^1 = \{a \in \mathbb{A}_K^\times \colon |a|_{\mathbb{A}} = 1\}.$$

We see that $K^\times \subseteq \mathbb{A}_K^1$ so that we can define $\mathbb{C}_K^1 = \mathbb{A}_K^1/K^\times$. It can be shown that this group is compact. (This is essentially equivalent to the finiteness of the classical class group.)

It remains to study the relation between the idele groups $\mathbb{A}_K^\times$ and $\mathbb{A}_L^\times$ when $L|K$ is a finite extension. We first define an injective homomorphism (interpreted as embedding)

$$\mathbb{A}_K^\times \ni a \mapsto a' \in \mathbb{A}_L^\times \text{ with } a'_w = a_v \text{ for } w \mid v.$$

Thus, the idea is to embed K_v diagonally in $\prod_{w|v} L_w$. Next suppose that $L|K$ is normal with Galois group $\mathrm{Gal}(L|K)$. We define the following action of the Galois group on the ideles: Given $a \in \mathbb{A}_L^\times$ and $\sigma \in \mathrm{Gal}(L|K)$ we define $\sigma a \in \mathbb{A}_L^\times$ by

$$(\sigma a)_{\mathfrak{P}} = \sigma(a_{\sigma^{-1}\mathfrak{P}}).$$

(Note that this induces the usual Galois action on the (fractional) ideal group $\mathcal{J}_L$.)

Remark 7.6. Algebraically we can write $\mathbb{A}_L = \mathbb{A}_K \otimes_K L$ and then the $\mathrm{Gal}(L|K)$ action is given by $\sigma(a \otimes l) = a \otimes \sigma(l)$. This is because (for separable extensions) there is an isomorphism

$$K_{\mathfrak{p}} \otimes_K L \to L_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}.$$

Theorem 7.7. *Let $L|K$ be a normal extension, then*

$$(\mathbb{A}_L^\times)^{\mathrm{Gal}(L|K)} = \mathbb{A}_K^\times.$$

Proof. Obviously $\mathrm{Gal}(L|K)$ acts trivially on $\mathbb{A}_K^\times$ (when viewed inside $\mathbb{A}_L^\times$).

Now take $a \in \mathbb{A}_L^\times$ with $\sigma a = a$ for all $\sigma \in \mathrm{Gal}(L|K)$. We first observe that by definition we must have

$$(\sigma a)_{\mathfrak{P}} = \sigma(a_{\sigma^{-1}\mathfrak{P}}) = a_{\mathfrak{P}}.$$

We get for each $\sigma \in G_{\mathfrak{P}}$ that $\sigma a_{\mathfrak{P}} = a_{\mathfrak{P}}$. Using the identification $G_{\mathfrak{P}} = \mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$ this yields $\mathfrak{a}_{\mathfrak{P}} \in K_{\mathfrak{p}}$. Now if $\mathfrak{P}$ and $\mathfrak{P}'$ are two places over $\mathfrak{p}$ we find $\sigma \in \mathrm{Gal}(L|K)$ with $\sigma^{-1}\mathfrak{P} = \mathfrak{P}'$. This directly implies $a_{\mathfrak{P}} = a_{\mathfrak{P}'}$, since we already now that both components are in $K_{\mathfrak{p}}$. ∎

Theorem 7.8. *Let $L|K$ be any extension. Then*

$$L^\times \cap \mathbb{A}_K^\times = K^\times.$$

Proof. Clearly $K^\times \subseteq L^\times \cap \mathbb{A}_K^\times$. For the other inclusion we take a normal extension $\tilde{L}|K$ containing L. Taking $a \in \tilde{L}^\times \cap \mathbb{A}_K^\times$ we observe that a is fixed by $\mathrm{Gal}(\tilde{L}|K)$. But this implies that $a \in (\tilde{L}^\times)^{\mathrm{Gal}(\tilde{L}|K)} = K^\times$ and we are done. ∎

This allows us to define the injective homomorphism

$$\iota\colon \mathbb{C}_K \to \mathbb{C}_L,\ a \cdot K^\times \mapsto a \cdot L^\times.$$

We therefore view $\mathbb{C}_K$ as a subgroup of $\mathbb{C}_L$. (Note that $a \cdot L^\times \in \mathbb{C}_L$ lies in $\mathbb{C}_K$ precisely when $a \cdot L^\times = a' \cdot L^\times$ with $a' \in \mathbb{A}_K^\times$.)

Theorem 7.9. *Let $L|K$ be a normal extension. Then $\mathbb{C}_L$ is a $\mathrm{Gal}(L|K)$-module and we have*

$$\mathbb{C}_L^{\mathrm{Gal}(L|K)} = \mathbb{C}_K.$$

Proof. The action is simply given by $\sigma(a \cdot L^\times) = \sigma(a) \cdot L^\times$. To see the Galois descent property we recall the exact sequence

$$1 \to (L^\times)^{\mathrm{Gal}(L|K)} \to (\mathbb{A}_L^\times)^{\mathrm{Gal}(L|K)} \to \mathbb{C}_L^{\mathrm{Gal}(L|K)} \to H^1(\mathrm{Gal}(L|K), L^\times).$$

By Hilbert 90 we have $H^1(\mathrm{Gal}(L|K), L^\times) = 1$, so that we obtain a short exact sequence. We are obviously done since $(L^\times)^{\mathrm{Gal}(L|K)} = K^\times$ and $(\mathbb{A}_L^\times)^{\mathrm{Gal}(L|K)} = \mathbb{A}_K^\times$. ∎

Remark 7.10. Note that these facts are all not true in general on ideal level:

- A non-principal ideal of K can be principal in some extension L.
- The classical ideal class group does not have Galois descent. To be more precise let $L|K$ be a Galois extension. Then the homomorphism $\mathcal{C}_K \to \mathcal{C}_L^{\mathrm{Gal}(L|K)}$ is in general neither injective nor surjective.

Sheet 10, Exercise 4: Let K be a global field with adele ring $\mathbb{A}_K$ and idele ring $\mathbb{A}_K^\times$.

(1) Show that the embedding $\mathbb{A}_K^\times \to \mathbb{A}_K$ is continuous.
(2) Show that the topology on $\mathbb{A}_K^\times$ is different from the subspace topology obtained via $\mathbb{A}_K^\times \subseteq \mathbb{A}_K$.
(3) Show that the topology on $\mathbb{A}_K^\times$ coincides with subspace topology obtained using the embedding

$$\mathbb{A}_K^\times \to \mathbb{A}_K \times \mathbb{A}_K,\ x \mapsto (x, x^{-1}),$$

where $\mathbb{A}_K \times \mathbb{A}_K$ is equipped with the product topology.

Sheet 11, Exercise 3: Let $L|K$ be a finite normal extension of algebraic number fields with ideles $\mathbb{A}_L^\times$ (resp. $\mathbb{A}_K^\times$).

(1) Show that the *norm* $N_{G_{L|K}}$ defines an homomorphism from $\mathbb{A}_L^\times \to \mathbb{A}_K^\times$.
(2) Show that for every place v of K we have

$$(N_{G_{L|K}} a)_v = \prod_{w|v} N_{L_w|K_v}(a_w), \text{ for } a \in \mathbb{A}_L^\times.$$

(3) Show that $N_{G_{L|K}}x = N_{L|K}x \in K^\times$, where $x \in L^\times \subseteq \mathbb{A}_L^\times$ is embedded diagonally as usual and $N_{L|K}$ is the usual norm.

Sheet 11, Exercise 4: Let $n \in \mathbb{N}$ be a natural number and let K be an algebraic number field containing the nth roots of unity μ_n. Show that

$$[K^S \colon (K^S)^n] = n^{\sharp S},$$

where S is a finite set of places containing all archimedean ones. (Hint: The Generalized Dirichlet Unit Theorem can be used here.)

8. Global Class Field Theory

We will continue to use notation from the previous section. In particular K is a number field. If we have an extension $L|K$ and S is a finite set of places of K, then we write $\overline{S}$ for the set of places that lie above those in S. We abuse notation and write $\mathbb{A}_L^{\times,S} = \mathbb{A}_L^{\times,\overline{S}}$.

For a place v (resp. $\mathfrak{p}$) of K and $S = \{v\}$ (resp. $\{\mathfrak{p}\}$) we introduce the notation

$$\mathbb{A}_{L,v}^\times = \prod_{w|v} L_w^\times \text{ (resp. } \mathbb{A}_{L,\mathfrak{p}}^\times = \prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}^\times).$$

Similarly we set

$$\mathcal{O}_{L,v}^\times = \prod_{w|v} \mathcal{O}_w^\times \text{ (resp. } \mathcal{O}_{L,\mathfrak{p}}^\times = \prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{\mathfrak{P}}^\times).$$

In particular we have

$$\mathbb{A}_L^{\times,S} = \prod_{v\in S} \mathbb{A}_{L,v}^\times \times \prod_{v\notin S} \mathcal{O}_{L,v}^\times.$$

8.1. **Cohomological Preparations.**

Theorem 8.1. *Let w be a place of L lying over v. Then we have*

$$H^q(G_{L|K}, \mathbb{A}_{L,v}^\times) \cong H^q(G_w, L_w^\times),$$

where G_w is the decomposition group of w over K. Note that we interpret G_w as the Galois group of the extension $L_w|K_v$. If v is a finite unramified place, then

$$H^q(G_{L|K}, \mathcal{O}_{L,v}^\times) = 1$$

for all q.

Proof. We write

$$\mathbb{A}_{L,v}^\times = \prod_{\sigma\in G/G_w} L_{\sigma w}^\times = \prod_{\sigma\in G/G_w} \sigma L_w^\times.$$

Similarly we have

$$\mathcal{O}_{L,v}^\times = \prod_{\sigma\in G/G_w} \sigma \mathcal{O}_{L,w}.$$

Thus, by the Lemma of Shapiro (Theorem 4.35) we have

$$H^q(G_{L|K}, \mathbb{A}_{L,v}^\times) \cong H^q(G_w, L_w^\times) \text{ and } H^q(G_{L|K}, \mathcal{O}_{L,v}^\times) \cong H^q(G_w, \mathcal{O}_{L,w}^\times).$$

The triviality of the second cohomology group follows from Theorem 6.1 of local class field theory. ∎

Theorem 8.2. *Let S be a finite set of places containing S_∞ as well as all ramified places. Then we have*

$$H^q(G_{L|K}, \mathbb{A}_L^{\times,S}) \cong \prod_{v\in S} H^q(G_w, L_w^\times) \text{ and}$$
$$H^q(G_{L|K}, \mathbb{A}_L^\times) \cong \bigoplus_v H^q(G_w, L_w^\times).$$

Proof. The first part follows directly from the previous result and Theorem 4.14. For the second isomorphism we observe that $\mathbb{A}_L^\times = \bigcup_S \mathbb{A}_L^{\times,S}$. We can compute

$$H^q(G_{L|K}, \mathbb{A}_L^\times) \cong \varinjlim_S H^q(G_{L|K}, \mathbb{A}_L^{\times,S}) \cong \bigoplus_v H^q(G_w, L_w^\times).$$

∎

Remark 8.3. Unraveling the construction of Shapiro's Lemma we find that the projections $H^q(G_{L|K}, \mathbb{A}_{L,v}^\times) \to H^q(G_w, L_w^\times)$ are given by

$$H^q(G_{L|K}, \mathbb{A}_L^\times) \overset{\text{Res}}{\to} H^q(G_w, \mathbb{A}_L^\times) \overset{\overline{\pi}}{\to} H^q(G_w, L_w^\times),$$

where $\overline{\pi}$ is induced by the projection $\mathbb{A}_L^\times \to L_w^\times$. Patching these together precisely gives the isomorphism in the previous theorem.

The theorem allows us to introduce the following notation. Given $c \in H^q(G_{L|K}, \mathbb{A}_L^\times)$ we attach v-components c_v using the isomorphism above. The local components are almost all trivial and completely determine c.

Theorem 8.4. *Let $N \supset L \supset K$ normal extensions and $w'|w|v$ places in the respective fields. We have*

$$(\text{Inf}_N c)_v = \text{Inf}_{N_{w'}}(c_v) \text{ for } c \in H^q(G_{L|K}, \mathbb{A}_L^\times) \text{ and } q \geq 1,$$
$$(\text{Res}_L c)_w = \text{Res}_{L_w}(c_v) \text{ for } c \in H^q(G_{N|K}, \mathbb{A}_N^\times) \text{ and}$$
$$(\text{CoRes}_K c)_v = \sum_{w|v} \text{CoRes}_{K_v}(c_w) \text{ for } c \in H^q(G_{N|L}, \mathbb{A}_N^\times).$$

Proof. This is Sheet 11, Exercise 2 below. (Note that the statement of the Exercise also includes a clarification on how the statement is to be interpreted.) ∎

The following direct corollary of the *complete localisation* of idele group cohomology is **not to be confused** with the Hasse Norm Theorem, which we will see later.

Corollary 8.5. *An idele $a \in \mathbb{A}_K^\times$ is a norm of an idele $b \in \mathbb{A}_L^\times$ if and only if it is locally a norm everywhere.*

Proof. We have

$$H^0(G_{L|K}, \mathbb{A}_L^\times) = \mathbb{A}_K^\times / N_{G_{L|K}} \mathbb{A}_L^\times \text{ and } H^0(G_\mathfrak{P}, L_\mathfrak{P}^\times) = K_\mathfrak{p}^\times / N_{G_\mathfrak{P}} L_\mathfrak{P}^\times.$$

Putting this together we obtain

$$\mathbb{A}_K^\times / N_{G_{L|K}} \mathbb{A}_L^\times = \bigoplus_\mathfrak{p} K_\mathfrak{p}^\times / N_{G_\mathfrak{P}} L_\mathfrak{P}^\times.$$

□

Similarly one can see that

$$H^1(G_{L|K}, \mathbb{A}_L^\times) = H^3(G_{L|K}, \mathbb{A}_L^\times) = 1.$$

In particular, the extensions $L|K$ (and the corresponding Galois groups) together with the idele groups $\mathbb{A}_L^\times \supseteq \mathbb{A}_K^\times$ form a field formation. Formally we write

$$H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times) = \bigcup_L H^2(G_{L|K}, \mathbb{A}_L^\times).$$

As before we view inflation as inclusion so that

$$H^2(G_{L|K}, \mathbb{A}_L^\times) \subseteq H^2(G_{N|K}, \mathbb{A}_N^\times) \subseteq H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times)$$

for $N \supseteq L \supseteq K$ both normal.

Remark 8.6. More precisely Ω is the field of all algebraic numbers and we view $\mathbb{A}_\Omega^\times = \varinjlim_L \mathbb{A}_L^\times$. Then $\mathbb{A}_\Omega^\times$ is a (discrete) $G_{\Omega|K}$-module and $H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times)$ can be defined directly.

Lemma 8.7. *Let K be an algebraic number field and S be a finite set of places and $m \in \mathbb{N}$. Then there is a cyclic extension $L|K$ such that*

- *$m \mid [L_\mathfrak{P} \colon K_\mathfrak{p}]$ for all finite $\mathfrak{p} \in S$;*
- *$[L_\mathfrak{P} \colon K_\mathfrak{p}] = 2$ for all $v \in S$ that are real.*

Proof. We start by considering $K = \mathbb{Q}$. Let l^n be a prime power and ζ be a primitive l^nth root of unity.

If $l \neq 2$, then $\mathbb{Q}(\zeta)|\mathbb{Q}$ is a cyclic extension of degree $l^{n-1}(l-1)$. We denote the cyclic subfield of degree l^{n-1} over $\mathbb{Q}$ by $L(l^n)$.

If $l = 2$ the situation is slightly different. In this case the Galois group of $\mathbb{Q}(\zeta)|\mathbb{Q}$ is the direct product of $\mathbb{Z}/2\mathbb{Z}$ and a cyclic group of order 2^{n-2}. We let $L(2^n)$ be the field $\mathbb{Q}(\xi)$ where $\xi = \zeta - \frac{1}{\zeta}$. One computes that the Galois group of $L(2^n)|\mathbb{Q}$ is cyclic of order 2^{n-2} and $L(2^n)$ is totally imaginary (for sufficiently large n).

We observe that for a prime p the degree $[L(l^n)_\mathfrak{P} \colon \mathbb{Q}_p]$ becomes an arbitrarily large power of l as n grows. Indeed $[\mathbb{Q}_p(\zeta) \colon \mathbb{Q}_p]$ gets arbitrarily large while $[\mathbb{Q}_p(\zeta) \colon L(l^n)_\mathfrak{P}] \leq \max(l-1, 2)$.

We conclude the proof (of the case $K = \mathbb{Q}$) by writing $m = 2^{r_0} \cdot l_1^{n_1} \cdots l_s^{r_s}$ and setting

$$L = L(l_1^{n_1}) \cdots L(l_s^{n_s}) \cdot L(2^t).$$

For sufficiently large $n_1, \ldots, n_2, t$ this field has the desired properties. Note that it is totally imaginary since $L(2^t)$ is. It further is cyclic since the extensions $L(l^{n_i})$ (resp. $L(2^t)$) are all cyclic of co-prime orders. Finally the divisibility condition is achieved by making the exponents sufficiently large.

Turning to the general case. Let $N|\mathbb{Q}$ be a (totally imaginary) cyclotomic field such that for each prime p lying under S (i.e. there is $\mathfrak{P} \in S$ with $\mathfrak{p} \mid p$ in the extension $K|\mathbb{Q}$) the degree of $[N_{\mathfrak{P}} \colon \mathbb{Q}_p]$ is divisible by $m \cdot [K \colon \mathbb{Q}]$. Then $L = K \cdot N$ has the desired property. ∎

Theorem 8.8. *For any algebraic number field K we have*

$$\mathrm{Br}(K) = \bigcup_{\substack{L|K,\\ cyclic}} H^2(G_{L|K}, L^\times) \text{ and } H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times) = \bigcup_{\substack{L|K,\\ cyclic}} H^2(G_{L|K}, \mathbb{A}_L^\times).$$

Proof. Take $[c] \in H^2(G_{L'|K}, \mathbb{A}_{L'}^\times) \subseteq H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times)$ and let m be the order of $[c]$. Further let S be the set of places v of K where the local component c_v is non-trivial.

Applying Lemma 8.7 we find a cyclic extension $L|K$ such that $m \mid [L_{\mathfrak{P}} \colon K_{\mathfrak{p}}]$ for $\mathfrak{p} \in S$ finite. We also have $[L_v \colon K_v] = 2$ for all real places $v \in S$. We consider the composite $N = L' \cdot L$. Note that

$$H^2(G_{L'|K}, \mathbb{A}_{L'}^\times), H^2(G_{L|K}, \mathbb{A}_L^\times) \subseteq H^2(G_{N|K}, \mathbb{A}_N^\times).$$

We claim $c \in H^2(G_{L|K}, \mathbb{A}_L^\times)$. To see this we use the exact sequence

$$1 \to H^2(G_{L|K}, \mathbb{A}_L^\times) \to H^2(G_{N|K}, \mathbb{A}_N^\times) \overset{\mathrm{Res}}{\to} H^2(G_{N|L}, \mathbb{A}_N^\times).$$

We need to show that $\mathrm{Res}(c) = 1$. This can be checked locally:

$$\begin{aligned} \mathrm{Res}(c) = 1 &\Leftrightarrow (\mathrm{Res}(c))_{\mathfrak{P}} = \mathrm{Res}(c_{\mathfrak{p}}) = 1 \text{ for all } \mathfrak{P} \\ &\Leftrightarrow \mathrm{inv}_{N_{\mathfrak{P}'}|L_{\mathfrak{P}}}(\mathrm{Res}(c_{\mathfrak{p}})) = \mathrm{inv}_{N_{\mathfrak{P}'}|K_{\mathfrak{p}}} c_{\mathfrak{p}}^{[L_{\mathfrak{P}} \colon K_{\mathfrak{p}}]} = 0 \text{ for all } \mathfrak{p} \\ &\Leftrightarrow c_{\mathfrak{p}}^{[L_{\mathfrak{P}} \colon K_{\mathfrak{p}}]} = \text{ for all } \mathfrak{p} \in S. \end{aligned}$$

The final statement is true since the order m of c divides $[L_{\mathfrak{P}} \colon K_{\mathfrak{p}}]$ for all finite places by construction. (The real places are easily dealt with.)

The proof for $\mathrm{Br}(K)$ is Sheet 12, Exercise 1 below. ∎

Instead of the ideles $\mathbb{A}_\Omega^\times$ themselves one uses the idele class group $\mathbb{C}_K$ in global class field theory. Thus we need to study the cohomology of this group.

Theorem 8.9 (First Fundamental Inequality)**.** *Let $L|K$ be a cyclic extension of prime order. We have*

$$h(\mathbb{C}_L) = p.$$

In particular

$$[\mathbb{C}_K \colon N_{G_{L|K}}\mathbb{C}_L] \geq p.$$

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

- It contains S_∞ and all places that ramify in L;
- $\mathbb{A}_K^\times = \mathbb{A}_K^{\times,S} \cdot K^\times$; and
- $\mathbb{A}_L^\times = \mathbb{A}_L^{\times,\overline{S}} \cdot L^\times$ (as announced earlier we will abuse notation and write $\overline{S} = S$).

In particular we have

$$\mathbb{C}_L = \mathbb{A}_L^{\times,S} \cdot L^\times / L^\times = \mathbb{A}_L^{\times,S}/L^S,$$

since $L^S = L^\times \cap \mathbb{A}_L^{\times,S}$. Using the properties of the Herbrand quotient we get

$$h(\mathbb{C}_L) = h(\mathbb{A}_L^{\times,S}) \cdot h(L^S)^{-1}.$$

It remains to compute the Herbrand quotients on the right hand side. (In particular, if they are defined then also $h(\mathbb{C}_L)$ is.)

The problem of computing $h(\mathbb{A}_L^{\times,S})$ is a purely local endeavour. We write $n = \sharp S$, $N = \sharp\overline{S}$ and let n_1 be the number of places that are non-split. Note that since $L|K$ is of prime degree we must have

$$N = n_1 + p(n - n_1).$$

First we recall that

$$H^1(G_{L|K}, \mathbb{A}_L^{\times,S}) = \prod_{v \in S} H^1(G_w, L_w^\times) = 1.$$

Thus we are left with the zeroth cohomology group. By local reciprocity we have

$$H^0(G_w, L_w^\times) \cong G_w.$$

This implies that

$$\sharp H^0(G_w, L_w^\times) = \begin{cases} 1 & \text{if } w|v \text{ with } v \text{ split,} \\ p & \text{else.} \end{cases}$$

Since also $H^0(G_{L|K}, \mathbb{A}_L^{\times,S})$ factorizes we arrive at

$$h(\mathbb{A}_L^{\times,S}) = \sharp H^0(G_{L|K}, \mathbb{A}_L^{\times,S}) = p^{n_1}.$$

To compute $h(L^S)$ we use the generalised Dirichlet unit theorem which implies that the S-units L^S have rank $N - 1$ and K^S has rank n. By Theorem 4.49 we have

$$h(L^S) = p^{(p\cdot(N-1)-(n-1))/(p-1)}.$$

It is easy to compute that $(p \cdot (N-1) - (n-1))/(p-1) = n_1 - 1$. This concludes the proof. ∎

Corollary 8.10. *Let $L|K$ be a cyclic extension of degree p^n (where p is prime and $n \in \mathbb{N}$). Then K has infinitely many non-split primes.*

Proof. We start with the case when $[L\colon K] = p$ (i.e. $n = 1$). Suppose that the set $\mathfrak{U}$ of non-split primes is finite. Take $\overline{a} \in \mathbb{C}_K$ represented by $a \in \mathbb{A}_K^\times$. For each $v \in \mathfrak{U}$ the set $a_v \cdot (K_v^\times)^p$ is an open neighbourhood of a_v in $K_v^\times$. By the approximation theorem we find $x \in K^\times$ such that $x \in a_v \cdot (K_v^\times)^p$ for all $v \in \mathfrak{U}$. We claim that $a' = a \cdot x^{-1}$ is in the image of the norm map from $\mathbb{A}_L^\times$. It suffices to check this at all places. For $v \in \mathfrak{U}$ this is obvious by construction since $[L_w\colon L_v] = p$ and $a'_v = a_v \cdot x^{-1} \in (K_v^\times)^p$. On the other hand, for $v \notin \mathfrak{U}$ we have $L_w = K_v$, since the extension is of prime degree. Thus we find that there is $b \in \mathbb{A}_L^\times$ with $N_{G_{L|K}} b = a' \in a \cdot K^\times$. This implies that $\mathbb{C}_K = N_{G_{L|K}} \mathbb{C}_L$. But this is a contradiction to the first fundamental inequality:

$$1 = [\mathbb{C}_K\colon N_{G_{L|K}} \mathbb{C}_L] \geq p.$$

We conclude that $\mathfrak{U}$ must be an infinite set.

Now we treat the general case. First note that there is exactly one prime cyclic extension $L_0|K$ contained in L. Suppose that almost all primes of K split in L. In particular, for almost all primes $\mathfrak{P}$ of L, the decomposition field $Z_\mathfrak{P}$ is a proper extension of K. In particular L_0 is contained in almost all decomposition fields $Z_\mathfrak{P}$. As a consequence almost all primes split in the extension L_0, which is a contradiction to the first part of the proof. ∎

Our next goal is to prove the second fundamental inequality

$$[\mathbb{C}_K\colon N_{G_{L|K}} \mathbb{C}_L] \leq p,$$

where $L|K$ is a prime cyclic extension. We do this in several steps.

Lemma 8.11. *Suppose that K contains the pth roots of unity. Let $N = K(\sqrt[p]{x})$ (with $x \in K^\times$) be an arbitrary kummerian field over K. Further let $\mathfrak{p} \nmid p$ be a finite prime. Then $\mathfrak{p}$ is unramified in N if and only if $x \in \mathcal{O}_\mathfrak{p}^\times \cdot (K_\mathfrak{p}^\times)^p$. Furthermore, $\mathfrak{p}$ splits completely if and only if $x \in (K_\mathfrak{p}^\times)^p$.*

Proof. Take $\mathfrak{P} \mid \mathfrak{p}$ (in the extension $N|K$). Then we have $N_\mathfrak{P} = K_\mathfrak{p}(\sqrt[p]{x})$. If we can write $x = u \cdot y^p$ with $u \in \mathcal{O}_\mathfrak{p}^\times$ and $y \in K_\mathfrak{p}^\times$, then $N_\mathfrak{P} = K_\mathfrak{p}(\sqrt[p]{u})$. We need to check two cases. First, if $X^p - u = 0$ is irreducible in the residue field of $K_\mathfrak{p}$, then it is also irreducible over $K_\mathfrak{p}$ and the extension $N_\mathfrak{P}|K_\mathfrak{p}$ is unramified. Second, if $X^p - u$ is reducible over the residue field, then it splits completely because the residue characteristic is different from p. Using Hensel's lemma we find that $X^p - u$ also splits over $K_\mathfrak{p}$ and we conclude that $N_\mathfrak{P} = K_\mathfrak{p}$.

Suppose $\mathfrak{p}$ is unramified. We write $\sqrt[p]{x} = u \cdot \varpi^k$ for $u \in \mathcal{O}_\mathfrak{P}^\times$ and a choice of uniformiser $\varpi \in K_\mathfrak{p}$. We trivially have $x = u^p \cdot \varpi^{kp} \in \mathcal{O}_\mathfrak{p}^\times \cdot (K_\mathfrak{p}^\times)^p$.

Finally $\mathfrak{p}$ splits completely if and only if $N_\mathfrak{P} = K_\mathfrak{p}$ if and only if $x \in (K_\mathfrak{p}^\times)^p$. ∎

Theorem 8.12. *Let K be an algebraic number field containing the pth roots of unity. Let S be a set finite set of places containing S_∞ and all the primes lying above p. Further assume that $\mathbb{A}_K^\times = \mathbb{A}_K^{\times,S} \cdot K^\times$. Take $x_0 \in K^S$ and suppose that $L = K(\sqrt[p]{x_0})$ is a cyclic extension of K with degree p.*

Then there are $m = \sharp S - 1$ finite places $\mathfrak{q}_1, \dots, \mathfrak{q}_m \notin S$ which split completely in L such that the following condition holds: If $N = K(\sqrt[p]{x})$ is a kummerian field over K so that $\mathfrak{p} \in S$ split completely and $\mathfrak{p} \neq \mathfrak{q}_1, \dots, \mathfrak{q}_m$ are unramified, then $N = K$.

Proof. We consider

$$T = K(\sqrt[p]{K^S}).$$

By Kummer Theory we have

$$\chi(G_{T|K}) \cong K^S \cdot (K^\times)^p/(K^\times)^p \cong K^S/(K^S)^p.$$

Computing the order of the latter group is easy using the generalized Dirichlet Unit Theorem and we find that

$$[T\colon K] = p^{\sharp S}.$$

One can even show that $G_{T|K} \cong \mathcal{Z}_1 \times \ldots \times \mathcal{Z}_{\sharp S}$ where $\mathcal{Z}_i$ for $i = 1, \dots, \sharp S$ is a cyclic group of order p.

Let $L = K(\sqrt[p]{x_0})$ with $x_0 \in K^S$. Then $L \subseteq T$ and without loss of generality we can assume that

$$G_{T|L} = \mathcal{Z}_1 \times \ldots \times \mathcal{Z}_{\sharp S - 1}.$$

For each $i = 1, \dots, \sharp S$ we let T_i be the field such that $G_{T|T_i} = \mathcal{Z}_i$. Note that $L \subseteq T_i$ for $i = 1, \dots, \sharp S - 1$.

For each $i = 1, \dots, \sharp S$ we choose a finite place $\mathfrak{Q}_i$ of T_i such that

- $\mathfrak{Q}_i$ is non-split in T;
- The primes $\mathfrak{q}_i$ of K lying under $\mathfrak{Q}_i$ are pairwise distinct; and
- $\mathfrak{q}_1, \dots, \mathfrak{q}_{\sharp S} \notin S$,

We claim that $\mathfrak{q}_1, \dots, \mathfrak{q}_{\sharp S - 1}$ fulfill the required property.

We first check that $\mathfrak{q}_1, \dots, \mathfrak{q}_{\sharp S - 1}$ split completely in L. Let $\mathfrak{Q}_i'$ be the (unique) prime of T lying above $\mathfrak{Q}_i$. The decomposition field Z_i of $\mathfrak{Q}_i'$ is obviously contained in T_i. Furthermore $\mathfrak{q}_i$ is unramified in every extension $K(\sqrt[p]{x})$ with $x \in K^S$. Thus they are unramified in T and the Galois groups $G_{T|Z_i}$ must be cyclic. It is easy to see that the order must be p, so that $[T\colon Z_i] = p$ and $Z_i = T_i$. We are done since for $i = 1, \dots, \sharp S - 1$ the field L is contained in T_i.

Next we write $U_i = \mathcal{O}_{\mathfrak{q}_i}^\times$ for $i = 1, \dots, \sharp S$. We define the homomorphism

$$K^S/(K^S)^p \to \prod_{i=1}^{\sharp S} U_i/(U_i)^p,\ x \cdot (K^S)^p \mapsto \prod_{i=1}^{\sharp S} x \cdot (U_i)^p.$$

We claim that this is bijective. The map is injective since $x \in (U_i)^p \subseteq (K_{\mathfrak{q}_i}^\times)^p$ implies that $\mathfrak{q}_1, \dots, \mathfrak{q}_{\sharp S}$ split completely in $K(\sqrt[p]{x})$. Thus $K(\sqrt[p]{x}) \subseteq Z_i = T_i$. We

conclude that $K(\sqrt[p]{x}) \subseteq \bigcap_{i=1}^{\sharp S} T_i = K$. Thus $x \in (K^\times)^p \cap K^S = (K^S)^p$. The map is then surjective since both sides have the same order. (To see this one recalls that $[U_i \colon (U_i)^p] = p \cdot |p|_{\mathfrak{q}_i}^{-1}$.)

Let $N = K(\sqrt[p]{x})$ be now a kummerian field in which all $\mathfrak{p} \in S$ split completely and all $\mathfrak{p} \nmid \prod_{i=1}^{\sharp S-1} \mathfrak{q}_i$ are unramified. We need to show that $N = K$. According to the first fundamental inequality it suffices to show that $\mathbb{C}_K = N_{G_{N|K}} \mathbb{C}_N$. To see this we take $\overline{a} \in \mathbb{C}_K$ represented by some idele $a \in \mathbb{A}_K^{S,\times}$. We set $\overline{a_i} = a_{\mathfrak{q}_i} \cdot (U_i)^p$. Note that $a_{\mathfrak{q}_i} \in U_i$. By the previous step of the proof we find $y \in K^S$ such that $y \cdot (U_i)^p = \overline{a_i}$. In particular we have that $a_{\mathfrak{q}_i} = y \cdot u_i^p$ for some $u_i \in U_i$. Obviously $a' = a \cdot y^{-1}$ also represents the class $\overline{a}$. It remains to see that $a' \in N_{G_{N|K}} \mathbb{A}_N^\times$. The latter fact can be checked locally:

- If $v \in S$, then a'_v is a norm, since v splits completely in N (i.e. $N_w = K_v$).
- For $v = \mathfrak{q}_i$ with $i = 1 \ldots, \sharp S - 1$ we have $a'_v = u_i^p$ and a pth power must also be a norm.
- If $v \nmid S$ and $v \neq \mathfrak{q}_i$ for $i = 1, \ldots, \sharp S - 1$ we observe that $a'_v \in \mathcal{O}_v^\times$. Furthermore, since v is unramified in $N|K$ the local norms are surjective on the local units.

This completes the proof. ∎

Theorem 8.13. *Let $L|K$ be a cyclic extension of prime degree p. Further assume that K contains the pth roots of unity. Then*

$$\sharp H^0(G_{L|K}, \mathbb{C}_L) = [\mathbb{C}_K \colon N_{G_{L|K}} \mathbb{C}_L] \leq p.$$

Proof. The strategy is to construct $\overline{F} \subseteq N_{G_{L|K}} \mathbb{C}_L$ and then to show that $[\mathbb{C}_K \colon \overline{F}] = p$. This gives the desired inequality.

Suppose $L = K(\sqrt[p]{x_0})$ with $x_0 \in K^\times$. Let S be a finite set of places such that

- S contains all primes lying over p as well as S_∞;
- $\mathbb{A}_K = \mathbb{A}_K^{\times,S} \cdot K^\times$; and
- $x_0 \in K^S = \mathbb{A}_K^S \cap K^\times$.

Further, let $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ be auxiliary places, which split completely in L. We set

$$S^* = S \cup \{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}.$$

We define the idele group

$$F = \prod_{v \in S} (K_v^\times)^p \times \prod_{i=1}^{m} K_{\mathfrak{q}_i}^\times \times \prod_{v \notin S^*} \mathcal{O}_v^\times.$$

We first check that $F \subseteq N_{G_{L|K}} \mathbb{A}_L^\times$. This can be done locally and we consider three cases:

- For $v \in S$ we have $\mathfrak{a}_v \in (K_v^\times)^p \subseteq N_{L_w|K_v} L_w^\times$ (for $w \mid v$).
- For $i = 1, \ldots, m$ we have $L_{\mathfrak{P}} = K_{\mathfrak{q}_i}$ by construction.

- For $v \notin S^*$ we have by construction of S that $x_0 \in \mathcal{O}_v^\times$. Thus $L = K(\sqrt[p]{x_0})$ is unramified at v and since $a_v \in \mathcal{O}_v^\times$ it must be in the image of the norm map.

We now put $\overline{F} = F \cdot K^\times / K^\times$ and observe that $\overline{F} \subseteq N_{G_{L|K}} \mathbb{C}_L$. To compute the index we will use the elementary fact that

$$[\mathbb{C}_K : \overline{F}] = [\mathbb{A}_K^{\times,S^*} \cdot K^\times : F \cdot K^\times] = \frac{[\mathbb{A}_K^{\times,S^*} : F]}{[(\mathbb{A}_K^{\times,S^*} \cap K^\times) : (F \cap K^\times)]}.$$

The index in the numerator is computed locally since

$$\mathbb{A}_K^{\times,S^*} / F \cong \prod_{v \in S} K_v^\times / (K_v^\times)^p$$

via the map induced by $a \mapsto \prod_{v \in S} a_v \cdot (K_v^\times)^p$, which is easily seen to be an isomorphism. By Theorem 3.20 we have

$$[K_v^\times : (K_v^\times)^p] = p^2 |p|_v^{-1}$$

for the finite places in S. For complex places v the index is obviously 1, but we also have $p^2|p|_v^{-1} = 1$. Finally we note that only for $p = 2$ there can be real places. In this case we have $[\mathbb{R}^\times : \mathbb{R}_+] = 2 = 4 \cdot |2|_v^{-1}$. We find

$$[\mathbb{A}_K^{\times,S^*} : F] = p^{2 \cdot \sharp S} \prod_{v \in S} |p|_v^{-1} = p^{2 \cdot \sharp S} \prod_v |p|_v^{-1} = p^{2 \cdot \sharp S}.$$

To compute the index in the denominator we further write

$$[(\mathbb{A}_K^{\times,S^*} \cap K^\times) : (F \cap K^\times)] = \frac{[K^{S^*} : (K^{S^*})^p]}{[(F \cap K^\times) : (K^{S^*})^p]}.$$

It is easily seen (i.e. See Sheet 11, Exercise 4 above) using the generalized Dirichlet Unit Theorem that

$$[K^{S^*} : (K^{S^*})^p] = p^{\sharp S + m}.$$

So far we have computed that

$$[\mathbb{C}_K : N_{G_{L|K}} \mathbb{C}_L] \leq [\mathbb{C}_K : \overline{F}] = p^{\sharp S - m} \cdot [(F \cap K^\times) : (K^{S^*})^p].$$

We choose $m = \sharp S - 1$ and take $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ as in Theorem 8.12. We claim that

$$K^\times \cap F = (K^{S^*})^p,$$

which directly implies that $\overline{F}$ has the correct index. To prove our claim we have to show that

$$K^\times \cap \bigcap_{v \in S} (K_v^\times)^p \cap \bigcap_{v \notin S^*} \mathcal{O}_v^\times = (K^{S^*})^p.$$

The inclusion $\supseteq$ is clear. Take $x \in K^\times \cap \bigcap_{v \in S} (K_v^\times)^p \cap \bigcap_{v \notin S^*} \mathcal{O}_v^\times$ and consider $N = K(\sqrt[p]{x})$. The splitting behavior of primes in $N|K$ is easily investigated using Lemma 8.11. It turns out that by construction of $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ (see Theorem 8.12)

we have $N = K$. We conclude that $x \in (K^\times)^p$. Since $x \in \mathcal{O}_v^\times$ for $v \notin S^*$ we must further have $x \in (K^{S^*})^p$ as claimed. ∎

Corollary 8.14. *Let $L|K$ be a cyclic extension of prime degree p and with Galois group $G_{L|K}$. Suppose K contains the pth roots of unity. Then*

$$H^0(G_{L|K}, \mathbb{C}_L) \cong H^2(G_{L|K}, \mathbb{C}_L) \cong G_{L|K}$$

and $H^1(G_{L|K}, \mathbb{C}_L) = 1$.

Theorem 8.15. *For every normal extension $L|K$ with Galois group $G_{L|K}$ we have*

$$H^1(G_{L|K}, \mathbb{C}_L) = 1.$$

Proof. We prove this by induction on the order n of $G_{L|K}$. The case $n = 1$ is trivial. Thus we suppose that $H^1(G_{L|K}, \mathbb{C}_L) = 1$ for every normal extension with $[L\colon K] < n$. If the order of $G_{L|K}$ is n but n is not a prime power, then the induction hypothesis applies to the p-Sylow groups of $G_{L|K}$. By Corollary 4.34 this implies our claim.

Thus we suppose that $G_{L|K}$ is a p-group and we let $H \subset G$ be a normal subgroup with index p. The fixed field of H is a field $M \subseteq L$ and $H = \mathrm{Gal}(L|M)$. If $p < n$, then we have

$$H^1(G_{L|K}/H, \mathbb{C}_M) = H^1(H, \mathbb{C}_L) = 1.$$

By exactness of the sequence

$$1 \to H^1(G_{L|K}/H, \mathbb{C}_M) \overset{\mathrm{Inf}}{\to} H^1(G_{L|K}, \mathbb{C}_L) \overset{\mathrm{Res}}{\to} H^1(H, \mathbb{C}_L)$$

we get $H^1(G_{L|K}, \mathbb{C}_L) = 1$.

It remains to treat the case $n = p$. In this case let ζ be a primitive pth root of unity and set $K' = K(\zeta)$. We also define $L' = K' \cdot L$. We have

$$[K'\colon K] \leq p - 1 < p = n \text{ and } [L'\colon K'] = p.$$

We have

$$H^1(G_{K'|K}, \mathbb{C}_{K'}) = H^1(G_{L'|K'}, \mathbb{C}_{L'}) = 1.$$

Using exactness of

$$1 \to H^1(G_{K'|K}, \mathbb{C}_{K'}) \overset{\mathrm{Inf}}{\to} H^1(G_{L'|K}, \mathbb{C}_{L'}) \overset{\mathrm{Res}}{\to} H^1(G_{L'|K'}, \mathbb{C}_{L'})$$

we find that $H^1(G_{L'|K}, \mathbb{C}_{L'}) = 1$. However inflation is also an injective map from $H^1(G_{L|K}, \mathbb{C}_L)$ to $H^1(G_{L'|K}, \mathbb{C}_{L'})$. Therefore $H^1(G_{L|K}, \mathbb{C}_L)$ must be trivial as desired. ∎

Corollary 8.16 (Hasse Norm Theorem)**.** *Let $L|K$ be a cyclic extension. Then $x \in K^\times$ is a norm if and only if it is a local norm everywhere.*

Proof. We use the exact sequence

$$1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{C}_L \to 1$$

to obtain the exact sequence

$$H^{-1}(G_{L|K}, \mathbb{C}_L) \to H^0(G_{L|K}, L^\times) \to H^0(G_{L|K}, \mathbb{A}_L^\times)$$

of cohomology. Recall that since $G_{L|K}$ is cyclic we have

$$H^{-1}(G_{L|K}, \mathbb{C}_L) \cong H^1(G_{L|K}, \mathbb{C}_L) = 1.$$

Thus the map

$$K^\times / N_{L|K} L^\times = H^0(G_{L|K}, L^\times) \to H^0(G_{L|K}, \mathbb{A}_L^\times) \cong \bigoplus_v K_v^\times / N_{L_w|K_v} L_w^\times$$

is injective. The result follows directly. ∎

Theorem 8.17. *Let $L|K$ be a normal extension with Galois group $G_{L|K}$. Then*

$$\sharp H^2(G_{L|K}, \mathbb{C}_L) \mid [L\colon K].$$

Proof. We argue again by induction on $n = [L\colon K]$. If $n = 1$ there is nothing to do, so that we can assume that the claim holds for all extensions of degree $< n$.

Suppose that n is not a prime power. Thus each p-Sylow subgroup G_p of $G_{L|K}$ has smaller order. By induction hypothesis we obtain

$$\sharp H^2(G_p, \mathbb{C}_L) \mid n_p,$$

where $n_p = \sharp G_p$ is the p-part of n. Recall that

$$H_p^2(G_{L|K}, \mathbb{C}_L) \overset{\text{Res}}{\to} H^2(G_p, \mathbb{C}_L)$$

is injective. This implies that $\sharp H_p^2(G_{L|K})$ divides n_p. Now we are done since $H^2(G_{L|K}, \mathbb{C}_L) = \prod_p H_p^2(G_{L|K}, \mathbb{C}_L)$.

It remains to treat the case when $G_{L|K}$ is a p-group. As usual let H be a normal subgroup of index p. By induction hypothesis we have

$$\sharp H^2(H, \mathbb{C}_L) \mid \frac{n}{p}.$$

Since $H^1(H, \mathbb{C}_L) = 1$ we have the exact sequence

$$1 \to H^2(G/H, \mathbb{C}_L^H) \overset{\text{Inf}}{\to} H^2(G_{L|K}, \mathbb{C}_L) \overset{\text{Res}}{\to} H^2(H, \mathbb{C}_L).$$

Previously we have seen that $\sharp H^2(G/H, \mathbb{C}_L^H) = p$. This is because $\mathbb{C}_L^H = \mathbb{C}_{L'}$ for a prime cyclic extension $L'|K$ with Galois group G/H. We conclude that $p^{-1} \cdot \sharp H^2(G, \mathbb{C}_L)$ divides n/p. This concludes the proof. ∎

The next step is to define the invariance map. Let $L|K$ be a normal extension of algebraic number fields with Galois group $G_{L|K}$. Recall that

$$H^2(G_{L|K}, \mathbb{A}_L^\times) = \bigoplus_v H^2(G_{L_w|K_v}, L_w^\times).$$

At each place local class field theory provides us with isomorphisms

$$\mathrm{inv}_{L_w|K_v}\colon H^2(G_{L_w|K_v}, L_w^\times) \to \frac{1}{[L_w\colon K_v]}\mathbb{Z}/\mathbb{Z} \subseteq \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z}.$$

Remark 8.18. This depends only very mildly on the choice of $w \mid v$. Indeed if w' is another place above v, then there is a K_v-isomorphism $L_w \to L_{w'}$, which induces an isomorphism between $H^2(G_{L_w|K_v}, L_w^\times)$ and $H^2(G_{L_{w'}|K_v}, L_{w'}^\times)$. This isomorphism respects the invariance map.

Definition 8.1 (Idele invariance)**.** Let $c \in H^2(G_{L|K}, \mathbb{A}_L^\times)$ with local components $c_v \in H^2(G_{L_w|K_v}, L_w^\times)$ (for a choice of $w \mid v$). Then we define

$$\mathrm{inv}_{L|K}(c) = \sum_v \mathrm{inv}_{L_w|K_v}(c_v) \in \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z}.$$

(Note that the sum has only finitely many non-trivial terms.)

Theorem 8.19. *Let $N \supset L \supset K$ be normal extensions of K. Then we have*

$$\begin{aligned}
&\mathrm{inv}_{N|K}(c) = \mathrm{inv}_{L|K}(c) \text{ for } c \in H^2(G_{L|K}, \mathbb{A}_L^\times) \subseteq H^2(G_{N|K}, \mathbb{A}_N^\times),\\
&\mathrm{inv}_{N|L}(\mathrm{Res}_L(c)) = [L\colon K]\cdot \mathrm{inv}_{N|K}(c) \text{ for } c \in H^2(G_{N|K}, \mathbb{A}_N^\times), \text{ and}\\
&\mathrm{inv}_{N|K}(\mathrm{CoRes}_K(c)) = \mathrm{inv}_{N|L}(c) \text{ for } c \in H^2(G_{N|L}, \mathbb{A}_N^\times).
\end{aligned}$$

Proof. This follows directly from the respective local properties. We only show the proof of the second identity. The other computations are very similar.

Take $c \in H^2(G_{N|K}, \mathbb{A}_N^\times)$ and compute

$$\begin{aligned}
\mathrm{inv}_{N|L}(\mathrm{Res}_L(c)) &= \sum_w \mathrm{inv}_{N_{w'}|L_w}(\mathrm{Res}_L(c)_w) = \sum_w \mathrm{inv}_{N_{w'}|L_w}(\mathrm{Res}_{L_w}(c_v))\\
&= \sum_w [L_w\colon K_v]\cdot \mathrm{inv}_{N_{w'}|K_v}(c_v) = \sum_v \sum_{w|v} [L_w\colon K_v]\cdot \mathrm{inv}_{N_{w'}|K_v}(c_v).
\end{aligned}$$

Recall that

$$\sum_{w|v} [L_w\colon K_v] = [L\colon K].$$

Further, observing that $\mathrm{inv}_{N_{w'}|K_v}(c_v)$ depends only on v, we find that

$$\mathrm{inv}_{N|L}(\mathrm{Res}_L(c)) = [L\colon K]\cdot \sum_v \mathrm{inv}_{N_{w'}|K_v}(c_v) = [L\colon K]\cdot \mathrm{inv}_{N|K}(c).$$

□

Remark 8.20. The idele invariance does **not** turn $(G_{\Omega|K}, \mathbb{A}_\Omega^\times)$ into a class formation. Indeed $\mathrm{inv}_{L|K}$ is not an isomorphism. However, it satisfies all the other properties.

Definition 8.2. Let $L|K$ be an abelian extension. Let $a \in \mathbb{A}_K^\times$ be an idele with local components $a_v \in K_v^\times$. We define

$$(a, L|K) = \prod_v (a_v, L_w|K_v) \in G_{L|K}.$$

This is well defined, because $a_v \in \mathcal{O}_v^\times$ for almost all v. Indeed if v is also unramified, then a_v is a local norm so that $(a_v, L_w|K_v) = 1$. Therefore the product has only finitely many non-trivial terms.

Recall the dual characterization of the local norm residue symbols given in Lemma 6.16. Together with the definitions we get the following lemma (essentially) for free:

Lemma 8.21. *Let $L|K$ be an abelian extension of algebraic number fields. Given $a \in \mathbb{A}_K^\times$ we write $[a] = a \cdot N_{L|K}\mathbb{A}_L^\times \in H^0(G_{L|K}, \mathbb{A}_L^\times)$. Then, for every $\chi \in \chi(G_{L|K}) = H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$ we have*

$$\chi((a, L|K)) = \mathrm{inv}_{L|K}([a] \cup \delta\chi) \in \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z}.$$

The exact sequence

$$1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{C}_L \to 1$$

and the fact that $H^1(G_{L|K}, \mathbb{C}_L) = 1$ gives us an injective homomorphism

$$H^2(G_{L|K}, L^\times) \to H^2(G_{L|K}, \mathbb{A}_L^\times).$$

The image consists precisely of those classes $[c] \in H^2(G_{L|K}, \mathbb{A}_L^\times)$ that can be represented by a cocycle c with image in the principal idele group $L^\times$. This allows us to view $H^2(G_{L|K}, L^\times)$ as a subset of $H^2(G_{L|K}, \mathbb{A}_L^\times)$.

Theorem 8.22. *If $c \in H^2(G_{L|K}, L^\times)$, then $\mathrm{inv}_{L|K}(c) = 0$.*

Proof. We first treat the critical case $K = \mathbb{Q}$ and $L = \mathbb{Q}(\zeta)$, where ζ is a primitive l^nth root of unity (with $n \geq 2$ if $l = 2$). We need to show that

$$(a, \mathbb{Q}(\zeta)|\mathbb{Q}) = \prod_v (a, \mathbb{Q}_v(\zeta)|\mathbb{Q}_v) = 1 \text{ for } a \in \mathbb{Q}^\times. \tag{10}$$

We compute the local symbols case by case:

- **Assume $p \nmid l \cdot \infty$:** We have $(a, \mathbb{Q}_v(\zeta)|\mathbb{Q}_p)\zeta = \varphi^{v(a)}(\zeta)$. Note that the Frobenius automorphism φ acts on ζ by $\varphi(\zeta) = \zeta^p$. Thus we have
$$(a, \mathbb{Q}_p(\zeta)|\mathbb{Q}_p)\zeta = \zeta^{p^{v(a)}}.$$
- **Assume $p = l$:** Then we had stated in (9) that
$$(a, \mathbb{Q}_l(\zeta)|\mathbb{Q}_l)\zeta = \zeta^r,$$
where r is given by $r \equiv a^{-1}p^{v_l(a)} \bmod p^n$.

- **Assume $v = \infty$:** In this case we have

$$(a, \mathbb{Q}_v(\zeta)|\mathbb{Q}_v)\zeta = (a, \mathbb{C}|\mathbb{R})\zeta = \zeta^{\mathrm{sgn}(a)}.$$

All together we find that

$$(a, \mathbb{Q}(\zeta)|\mathbb{Q})\zeta = \zeta^{\mathrm{sgn}(a)\cdot r\cdot\prod_{p\neq l} p^{v_p(a)}}.$$

Looking at the exponent modulo l^n we find that

$$\mathrm{sgn}(a)\cdot r\cdot\prod_{p\neq l} p^{v_p(a)} \equiv \prod_v |a|_v^{-1} = 1.$$

This establishes (10).[16]

The next step is to consider general cyclotomic extensions $L|\mathbb{Q}$. Let $\chi \in \chi(G_{L|\mathbb{Q}}) = H^1(G_{L|\mathbb{Q}}, \mathbb{Q}/\mathbb{Z})$ be a generating element (of the cyclic character group). Then $\delta\chi$ generates $H^2(G_{L|\mathbb{Q}}, \mathbb{Z})$. We obtain a bijective homomorphism

$$\delta\chi\cup\colon H^0(G_{L|\mathbb{Q}}, L^\times) \to H^2(G_{L|\mathbb{Q}}, L^\times).$$

Thus we can write $c \in H^2(G_{L|\mathbb{Q}}, L^\times)$ as $[a]\cup\delta\chi$ for $[a] = a\cdot N_{L|\mathbb{Q}}L^\times$ with $a \in \mathbb{Q}^\times$. We have

$$\mathrm{inv}_{L|\mathbb{Q}}(c) = \mathrm{inv}_{L|\mathbb{Q}}([a]\cup\delta\chi) = \chi((a, L|\mathbb{Q})).$$

Thus we need to show that $(a, L|\mathbb{Q}) = \prod_v (a, L_w|\mathbb{Q}_v) = 1$. Since L is a cyclotomic extension we see that $L \subseteq \mathbb{Q}(\zeta)$ for some primitive root of unity ζ. It obviously suffices to show that $(a, \mathbb{Q}(\zeta)|\mathbb{Q}) = 1$. Finally note that $\mathbb{Q}(\zeta)$ is generated by roots of unity with prime power order. Since it suffices to check triviality on the generators we can assume that ζ is an l^nth root of unity for some prime l. but this case has been treated above.

Finally we consider the general situation $L|K$. Let $N|\mathbb{Q}$ be a normal extension containing L. We observe that

$$c \in H^2(G_{L|K}, L^\times) \subseteq H^2(G_{N|K}, N^\times) \subseteq H^2(G_{N|K}, \mathbb{A}_N^\times).$$

Further we have

$$\mathrm{inv}_{L|K}(c) = \mathrm{inv}_{N|K}(c) = \mathrm{inv}_{N|\mathbb{Q}}(\mathrm{CoRes}_{\mathbb{Q}}(c)).$$

Because $\mathrm{CoRes}_{\mathbb{Q}}(c) \in H^2(G_{N|\mathbb{Q}}, N^\times)$ it suffices to consider the case $K = \mathbb{Q}$. According to Theorem 8.8 it even suffices to consider cyclotomic L. Since this case is already treated above the proof is complete. □

[16]Here we use the computation of the local norm residue symbol in the extension $\mathbb{Q}_l(\zeta)|\mathbb{Q}_l$, which we did not prove. Note that there is a purely local proof due to Dwork. The result can also be derived using the global reciprocity theorem. But then, in order not to obtain a cyclic argument, one first needs to give an alternative proof of the global reciprocity theorem for cyclotomic extensions of $\mathbb{Q}$. This was the approach taken by Artin and Tate in their Princeton lecture notes.

Theorem 8.23. *Let $L|K$ be a cyclic extension. Then*

$$1 \to H^2(G_{L|K}, L^\times) \to H^2(G_{L|K}, \mathbb{A}_L^\times) \overset{\mathrm{inv}_{L|K}}{\to} \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z} \to 0$$

is exact.

Proof. We first show that $\mathrm{inv}_{L|K}$ is surjective. If $[L\colon K] = p^r$ is a prime power we argue as follows. Obviously it suffices to find a pre-image of $\frac{1}{[L\colon K]} + \mathbb{Z}$. To construct this pre-image we recall the decomposition

$$H^2(G_{L|K}, \mathbb{A}_L^\times) \cong \bigoplus_v H^2(G_{L_w|K_v}, L_w^\times).$$

Because $L|K$ is cyclic and of prime-power degree there are infinitely many non-split primes of K (see Corollary 8.10). We fix such a prime $\mathfrak{p}_0$ with $[L_{\mathfrak{P}_0}\colon K_{\mathfrak{p}_0}] = [L\colon K]$. Thus locally we find an element $c_{\mathfrak{p}_0} \in H^2(G_{L_{\mathfrak{P}_0}|K_{\mathfrak{p}_0}}, L_{\mathfrak{P}_0}^\times)$ with

$$\mathrm{inv}_{L_{\mathfrak{P}_0}|K_{\mathfrak{p}_0}}(c_{\mathfrak{p}_0}) = \frac{1}{[L_{\mathfrak{P}_0}\colon K_{\mathfrak{p}_0}]} + \mathbb{Z} = \frac{1}{[L\colon K]} + \mathbb{Z}.$$

It is now clear that the global cohomology class determined by the local components $(\ldots, 1, c_{\mathfrak{p}_0}, 1, \ldots)$ does the job.

For general degrees $[L\colon K] = n$ we write $n = p_1^{r_1} \cdots p_s^{r_s}$. We decompose

$$\frac{1}{n} = \frac{n_1}{p_1^{r_1}} + \ldots + \frac{n_s}{p_s^{r_s}}.$$

For each i there is a cyclic intermediate field L_i with $[L_i\colon K] = p_i^{r_i}$. For each i we find $c_i \in H^2(G_{L_i|K}, \mathbb{A}_{L_i}^\times)$ such that

$$\mathrm{inv}_{L_i|K}(c_i) = \mathrm{inv}_{L|K}(c_i) = \frac{n_i}{p_i^{r_i}} + \mathbb{Z}.$$

The element $c = c_1 \cdots c_s$ then satisfies

$$\mathrm{inv}_{L|K}(c) = \frac{1}{n} + \mathbb{Z}.$$

Thus the map $\mathrm{inv}_{L|K}$ is surjective.

It remains to show exactness at $H^2(G_{L|K}, \mathbb{A}_L^\times)$. We have already seen that $H^2(G_{L|K}, L^\times)$ is contained in the kernel of $\mathrm{inv}_{L|K}$. The other inclusion will follow as soon as we can show that

$$H^2(G_{L|K}, \mathbb{A}_L^\times)/H^2(G_{L|K}, L^\times)$$

has order $\leq [L\colon K]$. To see this we use the exact sequence

$$1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{C}_L \to 1$$

and recall that $H^1(G_{L|K}, \mathbb{C}_L) = 1$. This gives the exact sequence of cohomology:

$$1 \to H^2(G_{L|K}, L^\times) \to H^2(G_{L|K}, \mathbb{A}_L^\times) \to H^2(G_{L|K}, \mathbb{C}_L).$$

We are done since the order of $H^2(G_{L|K}, \mathbb{C}_L)$ divides $[L\colon K]$ by Theorem 8.17. ∎

Recall the convention

$$H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times) = \bigcup_L H^2(G_{L|K}, \mathbb{A}_L^\times).$$

By extending the idele invariant map we obtain a homomorphism

$$\mathrm{inv}_K \colon H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times) \to \mathbb{Q}/\mathbb{Z}.$$

Theorem 8.24. *The homomorphism*

$$\mathrm{inv}_K \colon H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times) \to \mathbb{Q}/\mathbb{Z}$$

is surjective.

Proof. Note that for cyclic extensions $L|K$ the map $\mathrm{inv}_{L|K} \colon H^2(G_{L|K}, \mathbb{A}_L^\times) \to \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z}$ is surjective. But for each $m \in \mathbb{N}$ there is a cyclic extension $L|K$ such that $m \mid [L\colon K]$. ∎

Theorem 8.25. *For every (finite) algebraic number field we have the exact sequence*

$$1 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \overset{\mathrm{inv}_K}{\to} \mathbb{Q}/\mathbb{Z} \to 0.$$

Proof. This follows directly because we have the corresponding exact sequence for (finite) cyclic extensions. But these are sufficient by Theorem 8.8. ∎

Going back to the exact sequence

$$1 \to L^\times \to \mathbb{A}_L^\times \to \mathbb{C}_L \to 1$$

and recalling that $H^1(G_{L|K}, \mathbb{C}_L) = 1 = H^3(G_{L|K}, \mathbb{A}_L^\times)$ we obtain the exact sequence

$$1 \to H^2(G_{L|K}, L^\times) \to H^2(G_{L|K}, \mathbb{A}_L^\times) \overset{j}{\to} H^2(G_{L|K}, \mathbb{C}_L) \overset{\delta}{\to} H^3(G_{L|K}, L^\times) \to 1.$$

Note that if j is surjective (i.e. $H^3(G_{L|K}, L^\times) = 1$), then we can push the invariance map defined on $H^2(G_{L|K}, \mathbb{A}_L^\times)$ to $H^2(G_{L|K}, \mathbb{C}_L)$ via j. However this is not always the case.

Theorem 8.26. *Let $L|K$ be a cyclic extension. Then $j \colon H^2(G_{L|K}, \mathbb{A}_L^\times) \to H^2(G_{L|K}, \mathbb{C}_L)$ is surjective.*

Proof. Note that in this case $H^3(G_{L|K}, L^\times) = H^1(G_{L|K}, L^\times) = 1$. ∎

Note that the map $H^2(G_{L|K}, \mathbb{A}_L^\times) \overset{j}{\to} H^2(G_{L|K}, \mathbb{C}_L)$ commutes with Res and Inf. More precisely:

$$j \circ \mathrm{Inf}_N = \mathrm{Inf}_N \circ j \text{ and } j \circ \mathrm{Res}_L = \mathrm{Res}_L \circ j,$$

where $N \supseteq L \supseteq K$ are normal extensions of K. We define the short hand notation:

$$H^q(L|K) = H^q(G_{L|K}, \mathbb{C}_L).$$

Note that by Theorem 8.15 this is a field formation. In particular

$$\mathrm{Inf}\colon H^2(L|K) \to H^2(N|K)$$

is injective and as before we view it as inclusion. We write

$$H^2(\Omega|K) = \bigcup_L H^2(L|K)\,(= \varinjlim_L H^2(L|K)).$$

Theorem 8.27. *Let $L|K$ be a normal extension and $L'|K$ be a cyclic extension of same degree (i.e. $[L'\colon K] = [L\colon K]$) Then we have*

$$H^2(L'|K) = H^2(L|K) \subseteq H^2(\Omega|K).$$

In particular we have

$$H^2(\Omega|K) = \bigcup_{\substack{L|K,\\ cyclic}} H^2(L|K).$$

Proof. We first show that $H^2(L'|K) \subseteq H^2(L|K)$. To do so we set $N = L' \cdot L$ and observe that $N|L$ is a cyclic. Take $c \in H^2(L'|K) \subseteq H^2(N|K)$. By exactness of the sequence

$$1 \to H^2(L|K) \to H^2(N|K) \overset{\mathrm{Res}}{\to} H^2(N|L)$$

we need to show that $\mathrm{Res}_L(c) = 1$. To do so we recall that in the cyclic case the map

$$j\colon H^2(G_{L'|K}, \mathbb{A}_L^\times) \to H^2(L'|K)$$

is surjective. Thus we write $c = jb$ with $b \in H^2(G_{L'|K}, \mathbb{A}_{L'}^\times) \subseteq H^2(G_{N|K}, \mathbb{A}_N^\times)$. We get

$$\mathrm{Res}_L(c) = \mathrm{Res}_L(jb) = j\mathrm{Res}_L(b).$$

Thus we have to show that $\mathrm{Res}_L(b) \in \ker(j) = H^2(G_{N|L}, N^\times)$. Since $N|L$ is cyclic we can do this by showing that

$$\mathrm{inv}_{N|L}(\mathrm{Res}_L(b)) = 0.$$

But this is the case because:

$$\mathrm{inv}_{N|L}(\mathrm{Res}_L(b)) = [L\colon K] \cdot \mathrm{inv}_{\mathrm{N|K}}(b) = [L'\colon K] \cdot \mathrm{inv}_{L'|K}(b) = 0.$$

This concludes the proof of the inclusion $H^2(L'|K) \subseteq H^2(L|K)$.

Equality follows from a simple consideration concerning orders. Indeed from the exact sequence

$$1 \to H^2(G_{L'|K}, (L')^\times) \to H^2(G_{L'|K}, \mathbb{A}_{L'}^\times) \to H^2(L'|K) \to 1$$

and Theorem 8.23 it follows that $\sharp H^2(L'|K) = [L'\colon K] = [L\colon K]$. This forces equality as claimed. ∎

This allows us to construct the global invariance map as follows. We first note that we can extend

$$j\colon H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times) \to H^2(\Omega|K)$$

simply by requiring that the restrictions to $H^2(G_{L|K}, \mathbb{A}_L^\times)$ (with $L|K$ finite normal extensions) are given by the earlier defined maps $j\colon H^2(G_{L|K}, \mathbb{A}_L^\times) \to H^2(L|K)$. This is well defined because j is compatible with inflation (aka inclusion).

Theorem 8.28. *The homomorphism $j\colon H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times) \to H^2(\Omega|K)$ is surjective.*

Proof. This follows directly because for any $c \in H^2(\Omega|K)$ there is a cyclic extension $L|K$ such that $c \in H^2(L|K)$. But

$$j|_{H^2(G_{L|K}, \mathbb{A}_L^\times)}\colon H^2(G_{L|K}, \mathbb{A}_L^\times) \to H^2(L|K)$$

is surjective. ∎

We are now ready to define inv:

Definition 8.3 (and Lemma)**.** Let $c \in H^2(\Omega|K)$ and $c = jb$ with $b \in H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times)$. Then we put

$$\mathrm{inv}_K(c) = \mathrm{inv}_K(b) \in \mathbb{Q}/\mathbb{Z}.$$

Proof. Suppose $c = j(b) = j(b')$ for $b, b' \in H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times)$. We need to show that

$$\mathrm{inv}_K(b) = \mathrm{inv}_K(b').$$

For a sufficiently large normal extension $L|K$ we find that, since $j(b) = j(b')$, the elements b and b' differ at most by an element of $\ker(j)$. But $\ker(j) = H^2(G_{L|K}, L^\times) \subseteq \ker(\mathrm{inv}_{L|K})$. ∎

We have obtained a homomorphism

$$\mathrm{inv}_K\colon H^2(\Omega|K) \to \mathbb{Q}/\mathbb{Z}.$$

Let $L|K$ be a normal extension then we put

$$\mathrm{inv}_K|_{H^2(L|K)} = \mathrm{inv}_{L|K}.$$

Note that the image of $\mathrm{inv}_{L|K}$ is in $\frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z}$. This is because elements in $H^2(L|K)$ have order dividing $[L\colon K]$ and must thus be contained in the (only) subgroup of $\mathbb{Q}/\mathbb{Z}$ with order $[L\colon K]$.

Theorem 8.29. *Let $c = j(b)$ with $c \in H^2(L|K)$ and $b \in H^2(G_{L|K}, \mathbb{A}_L^\times)$. Then we have*

$$\mathrm{inv}_{L|K}(c) = \mathrm{inv}_{L|K}(b).$$

The proof is obvious. Note that this only true for elements in the image of j. Since in general j is not surjective the route through cyclic extensions is not avoidable in general.

Theorem 8.30. *The maps*

$$\mathrm{inv}_K\colon H^2(\Omega|K) \to \mathbb{Q}/\mathbb{Z} \text{ and } \mathrm{inv}_{L|K}\colon H^2(L|K) \to \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z}$$

are isomorphisms.

Proof. It suffices to establish that $\mathrm{inv}_{L|K}$ is bijective. To see this we take a cyclic extension $L'|K$ of degree $[L'\colon K] = [L\colon K]$. We have $H^2(L|K) = H^2(L'|K)$. That the map is surjective is now easily seen: Take $x \in \frac{1}{[L\colon K]}\mathbb{Z}/\mathbb{Z}$ and find $b \in H^2(G_{L'|K}, \mathbb{A}_{L'}^\times)$ with $\mathrm{inv}_{L'|K}(b) = x$. For $c = j(b)$ we have by definition

$$\mathrm{inv}_{L|K}(c) = \mathrm{inv}_{L'|K}(c) = \mathrm{inv}_{L'|K}(b) = x.$$

This suffices because observing that $\sharp H^2(L|K) \mid [L\colon K]$ forces bijectivity. ∎

Sheet 11, Exercise 1: Let $L_1, \dots, L_r|K$ be r finite extensions of algebraic number fields. Assume that $L_i|K$ is cyclic of prime degree p for all $i = 1, \dots, r$. Further, assume that all fields are mutually disjoint:

$$L_s \cap (L_1 \cdots L_{s-1} \cdot L_{s+1} \cdots L_r) = K \text{ for all } 1 \le s \le r.$$

Show that there are infinitely many primes that split completely in L_i for $i = 2, \dots, r$ but remain prime in L_1.

Sheet 11, Exercise 2: Prove Theorem 8.4. More precisely, let $N \supset L \supset K$ be normal extensions. We use the symbols w', w and v to denote places of N, L and K respectively with $w'|w|v$. Show that

$$\begin{aligned}(\mathrm{Inf}_N c)_v &= \mathrm{Inf}_{N_{w'}}(c_v) \text{ for } c \in H^q(G_{L|K}, \mathbb{A}_L^\times) \text{ and } q \ge 1,\\ (\mathrm{Res}_L c)_w &= \mathrm{Res}_{L_w}(c_v) \text{ for } c \in H^q(G_{N|K}, \mathbb{A}_N^\times) \text{ and}\\ (\mathrm{CoRes}_K c)_v &= \sum_{w|v} \mathrm{CoRes}_{K_v}(c_w) \text{ for } c \in H^q(G_{N|L}, \mathbb{A}_N^\times).\end{aligned}$$

(Hint: Check the first two identities directly for $q \ge 1$ and then apply a dimension shifting argument. The third identity can be seen directly for $q = 0, -1$ and generalized by dimension shifting again.)

Clarification: Note that $\mathrm{CoRes}_{K_v}(c_w) \in H^q(G_{N_{w'}|K_v}, N_{w'}^\times)$. Thus the sum over $w \mid v$ contains terms that appear to be elements of different groups. To fix this we identify these cohomology groups as follows. We take $\sigma \in G_{N|K}$ and obtain an isomorphism $\sigma^*\colon N_{w'}^\times \to N_{\sigma w'}^\times$. This isomorphism allows us to identify $H^q(G_{N_{w'}|K_v}, N_{w'}^\times) \cong H^q(G_{N_{\sigma w'}|K_v}, N_{\sigma w'}^\times)$. We can use this procedure to view all the elements $\mathrm{CoRes}_{K_v}(c_w) \in H^q(G_{N_{w'}|K_v}, N_{w'}^\times)$ in the same group $H^q(G_{N_{\tilde{w}}|K_v}, N_{\tilde{w}}^\times)$ for some fixed $\tilde{w} \mid v$.

Sheet 12, Exercise 1: Let K be an algebraic number field. The Brauer group is defined as

$$\mathrm{Br}(K) = \bigcup_L H^2(G_{L|K}, L^\times),$$

where the union runs over all finite normal extensions $L|K$. Show that it suffices to take the union over cyclic extensions:

$$\mathrm{Br}(K) = \bigcup_{\substack{L|K,\\ \text{cyclic}}} H^2(G_{L|K}, L^\times),$$

(Hint: This is part of Theorem 8.8 of the lecture notes. Furthermore, Theorem 8.15 does not rely on this statement.)

Sheet 12, Exercise 2: Let $K = \mathbb{Q}(\sqrt{13}, \sqrt{17})$.

(1) Show that $\mathrm{Gal}(K|\mathbb{Q})$ is non-cyclic of order 4.
(2) Show that any prime splits completely in one of the quadratic subfields and deduce that $[K_\mathfrak{P} \colon \mathbb{Q}_p] \in \{1, 2\}$.
(3) Show that every rational square is a local norm at all primes.

Remark: It can be shown that $5^2 \notin N_{K|\mathbb{Q}} K^\times$. Thus the assumption that $L|K$ is cyclic in Hasse's norm theorem is necessary. Details can be found for example in [1].

Sheet 12, Exercise 3: Let K be an algebraic number field. Show that $x \in K^\times$ is a global square (i.e. $x = y^2$ for some $y \in K^\times$) if and only if it is a local square at all places (i.e. for each place v of K there is $y_v \in K_v^\times$ with $x = y_v^2$).

Sheet 12, Exercise 4: Let ζ be a 4th root of unity such that $\zeta^2 = i$. Put

$$L = \mathbb{Q}(\zeta) = \mathbb{Q}(i, \sqrt{2}) \supseteq M = \mathbb{Q}(i) \supseteq \mathbb{Q}.$$

(1) Show that 2 is the only prime ramified in $L|\mathbb{Q}$. Further show that 2 totally ramifies. For later reference let $\mathfrak{P}|\mathfrak{p}|2$ be the primes lying over 2 in L resp. M.
(2) Show that $z = (2+i)/(2-i) \in M^\times$ is a norm from $L^\times$.
(3) Show that the set $z \cdot (M_\mathfrak{p}^\times)^2$ does not contain $y \in N_{N|M} L^\times$ with $N_{M|\mathbb{Q}}(y) = 1$.
(4) Conclude that the set $\{x \in L \colon N_{L|\mathbb{Q}}(x) = 1\}$ is not dense in $\{x_\mathfrak{P} \in L_\mathfrak{P} \colon N_{L_\mathfrak{P}|\mathbb{Q}_2}(x_\mathfrak{P}) = 1\}$.

8.2. **The main theorems of Global Class Field Theory.** We fix some underlying algebraic number field K_0 and let Ω be the field of all algebraic numbers over K. Put $G = G_{\Omega|K_0}$. We set

$$\mathbb{C}_\Omega = \bigcup_K \mathbb{C}_K \; (= \varinjlim_K \mathbb{C}_K).$$

This is obviously a G-module.

Building on the foundations constructed in the previous subsection we can now obtain the following key theorem:

Theorem 8.31. *The formation $(G, \mathbb{C}_\Omega)$ with the invariance map defined in Definition 8.3 is a class formation.*

Proof. Axiom 1 is satisfied by Theorem 8.15. We have also seen iin Theorem 8.30 above that the maps

$$\mathrm{inv}_{L|K}\colon H^2(L|K) \to \frac{1}{[L\colon K]}\mathbb{Z}/Z$$

are isomorphisms. To verify Axiom 2 we need to check the required compatibility properties:

- Let $N \supset L \supset K$ be two normal extensions. For $c \in H^2(L|K) \subseteq H^2(N|K)$ we obviously have
$$\mathrm{inv}_{N|K}(c) = \mathrm{inv}_{L|K}(c)$$
by construction.
- Let $N \supset L \supset K$ be two extensions with $N|K$ normal. Let $c \in H^2(N|K)$ so that $\mathrm{Res}_L(c) \in H^2(N|L)$. We take $b \in H^2(G_{\Omega|K}, \mathbb{A}_\Omega^\times)$ with $j(b) = c$. We can take $M \supset N$ with $M|K$ normal so that $b \in H^2(G_{M|K}, \mathbb{A}_M^\times)$. Using the definition and Theorem 8.19 we get
$$\begin{aligned}\mathrm{inv}_{N|L}(\mathrm{Res}_L(c)) &= \mathrm{inv}_{M|L}(\mathrm{Res}_L(j(b))) = \mathrm{inv}_{\mathrm{M|L}}(j(\mathrm{Res}_L(b)))\\ &= \mathrm{inv}_{M|L}(\mathrm{Res}_L(b)) = [L\colon K]\cdot \mathrm{inv}_{M|K}(b)\\ &= [L\colon K]\cdot \mathrm{inv}_{M|K}(c).\end{aligned}$$

This allows us to use the abstract results earlier. Recall that the fundamental class $u_{L|K}$ was defined by

$$\mathrm{inv}_{L|K}(u_{L|K}) = \frac{1}{[L\colon K]} + \mathbb{Z}.$$

The abstract reciprocity theorem (Theorem 5.4) yields for example the isomorphisms

$$H^3(L|K) = 1 \text{ and } H^4(L|K) \cong \chi(G_{L|K}).$$

More importantly, an application with $q = -2$ yields:

Theorem 8.32 (Artin's Reciprocity Theorem)**.** *The map*

$$G_{L|K}^{\mathrm{ab}} \cong H^{-2}(G_{L|K}, \mathbb{Z}) \overset{u_{L|K}\cup}{\to} H^0(L|K) = \mathbb{C}_K/N_{L|K}\mathbb{C}_L$$

gives the (canonical isomorphism)

$$\theta_{L|K}\colon G_{L|K}^{\mathrm{ab}} \to \mathbb{C}_K/N_{L|K}\mathbb{C}_L.$$

This is called the reciprocity isomorphism.

The inverse of the reciprocity isomorphism $\theta_{L|K}$ leads to the exact sequence

$$1 \to N_{L|K}\mathbb{C}_L \to \mathbb{C}_K \overset{(\,,L|K)}{\to} G_{L|K}^{\mathrm{ab}} \to 1$$

where $(\,, L|K)$ is the norm residue symbol. According to Theorem 5.7 we have:

(1) For the canonical projection $\pi\colon G^{\mathrm{ab}}_{N|K} \to G^{\mathrm{ab}}_{L|K}$ we have

$$\begin{array}{ccc} \mathbb{C}_K & \xrightarrow{(\,,N|K)} & G^{\mathrm{ab}}_{N|K} \\ \| & & \downarrow{\scriptstyle \pi} \\ \mathbb{C}_K & \xrightarrow{(\,,L|K)} & G^{\mathrm{ab}}_{L|K} \end{array}$$

(2) For the Verlagerung we have

$$\begin{array}{ccc} \mathbb{C}_K & \xrightarrow{(\,,N|K)} & G^{\mathrm{ab}}_{N|K} \\ {\scriptstyle \mathrm{Incl}}\downarrow & & \downarrow{\scriptstyle \mathrm{Ver}} \\ \mathbb{C}_L & \xrightarrow{(\,,N|L)} & G^{\mathrm{ab}}_{N|L} \end{array}$$

(3) For the canonical homomorphism $\kappa\colon G^{\mathrm{ab}}_{N|L} \to G^{\mathrm{ab}}_{N|K}$ we have

$$\begin{array}{ccc} \mathbb{C}_L & \xrightarrow{(\,,N|L)} & G^{\mathrm{ab}}_{N|L} \\ {\scriptstyle N_{L|K}}\downarrow & & \downarrow{\scriptstyle \kappa} \\ \mathbb{C}_K & \xrightarrow{(\,,N|K)} & G^{\mathrm{ab}}_{N|K} \end{array}$$

(4) For the maps $\sigma\colon a \mapsto \sigma a$ and $\sigma^*\colon \tau \mapsto \sigma\tau\sigma^{-1}$ we have

$$\begin{array}{ccc} \mathbb{C}_K & \xrightarrow{(\,,N|K)} & G^{\mathrm{ab}}_{N|K} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma^*} \\ \mathbb{C}_{\sigma K} & \xrightarrow{(\,,\sigma N|\sigma K)} & G^{\mathrm{ab}}_{\sigma N|\sigma K} \end{array}$$

The following description of the norm residue symbol (going back to Hasse) is of key importance:

Theorem 8.33. *Let $L|K$ be an abelian extension and $a \cdot K^\times \in \mathbb{C}_K$ represented by an idele $a \in \mathbb{A}_K^\times$. Then we have*

$$(a \cdot K^\times, L|K) = \prod_v (a_v, L_w|K_v) \in G_{L|K}.$$

(All but finitely many factors in the product are trivial.)

Proof. We will use the characterisation

$$\chi((a \cdot K^\times, L|K)) = \mathrm{inv}_{L|K}([a \cdot K^\times] \cup \delta\chi)$$

given by Lemma 5.6. Here $\chi \in \chi(G_{L|K}) = H^1(G_{L|K}, \mathbb{Q}/\mathbb{Z})$ and $[a \cdot K^\times] = a \cdot K^\times \cdot N_{L|K}\mathbb{C}_L$. On the other hand, in Lemma 8.21 we have seen that

$$\chi\left(\prod_v (a_v, L_w|K_v)\right) = \mathrm{inv}_{L|K}([a] \cup \delta\chi),$$

for $[a] = a \cdot N_{L|K}\mathbb{A}_L^\times$.

Recall the map

$$j\colon H^q(G_{L|K}, \mathbb{A}_L^\times) \to H^q(G_{L|K}, \mathbb{C}_L)$$

and note that $j([a]) = [a \cdot K^\times]$. Thus we get

$$j([a] \cup \delta\chi) = [a \cdot K^\times] \cup \delta\chi.$$

But this implies

$$\chi((a \cdot K^\times, L|K)) = \mathrm{inv}_{L|K}([a \cdot K^\times] \cup \delta\chi) = \mathrm{inv}_{L|K}([a] \cup \delta\chi) = \chi\left(\prod_v (a_v, L_w|K_v)\right)$$

for any $\chi \in \chi(G_{L|K})$ and we are done. ∎

Remark 8.34. Let $G_K^{\mathrm{ab}} = \varprojlim_L G_{L|K}$ where L is running over all finite abelian extensions $L|K$. (G_K^{ab} is the Galois group of the maximal abelian extension A_K of K.) We set

$$(c, K) = \varprojlim (c, L|K) \in G_K^{\mathrm{ab}} \text{ for } c \in \mathbb{C}_K$$

to get the universal norm residue symbol

$$(\,, K)\colon \mathbb{C}_K \to G_K^{\mathrm{ab}}.$$

The kernel is given by

$$D_K = \bigcap_L N_{L|K}\mathbb{C}_L$$

and the image is dense. Further one has the product formula

$$(a \cdot K^\times, K) = \prod_v (a, K_v).$$

As in the abstract case we call a subgroup $I \subseteq \mathbb{C}_K$ a norm group (of K) if there is a normal extension $L|K$ with $I = N_{L|K}\mathbb{C}_L$. By Theorem 5.10 these classify finite abelian extensions of K:

Theorem 8.35. *The map*

$$L \mapsto I_L = N_{L|K}\mathbb{C}_L$$

gives an inclusion reversing isomorphism between finite abelian extensions L of K and norm groups I of K. Indeed we have

$$I_{L_1} \supseteq I_{L_2} \Leftrightarrow L_1 \subseteq L_2;\ I_{L_1 \cdot L_2} = I_{L_1} \cap I_{L_2} \text{ and } I_{L_1 \cap L_2} = I_{L_1} \cdot I_{L_2}.$$

Furthermore, every group containing a norm group $I \subseteq \mathbb{C}_K$ is itself a norm group.

The field L associated to a norm group of $I \subseteq \mathbb{C}_K$ is called the class field of I. To turn the last theorem into a more useful result we need to understand the norm groups of $\mathbb{C}_K$ better. This is where the topology of the ideles comes into play.

Theorem 8.36. *Let K be a field containing the nth roots of unity. Further let $S \supseteq S_\infty$ be a finite set of places such that*

- *S contains all finite places lying above prime divisors of n; and*
- $\mathbb{A}_K^\times = \mathbb{A}_K^{\times,S} \cdot K^\times$.

We define

$$U_K(S) = \{a \in \mathbb{A}_K^\times \colon a_v = 1 \text{ for } v \in S,\ a_v \in \mathcal{O}_v^\times \text{ if } v \notin S\}$$

and set $\overline{U}_K(S) = U_K(S) \cdot K^\times/K^\times \subseteq \mathbb{C}_K$. Then $\mathbb{C}_K^n \cdot \overline{U}_K(S)$ is the norm group corresponding to the kummerian field $T = K(\sqrt[n]{K^S})$. Further, even if K does not contain the nth roots of unity, then $\mathbb{C}_K^n \cdot \overline{U}_K(S)$ is still a norm group.

Proof. We first recall that

$$\chi(G_{T|K}) \cong K^S \cdot (K^\times)^n/(K^\times)^n \cong K^S/(K^S)^n.$$

Further recall that, by the (generalized) Dirichlet unit theorem, the rank of K^S is $\sharp S - 1$. As before, since K contains the nth roots of unity, one concludes that $K^S/(K^S)^n$ is the direct product of $\sharp S$ cyclic groups of order n.

Take $[a] = a \cdot K^\times \in \mathbb{C}_K$ and observe

$$([a]^n, T|K) = ([a], T|K)^n = 1.$$

This implies $[a]^n \in N_{T|K}\mathbb{C}_T$, so that

$$(\mathbb{C}_K)^n \subseteq N_{T|K}\mathbb{C}_T.$$

Next we will show that each $a \in U_K(S)$ is the norm of an idele in the extension $T|K$. This can be checked locally. If $v \in S$, then $a_v = 1$ and there is nothing to show. For $\mathfrak{p} \notin S$ we have $a_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^\times$. Now by local class field theory $a_\mathfrak{p}$ is a norm as soon as we can show that $K_\mathfrak{p}(\sqrt[n]{K^S})|K_\mathfrak{p}$ is unramified. But this is easily shown by considering the equation $X^n - t$ over the residue field. (Keeping in mind that n is co-prime to the residue characteristic and t is a unit.)

Since $U_K(S) \subseteq N_{T|K}\mathbb{A}_T^\times$ we have $\overline{U}_K(S) \subseteq N_{T|K}\mathbb{C}_T$. In summary we have already seen that

$$(\mathbb{C}_K)^n \cdot \overline{U}_K(S) \subseteq N_{T|K}\mathbb{C}_T.$$

Equality will follow from an index computation using the reciprocity law:

$$[\mathbb{C}_K \colon N_{T|K}\mathbb{C}_T] = \sharp G_{T|K} = n^{\sharp S}$$

It now remains to show that

$$n^{\sharp S} = [\mathbb{C}_K \colon (\mathbb{C}_K)^n \cdot \overline{U}_K(S)] = \frac{[\mathbb{A}_K^{\times,S} \colon (\mathbb{A}_K^{\times,S})^n U_K(S)]}{[K^S \colon ((\mathbb{A}_K^{\times,S})^n U_K(S) \cap K^\times)]}.$$

The numerator is easy to compute via:

$$[\mathbb{A}_K^{\times,S} \colon (\mathbb{A}_K^{\times,S})^n U_K(S)] = \prod_{v \in S} \underbrace{[K_v^\times \colon (K_v^\times)^n]}_{=n^{2\cdot|n|_v}} = n^{2\sharp S}.$$

To compute the denominator we will first show that $(\mathbb{A}_K^{\times,S})^n U_K(S) \cap K^\times = (K^S)^n$. This then directly implies $[K^S \colon ((\mathbb{A}_K^{\times,S})^n U_K(S) \cap K^\times)] = n^{\sharp S}$ and we are

done. Note that the inclusion $(K^S)^n \subseteq (\mathbb{A}_K^{\times,S})^n U_K(S) \cap K^\times$ is obvious. On the other hand we can take $x \in (\mathbb{A}_K^{\times,S})^n U_K(S) \cap K^\times$ and write $x = a^n \cdot u$ with $a \in \mathbb{A}_K^{\times,S}$ and $u \in U_K(S)$. It suffices to show that $K(\sqrt[n]{x}) = K$. This is done following the old strategy and showing that

$$N_{K(\sqrt[n]{x})|K}\mathbb{C}_{K(\sqrt[n]{x})} = \mathbb{C}_K$$

and applying the reciprocity theorem.

Finally let us take a look at the case when K does not contain the nth roots of unity. Then we let $\widetilde{K} = K(\mu_n)$ be the extension of K obtained by adjoining the nth roots of unity. Let $\tilde{S}$ be a finite set of places containing all places lying above S and that satisfies $\mathbb{A}_{\widetilde{K}}^\times = \mathbb{A}_{\widetilde{K}}^{\times,\tilde{S}} \cdot \widetilde{K}^\times$. As seen above the extension $T|\widetilde{K}$ has norm group $(\mathbb{C}_{\widetilde{K}})^n \overline{U}_{\widetilde{K}}(\tilde{S})$. Let $L|K$ be the smallest normal extension such that $T \subseteq L$. We compute

$$\begin{aligned} N_{L|K}\mathbb{C}_L &= N_{\widetilde{K}|K}(N_{T|\widetilde{K}}(N_{L|T}\mathbb{C}_L)) \subseteq N_{\widetilde{K}|K}(N_{T|\widetilde{K}}\mathbb{C}_T) \\ &= N_{\widetilde{K}|K}((\mathbb{C}_{\widetilde{K}})^n \overline{U}_{\widetilde{K}}(\tilde{S})) \subseteq (\mathbb{C}_K)^n \overline{U}_K(S). \end{aligned}$$

This completes the proof, since subgroups containing norm groups are themselves norm groups. ∎

Theorem 8.37 (Existence Theorem)**.** *The norm groups of $\mathbb{C}_K$ are precisely the closed subgroups of finite index.*

Proof. Let $\mathcal{N}_L = N_{L|K}\mathbb{C}_L$ be the norm group of a (finite) normal extension. Then by the reciprocity theorem we have

$$[\mathbb{C}_K : \mathcal{N}_L] = \sharp G_{L|K}^{\mathrm{ab}} < \infty.$$

To see that it is closed we argue as follows. We write

$$\mathbb{C}_K = \mathbb{C}_K^1 \times \Gamma_K \text{ and } \mathbb{C}_L = \mathbb{C}_L^1 \times \Gamma_L$$

with $\mathbb{R}_+ \cong \Gamma_K = \Gamma_L \subseteq \mathbb{C}_L$. We have

$$\mathcal{N}_L = N_{L|K}\mathbb{C}_L^1 \times N_{L|K}\Gamma_K = N_{L|K}\mathbb{C}_L^1 \times \Gamma_K^n = N_{L|K}\mathbb{C}_L^1 \times \Gamma_K$$

But since $\mathbb{C}_L^1$ is compact also $N_{L|K}\mathbb{C}_L^1$ is compact (and in particular closed) by continuity of $N_{L|K}$.

Next let $I \subseteq \mathbb{C}_K$ be closed and of finite index. We write $[\mathbb{C}_K : I] = n$. Then $\mathbb{C}_K^n \subseteq I$. Further we observe that I must contain $\overline{U}_K(S)$ for a sufficiently large finite set S. But by the previous result (making S larger if necessary) the set $\mathbb{C}_K^n \cdot \overline{U}_K(S)$ is a norm group of K. Thus also I is one. ∎

A modulus $\mathfrak{m}$ is a formal product

$$\mathfrak{m} = \mathfrak{m}_\infty \cdot \prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}},$$

where $n_\mathfrak{p} = 0$ for almost all (finite places) $v = v_\mathfrak{p}$ and $\mathfrak{m}_\infty$ is a formal product of infinite places. We set

$$\mathbb{A}_K^{\times,\mathfrak{m}} = \prod_v U_v^{n_v} \subseteq \mathbb{A}_K^\times.$$

We also define the $\mathfrak{m}$th congruence subgroup

$$\mathbb{C}_K^\mathfrak{m} = \mathbb{A}_K^{\times,\mathfrak{m}} \cdot K^\times / K^\times$$

of $\mathbb{C}_K$ and associate the ray class group modulo $\mathfrak{m}$: $\mathbb{C}_K/\mathbb{C}_K^\mathfrak{m}$.

Theorem 8.38. *The norm groups of K are precisely those subgroups of $\mathbb{C}_K$ containing a congruence subgroup $\mathbb{C}_K^\mathfrak{m}$.*

Proof. It is easy to see that $\mathbb{C}_K^\mathfrak{m}$ is closed and has finite index (Exercise). Thus they are norm groups and so are all the groups containing them.

Next given a norm group $I \subseteq \mathbb{C}_K$, by the existence theorem I is closed and of finite index. It is easy to see that I must contain $\mathbb{C}_K^\mathfrak{m}$ for a sufficiently large modulus $\mathfrak{m}$. ∎

The class field L of $\mathbb{C}_K^\mathfrak{m}$ is called the ray class field modulo $\mathfrak{m}$. By the reciprocity theorem we have

$$G_{L|K} \cong \mathbb{C}_K/\mathbb{C}_K^\mathfrak{m}.$$

The ray class field modulo $\mathbf{1}$ (i.e. the trivial modulus) is called the Hilbert Class field. If H is the Hilbert class field of K, then it is easy to see that $[H\colon K] = h_K$ and $G_{H|K} \cong \mathcal{C}_K$. Making the modulus larger makes the corresponding congruence subgroup smaller. This in turn makes the corresponding ray class field larger. The previous theorem tells us that every abelian extension $L|K$ is contained in a ray class field modulo $\mathfrak{m}$ with $\mathfrak{m}$ sufficiently large.

Theorem 8.39. *Let $m \in \mathbb{N}$ and write p_∞ for the (unique) archimedean place of $\mathbb{Q}$. Then the ray class field modulo $\mathfrak{m} = p_\infty \cdot m$ is the cyclotomic field $\mathbb{Q}(\zeta)$ generated by an mth root of unity ζ.*

Note that this immediately implies the Kronecker-Weber Theorem (compare Theorem 6.23).

Proof. Let ζ be a primitive mth root of unity and write $m = \prod_p p^{n_p}$. An easy local computation shows that $U_p^{n_p}$ is contained in the norm group of $\mathbb{Q}_p(\zeta)$ (over $\mathbb{Q}_p$). Thus $\mathbb{A}_\mathbb{Q}^{\times,\mathfrak{m}}$ indeed consists of norms from $\mathbb{A}_{\mathbb{Q}(\zeta)}^\times$. This implies

$$\mathbb{C}_Q^\mathfrak{m} \subseteq N_{\mathbb{Q}(\zeta)|\mathbb{Q}}\mathbb{C}_{\mathbb{Q}(\zeta)}.$$

This shows that $\mathbb{Q}(\zeta)$ is contained in the ray class field modulo $\mathfrak{m}$. To see equality we simply have to show that $[\mathbb{C}_\mathbb{Q}\colon \mathbb{C}_\mathbb{Q}^\mathfrak{m}] = \varphi(m)$. We first observe that

$$[\mathbb{C}_\mathbb{Q}\colon \mathbb{C}_\mathbb{Q}^\mathfrak{m}] = [\mathbb{A}_Q^{\times,\mathbf{1}}\colon \mathbb{A}_\mathbb{Q}^{\times,\mathfrak{m}}]/[(\mathbb{A}_Q^{\times,\mathbf{1}} \cap \mathbb{Q}^\times)\colon (\mathbb{A}_\mathbb{Q}^{\times,\mathfrak{m}} \cap \mathbb{Q}^\times)].$$

Clearly one has

$$[\mathbb{A}_Q^{\times,\mathbf{1}}\colon \mathbb{A}_{\mathbb{Q}}^{\times,\mathfrak{m}}] = 2\varphi(m) \text{ and } [(\mathbb{A}_Q^{\times,\mathbf{1}} \cap \mathbb{Q}^\times)\colon (\mathbb{A}_{\mathbb{Q}}^{\times,\mathfrak{m}} \cap \mathbb{Q}^\times)] = \sharp\mathbb{Z}^\times = 2.$$

This completes the argument. ∎

Turning to the (universal) norm residue symbol again we can derive the following result:

Theorem 8.40. *The universal norm residue symbol*

$$(\,,K)\colon \mathbb{C}_K \to G_K^{\mathrm{ab}} \tag{11}$$

is continuous, surjective and its kernel is

$$D_K = \bigcap_{n=1}^{\infty} (\mathbb{C}_K)^n.$$

Proof. We first look at the kernel. It is obvious that $\bigcap_n (\mathbb{C}_K)^n \subseteq D_K$. On the other hand $D_K \subseteq \mathbb{C}_K^n \cdot \overline{U}_K(S)$ (by the existence theorem.) Thus it suffices to show that $\bigcap_S \mathbb{C}_K^n \cdot \overline{U}_K(S) = \mathbb{C}_K^n$. To see this take

$$[a] \in \bigcap_S \mathbb{C}_K^n \overline{U}_K(S).$$

Thus for each S we write $[a] = [b_S]^n \cdot [u_S]$ accordingly. Since $\bigcap_S U_K(S) = 1$ the u_S must approach 1 for sufficiently large S. Thus

$$[a] = \lim_S [a] \cdot [u_S]^{-1} \in \mathbb{C}_K^n.$$

The containment follows since $\mathbb{C}_K^n$ is closed (Exercise).

To see continuity we take $H \subseteq G_K^{\mathrm{ab}}$ open. Thus H is precisely closed and of finite index. Let L be the field fixed by H. Then the corresponding norm group $N_{L|K}\mathbb{C}_L$ is open and is mapped into H by the universal norm residue symbol.

From $\mathbb{C}_K = \mathbb{C}_K^1 \times \Gamma_K$ and $\Gamma_K \cong \mathbb{R}_+$ it follows that $\mathbb{C}_K^n = (\mathbb{C}_K^1)^n \times \Gamma_K$. In particular Γ_K is contained in the kernel of $(\,,K)$. We have

$$(\mathbb{C}_K, K) = (\mathbb{C}_K^1, K).$$

By compactness of $\mathbb{C}_K^1$ the image must be closed. We can now conclude that $(\,,K)$ is surjective because the image is known to be dense. ∎

We finally come to the relevance of class field theory to the splitting behaviour of primes (in abelian extensions).

Theorem 8.41. *Let $L|K$ be an abelian extension of degree n and let $\mathfrak{p}$ be an unramified prime ideal of K. Let ϖ be the uniformiser in $K_\mathfrak{p}$ and define $\mathfrak{n}_\mathfrak{p}(\varpi) = (\ldots, 1, \varpi, 1, \ldots) \in \mathbb{A}_K^\times$. Further let f be the smallest (positive) integer so that*

$$\overline{\mathfrak{n}}_\mathfrak{p}(\varpi)^f \in N_{L|K}\mathbb{C}_L.$$

Then $\mathfrak{p} \cdot \mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ for $r = \frac{n}{f}$. Each of the prime ideals $\mathfrak{P}_i$ of L has degree f.

Proof. Since $\mathfrak{p}$ is unramified the only thing to show is that the prime ideals $\mathfrak{P}$ lying above $\mathfrak{p}$ have degree f. Recall that Artin's reciprocity law tells us that $\mathbb{C}_K/N_{L|K}\mathbb{C}_L \cong G_{L|K}$. Now the order of $\overline{\mathfrak{n}}_\mathfrak{p}(\varpi)$ mod $N_{L|K}\mathbb{C}_L$ has the same order (i.e. f) as the element

$$(\overline{\mathfrak{n}}_\mathfrak{p}(\varpi), L|K) = (\varpi, L_\mathfrak{P}|K_\mathfrak{p}) = \varphi_\mathfrak{p} \in G_{L_\mathfrak{P}|K_\mathfrak{p}} \subseteq G_{L|K}.$$

But the order of the Frobenius automorphism $\varphi_\mathfrak{p}$ must by definition agree with the degree $[L_\mathfrak{P}\colon K_\mathfrak{p}]$. ∎

Theorem 8.42. *Let $L|K$ be an abelian extension. When viewing the map $\overline{\mathfrak{n}}_\mathfrak{p}\colon K_\mathfrak{p}^\times \to \mathbb{C}_K$ as an embedding we obtain*

$$N_{L|K}\mathbb{C}_L \cap K_\mathfrak{p}^\times = N_{L_\mathfrak{P}|K_\mathfrak{p}} L_\mathfrak{P}^\times.$$

Proof. It is obvious that if $x_\mathfrak{p} \in N_{L_\mathfrak{P}|K_\mathfrak{p}} L_\mathfrak{P}^\times$, then $\mathfrak{n}_\mathfrak{p}(x_\mathfrak{p}) \in N_{L|K}\mathbb{A}_L^\times$. This implies the first inclusion.

Now take $[a] \in N_{L|K}\mathbb{C}_L \cap K_\mathfrak{p}^\times$. Thus we can write the representative $a \in \mathbb{A}_K^\times$ as $a = N_{L|K} b$ with $b \in \mathbb{A}_L^\times$. Thus there is $k \in K^\times$ such that

$$\mathfrak{n}_\mathfrak{p}(x_\mathfrak{p}) \cdot k = N_{L|K} b.$$

Looking componentwise we see that k is a (local) norm at all places $v \neq \mathfrak{p}$. By the product formula we find that it is also a norm at the place $\mathfrak{p}$, which in turn implies that $\mathfrak{n}_\mathfrak{p}(x_\mathfrak{p})$ is a local norm. This shows the reverse inclusion and thus the statement. ∎

Theorem 8.43. *Let $L|K$ be an abelian extension with norm group $\mathcal{N}_L = N_{L|K}\mathbb{C}_L$. Let v be a place of K. Then v is unramified in L if and only if $\mathcal{O}_v^\times \subseteq \mathcal{N}_L$. Furthermore, v splits completely in L if and only if $K_\mathfrak{p}^\times \subseteq \mathcal{N}_L$. (Recall that an infinite place v is called unramified if $L_w = K_v$.)*

Proof. This is an easy exercise combining the previous observations with local results. ∎

Definition 8.4. Let $L|K$ be an abelian extension with norm group $\mathcal{N}_L = N_{L|K}\mathbb{C}_L$. Then the conductor $\mathfrak{f}$ of $\mathcal{N}_L$ (or of $L|K$) is the greatest common divisor of all moduli $\mathfrak{m}$ with $\mathbb{C}_K^\mathfrak{m} \subseteq \mathcal{N}_L$.

Theorem 8.44. *Let $\mathfrak{f}$ be the conductor of the abelian extension $L|K$ and $\mathfrak{f}_\mathfrak{p}$ be the conductor of the local extension $L_\mathfrak{P}|K_\mathfrak{p}$. Then we have*

$$\mathfrak{f} = \prod_\mathfrak{p} \mathfrak{f}_\mathfrak{p}.$$

Proof. The claim is a consequence of the following sequence of equivalences:

$$\begin{aligned}
\mathbb{C}_K^{\mathfrak{m}} \subseteq \mathcal{N}_L &\Leftrightarrow [a \equiv 1 \bmod \mathfrak{m} \implies [a] \in \mathcal{N}_L] \text{ for } a \in \mathbb{A}_K^\times \\
&\Leftrightarrow [a_\mathfrak{p} = 1 \bmod \mathfrak{p}^{n_\mathfrak{p}} \implies \overline{\mathfrak{n}}_\mathfrak{p}(a_p) \in \mathcal{N}_L \cap K_\mathfrak{p}^\times] \\
&\Leftrightarrow [a_\mathfrak{p} \in U_\mathfrak{p}^{n_\mathfrak{p}} \implies a_\mathfrak{p} \in N_{L_\mathfrak{P}|K_\mathfrak{p}} L_\mathfrak{P}^\times] \\
&\Leftrightarrow U_\mathfrak{p}^{n_\mathfrak{p}} \subseteq N_{L_\mathfrak{P}|K_\mathfrak{p}} L_\mathfrak{P}^\times \\
&\Leftrightarrow \mathfrak{f}_\mathfrak{p} \mid \mathfrak{p}^{n_\mathfrak{p}}.
\end{aligned}$$

□

We arrive at the following theorem:

Theorem 8.45. *Let $L|K$ be an abelian extension. A place $\mathfrak{p}$ of K is ramified in L if and only if $\mathfrak{p} \mid \mathfrak{f}$. In particular, all places of K are unramified in L if and only if $\mathfrak{f} = 1$.*

A direct but very important consequence is the following characterisation of the Hilbert class field:

Theorem 8.46. *The Hilbert class field of K is the maximal unramified abelian extension of K.*

Remark 8.47. Note that since $\mathbb{C}_K/\mathbb{C}_K^{\mathbf{1}} \cong \mathcal{C}_K$ the Hilbert class field has degree h_K. In particular, if $h_K = 1$, then every abelian extension of K is ramified. (Taking $K = \mathbb{Q}$ we recover Minkowski's classical theorem.)

We define the class field tower inductively as follows. Let $K_0 = K$ and write K_n for the Hilbert class field of K_{n-1} (where $n \in \mathbb{N}$).

Theorem 8.48. *The ith class field K_i is normal over K and K_1 is the biggest abelian subfield of K_2 (i.e. $G_{K_2|K_1} = [G_{K_2|K}, G_{K_2|K}]$).*

Proof. We proof the normality inductively. Let σ be an isomorpism of K_{i+1} over K. Then (since $\sigma K_i = K_i$) the extension $\sigma K_{i+1}|K_i$ is abelian and unramified. In particular $\sigma K_{i+1} \subseteq K_{i+1}$. Thus $K_{i+1}|K$ is normal as claimed.

For the second part let K' be the maximal abelian subextension of $K_2|K$. Of course we must have $K_1 \subseteq K'$, because $K_1|K$ is abelian. But $K'|K$ is unramified, so that also $K' \subseteq K_1$. □

Remark 8.49. The class field tower problem asks if the tower $K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots$ terminates after finitely many steps. It turns out that this is not the case. Indeed in 1964 it was shown by Golod and Shaferevic that infinite class field towers exist.

Theorem 8.50 (Principal Ideal Theorem)**.** *In the Hilbert class field of K every ideal $\mathfrak{a}$ of K is principal.*

Proof. We need to translate this into idelic language. First note that we have to show that the obvious map

$$\mathcal{C}_K \to \mathcal{C}_{K_1}$$

is trivial. However, we have the commutative diagram

$$\begin{array}{ccc} \mathbb{C}_K/\mathbb{C}_K^{\mathbf{1}} & \xrightarrow{\cong} & \mathcal{C}_K \\ \downarrow{\scriptstyle i} & & \downarrow \\ \mathbb{C}_{K_1}/\mathbb{C}_{K_1}^{\mathbf{1}} & \xrightarrow{\cong} & \mathcal{C}_{K_1} \end{array}$$

where i is obtained from the inclusion $\mathbb{C}_K \to \mathbb{C}_{K_1}$. Thus we need to show that $\mathbb{C}_K \subseteq \mathbb{C}_{K_1}^{\mathbf{1}}$.

To see this we observe that (by construction of the class field tower) $\mathbb{C}_{K_1}^{\mathbf{1}}$ is the norm group of $K_2|K_1$. The problem reduces to showing that

$$1 = (\mathbb{C}_K, K_2|K_1) = \mathrm{Ver}(\mathbb{C}_K, K_2|K).$$

Recall that

$$(\mathbb{C}_K, K_2|K) = G_{K_2|K}^{\mathrm{ab}} = G_{K_1|K}.$$

Thus the problem is reduced to the purely group theoretic statement: Let G be a finite group with abelian commutator group G', then the Verlagerung

$$\mathrm{Ver}\colon G^{\mathrm{ab}} \to G'$$

is trivial. (This statement was discussed in Sheet 6, Exercise 3 and Sheet 7, Exercise 1.) □

Sheet 13, Exercise 1: Let $m \in \mathbb{N}$ be an integer. Compute the ray class field of $\mathbb{Q}$ modulo $\mathfrak{m} = m$.

Sheet 13, Exercise 2: Let p and q be two odd prime numbers. Recall that the Legendre symbol is defined by

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{if } q \equiv x^2 \bmod p, \\ -1 & \text{else.} \end{cases}$$

The law of quadratic reciprocity states that

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{12}$$

Derive (12) from the reciprocity theorem of global class field theory. This can be done by considering the extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p'}) \subseteq \mathbb{Q}(\zeta),$$

where $p' = (-1)^{\frac{p-1}{2}} \cdot p$ and ζ is a primitive pth root of unity.

Sheet 13, Exercise 3: Let $L|K$ be a (finite) normal extension of algebraic number fields.

(1) Show that $\delta\colon H^2(G_{L|K}, \mathbb{C}_L) \to H^3(G_{L|K}, L^\times)$ is surjective.
(2) Show that $H^3(G_{L|K}, L^\times)$ is cyclic and compute its order.

Sheet 13, Exercise 4: Let $K = \mathbb{Q}(\sqrt{-5})$. Show that the Hilbert Class Field of K is $K(i)$. (It can be used without proof that the ideal class group of K has order 2.)

8.3. **Reflections on the Ideal Theoretic Formulation.** Let $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ be a modulus for K. Then we let $\mathcal{J}_K^{\mathfrak{m}}$ be the group of all (fractional) ideals co-prime to $\mathfrak{m}$. Similarly $\mathcal{P}_{0,K}^{\mathfrak{m}}$ is defined to be the group of all principal ideal $(a) \in \mathcal{P}_K$ with $a \equiv 1 \bmod \mathfrak{m}$.

Definition 8.5. Let $L|K$ be an abelian extension and let $\mathfrak{m}$ be a modulus for $L|K$ (i.e. $\mathbb{C}_K^{\mathfrak{m}} \subseteq N_{L|K}\mathbb{C}_L$). Then we define

$$H^{\mathfrak{m}} = N_{L|K}\mathcal{J}_L^{\mathfrak{m}} \cdot \mathcal{P}_{0,K}^{\mathfrak{m}}.$$

This is called the mod $\mathfrak{m}$ ideal group associated to $L|K$.

For a prime ideal $\mathfrak{p}$ away from a modulus $\mathfrak{m}$ of $L|K$ we can define the Artin symbol as usual by

$$\left(\frac{L|K}{\mathfrak{p}}\right) = \varphi_{\mathfrak{p}} \in G_{L|k}.$$

This is extended multiplicatively to $\mathcal{J}_K^{\mathfrak{m}}$. Artin's reciporicty theorem can now be formulated as:

Theorem 8.51. *Let $L|K$ be an abelian extension and let $\mathfrak{m}$ be a modulus for $\mathfrak{m}$. Then we have the exact sequence*

$$1 \to H^{\mathfrak{m}}/\mathcal{P}_{0,K}^{\mathfrak{m}} \to \mathcal{J}_K^{\mathfrak{m}}/\mathcal{P}_{0,K}^{\mathfrak{m}} \overset{\left(\frac{L|K}{\cdot}\right)}{\to} G_{L|K} \to 1.$$

Proof. Of course this can be reduced to the exactness of

$$1 \to N_{L|K}\mathbb{C}_L \to \mathbb{C}_K \overset{(\,,L|K)}{\to} G_{L|K} \to 1.$$

We only sketch the necessary steps. First one defines the homomorphism

$$\kappa\colon \mathbb{A}_K^{\times} \to \mathcal{J}_K,\ a \mapsto \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(a_{\mathfrak{p}})}.$$

It can be computed that κ induces an ismorphism[17]

$$\overline{\kappa}_{\mathfrak{m}}\colon \mathbb{C}_K/\mathbb{C}_K^{\mathfrak{m}} \to \mathcal{J}^{\mathfrak{m}}/\mathcal{P}_{0,K}^{\mathfrak{m}}.$$

Even more, its restriction to $N_{L|K}\mathbb{C}_L/\mathbb{C}_K^{\mathfrak{m}}$ has image $H^{\mathfrak{m}}/\mathcal{P}_{0,K}^{\mathfrak{m}}$.

Next it can be shown that the diagram

[17] This is done as follows. We define

$$U(\mathfrak{m}) = \{a \in \mathbb{A}_K^{\times}\colon a_{\mathfrak{p}} \in U_{\mathfrak{p}}^{(n_{\mathfrak{p}})} \text{ for } \mathfrak{p} \mid \mathfrak{m}\} \subseteq \mathbb{A}_K^{\times}.$$

Using the approximation theorem (i.e. Theorem 3.5) one shows that $\mathbb{C}_K = U(\mathfrak{m})K^{\times}/K^{\times}$. The map κ (restricted to $U(\mathfrak{m})$) now induces the surjective map

$$\mathbb{C}_K = U(\mathfrak{m})K^{\times}/K^{\times} = U(\mathfrak{m})/[U(\mathfrak{m}) \cap K^{\times}] \to \mathcal{J}_K^{\mathfrak{m}}/\mathcal{P}_{0,K}^{\mathfrak{m}}.$$

One concludes easily by computing the kernel.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & N_{L|K}\mathbb{C}_L & \longrightarrow & \mathbb{C}_K & \xrightarrow{(\,,L|K)} & G_{L|K} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \kappa_{\mathfrak{m}}} & & \downarrow{\scriptstyle \kappa_{\mathfrak{m}}} & & \downarrow{\scriptstyle =} & & \\ 1 & \longrightarrow & H^{\mathfrak{m}}/\mathcal{P}^{\mathfrak{m}}_{0,K} & \longrightarrow & \mathcal{J}^{\mathfrak{m}}_K/\mathcal{P}^{\mathfrak{m}}_{0,K} & \xrightarrow{\left(\frac{L|K}{}\right)} & G_{L|K} & \longrightarrow & 1 \end{array}$$

commutes. Moreover, both arrows featuring $\kappa_{\mathfrak{m}}$ are surjective and have kernel $\mathbb{C}^{\mathfrak{m}}_K$. The commutativity of the right hand block relies on the identity

$$\left(\frac{L|K}{\mathfrak{p}}\right) = (\overline{\mathfrak{n}}_{\mathfrak{p}}(\varpi), L|K).$$

□

Finally we can give a classical formulation of the decomposition theorem:

Theorem 8.52. *Let $L|K$ be an abelian extension and let $\mathfrak{p}$ be an unramified prime ideal (of K in L). Further let $\mathfrak{m}$ be a modulus for $L|K$ that is not divisible by $\mathfrak{p}$ (for example the conductor $\mathfrak{f}$). Let f be the order of $\mathfrak{p}$ mod $H^{\mathfrak{m}}$ in $\mathcal{J}^{\mathfrak{m}}_K/H^{\mathfrak{m}}$. Then $\mathfrak{p}$ decomposes in $r = [L\colon K]/f$ distinct prime ideals $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ of degree f.*

Note that going back to the introduction (Section 1) it is now easy to verify the claims made therein.

References

1. John William Scott Cassels, Albrecht Fröhlich, et al., *Algebraic number theory: Proceedings of an instructional conference organized by the london mathematical society (a nato advanced study institute) with the support of the international mathematical union*, (No Title) (1967).
2. F. Lorenz, *Ein Scholion zum Satz 90 von Hilbert*, Abh. Math. Sem. Univ. Hamburg **68** (1998), 347–362. MR 1658433
3. Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859
4. Jürgen Neukirch, *Klassenkörpertheorie: Neu herausgegeben von alexander schmidt*, Springer-Verlag, 2011.
5. Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR 2392026
6. B. F. Wyman, *What is a reciprocity law?*, Amer. Math. Monthly **79** (1972), 571–586; correction, ibid. 80 (1973), 281. MR 308084