The Grunwald-Wang Theorem

Part III Essay by Martin Luedtke

Supervised by Tom Fisher
at the University of Cambridge

May 1, 2013

Contents

Introduction

The aim of this essay is to give a proof of the Grunwald-Wang theorem, which roughly states that, given a number field k, one can prescribe a finite abelian Galois group and finitely many local extensions $K_\mathfrak{p}|k_\mathfrak{p}$ of the completions of k, and there will always (under reasonable assumptions) be an extension $K|k$ that realises the given data, i.e. has the given Galois group and the given completions $K_\mathfrak{p}$. There is however one special case involving the prime 2 in which the Grunwald-Wang theorem does not hold. A similar situation occurs for the question whether a number $a \in k^\times$ that is an mth power in all completions of k, is already an mth power in k. It turns out that this, too, is only

almost true: There is again a special case involving the prime 2 for which the assertion does not hold. In fact the two questions are closely related, and often both go under the name "Grunwald-Wang theorem". We will however refer to the second question as the "Hasse principle for mth powers" and use the name Grunwald-Wang theorem only for the first one to avoid confusion.

German mathematician Wilhelm Grunwald introduced the Hasse principle for mth powers in 1933, but it contained a mistake in that the special case was not handled. Another proof was presented by George Whaples in 1942, but he too didn't notice the special case. It was Shianghaw Wang who in 1948 discovered a counterexample to the original statement, upon which he identified the special case and proved the corrected statement.

Here we shall first prove the Hasse principle for mth powers, and then use it to prove the Grunwald-Wang theorem. For the former we will use Galois cohomology, and class field theory for the latter. The first section introduces group cohomology of profinite groups, though we restrict ourselves to dimensions 0 and 1 since this is all we need for the purposes of this essay. In the second section we see some applications of group cohomology in a number-theoretic context, i.e. for modules over Galois groups, in particular we treat Hilbert's theorem 90 and Kummer theory. In the third section we prove the Hasse principle for mth powers. Next we summarise the main results from local and global class field theory. In section 6 we finally prove the Grunwald-Wang theorem by reducing it to the Hasse principle for mth powers via class field theory and Pontryagin duality. In general, I made an attempt to keep the number of references to the literature to a minimum, but from time to time the reader must be willing to accept some theorems whose proof could not be given here. This applies especially to the sections on class field theory.

As for the literature, I used mainly the book "Cohomology of Number Fields" [NSW08] for the part on group cohomology and the Hasse principle. (In case the reader wonders why in this essay natural numbers are often denoted m rather than n: I was following the conventions in that book.) For the sections on class field theory, I was working with Neukirch's "Algebraic Number Theory" [Neu99], and the German edition of his "Class Field Theory" of which an English translation has just been published [Neu13]. The proofs in the section on the Grunwald-Wang theorem I worked out mostly for myself, except for one special case: The last one is taken from [NSW08].

1 Group Cohomology

In this section, we introduce the concept of modules over profinite groups and their cohomology. We start with the definition of profinite groups and prove some of their properties.

1.1 Profinite Groups

Definition 1.1. A **topological group** is a group G together with a topology on G such that the group operations

$$G \times G \longrightarrow G,\ (\sigma, \tau) \longmapsto \sigma\tau$$
$$G \longrightarrow G,\ \sigma \longmapsto \sigma^{-1}$$

are continuous.

Proposition 1.2. *In a topological group G, every open subgroup is closed. If G is compact, then every open subgroup has finite index.*

Proof. Let $U \subseteq G$ be an open subgroup. The translations $G \to G, \tau \mapsto \sigma\tau$ are homeomorphisms, therefore the left cosets σU are also open in G. Write $G = \bigcup_{\sigma \in R} \sigma U$ as a disjoint union of left cosets of U with $1 \in R$. Then the complement of U in G is

$$G \setminus U = \bigcup_{\substack{\sigma \in R \\ \sigma \neq 1}} \sigma U$$

which is open, thus U is closed.

If G is compact then the open cover $G = \bigcup_{\sigma \in R} \sigma U$ has a finite subcover, hence the index $(G : U)$ is finite. □

We assume that the reader is familiar with the definition of projective systems (see [Neu99], Def. IV.2.1). For a projective system (X_i, f_{ij}) of topological groups, the **projective limit** (or **inverse limit**)

$$\varprojlim_{i \in I} X_i = \left\{ (x_i) \in \prod_{i \in I} X_i \;\middle|\; f_{ij}(x_j) = x_i \ \forall i \leq j \right\}$$

is a closed subgroup of $\prod_{i \in I} X_i$, making it a topological group with the induced topology. If the X_i are compact then by Tychonoff's theorem the product $\prod_{i \in I} X_i$ and thus $\varprojlim_{i \in I} X_i$ are compact as well.

Proposition 1.3. *For a Hausdorff topological group G, the following are equivalent:*

(i) G is an inverse limit of finite discrete groups.

(ii) G is compact and the unit element has a neighbourhood basis consisting of open normal subgroups.

Proof. $(i) \Rightarrow (ii)$: If G is an inverse limit of finite discrete groups X_i, it is clearly compact. Furthermore, the unit element of G has a neighbourhood basis consisting of open subgroups since this is true for the product $\prod_i X_i$. Thus it suffices to show that every open subgroup U of G contains a *normal* open subgroup. Let

$$N = \{\sigma \in G \mid \sigma U = U\sigma\}$$

be the normaliser of U in G. Since $U \subseteq N$ and U has finite index, N has finite index as well. It follows that U has only finitely many conjugate subgroups. Let $V = \bigcap_{\sigma \in G} U^\sigma$ be their intersection. Then V is an open normal subgroup containing U.

$(ii) \Rightarrow (i)$**:** Suppose G is compact and the unit element has a neighbourhood basis consisting of open normal subgroups. Let N run through this neighbourhood basis. We claim that the canonical homomorphism

$$\varphi : G \longrightarrow \varprojlim_N G/N$$

is an isomorphism of topological groups for the discrete topology on the G/N . The projections $\pi_N : G \to G/N$ are clearly continuous, so φ is continuous. Since G is Hausdorff, the kernel of φ is $\bigcap_N N = \{1\}$, hence φ is injective. For the surjectivity, assume there is an element $(x_N) \in \varprojlim_N G/N$ which has no preimage in G, i.e. $\bigcap_N \pi_N^{-1}(x_N)$ is empty. By compactness, there is an empty finite subintersection, say $\bigcap_{i=1}^n \pi_{N_i}^{-1}(x_{N_i}) = \emptyset$. Let N be an open normal subgroup of G contained in the open subgroup $\bigcap_{i=1}^n N_i$. Then any lift of x_N to G is in $\bigcap_{i=1}^n \pi_{N_i}^{-1}(x_{N_i})$, contradiction! Thus, φ is surjective.

□

Definition 1.4. A Hausdorff topological group G is called **profinite** if it satisfies the equivalent conditions of proposition 1.3.

The proof of proposition 1.3 shows that for a profinite group G there is an isomorphism

$$G \cong \varprojlim_N G/N$$

where N runs over the open normal subgroups of G. Typical examples of profinite groups are the p-adic integers $\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ and Galois groups $G(K|k) = \varprojlim_L G(L|K)$, L running over the finite Galois extensions $L|k$ inside K.

1.2 G-Modules

Definition 1.5. Let G be a group. An (abstract) **G-module** is an abelian group A (written additively) together with an action of G on A by group automorphisms, i.e. a map

$$\begin{aligned} G \times A &\longrightarrow A, \\ (\sigma, a) &\longmapsto \sigma a \end{aligned}$$

such that the following holds

1. $\sigma(a + b) = \sigma a + \sigma b$,
2. $1a = a$,

3. $(\sigma\tau)a = \sigma(\tau a)$,

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

A G-action on A can be linearly extended to an action of the group ring $\mathbb{Z}[G]$ on A by defining

$$\left(\sum_{\sigma\in G} c_\sigma \sigma\right) a := \sum_{\sigma\in G} c_\sigma \sigma a$$

making A into a $\mathbb{Z}[G]$-module. Conversely, a $\mathbb{Z}[G]$-module A is naturally a G-module. Therefore G-modules are the same thing as (left) $\mathbb{Z}[G]$-modules, giving us natural notions of G-homomorphisms, G-submodules, direct sums, kernels, quotients, images, exact sequences and inverse limits of G-modules. Explicitly, a **G-submodule** of a G-module A is a subgroup $A' \subseteq A$ such that $\sigma A' \subseteq A'$ for all $\sigma \in G$. A **G-homomorphism** $f : A \to B$ between two G-modules is a homomorphism of abelian groups that commutes with the G-action, i.e.

$$f(\sigma a) = \sigma f(a) \quad \text{for all } a \in A, \sigma \in G.$$

G-modules together with G-homomorphisms form an abelian category which we will call G-Mod. The set of all G-homomorphisms $f : A \to B$ is denoted by $\mathrm{Hom}_G(A, B)$. It is a subgroup of $\mathrm{Hom}(A, B)$, the abelian group of all $\mathbb{Z}$-linear homomorphisms $A \to B$ under pointwise operations. If A and B are G-modules, then so is $\mathrm{Hom}(A, B)$ if we define the G-action by

$$(\sigma f)(a) := \sigma f(\sigma^{-1} a).$$

We can think of this as a "conjugation" action since $\sigma.f = \sigma \circ f \circ \sigma^{-1}$. Thus, $f \in \mathrm{Hom}(A, B)$ is a G-homomorphism if and only if f is fixed under the action of G on $\mathrm{Hom}(A, B)$.

We will mainly consider modules over profinite groups G. In this case G carries a topology and it is natural to require some compatibility of the group action with the profinite topology on G. Therefore we introduce the notion of discrete G-modules which are characterised by the equivalent conditions in the following lemma.

Lemma 1.6. *Let G be a profinite group and let A be an abstract G-module. Then the following conditions are equivalent:*

(i) The action $G \times A \to A$ is continuous for the discrete topology on A.

(ii) For every $a \in A$ the stabiliser $G_a := \{\sigma \in G \mid \sigma a = a\}$ is an open subgroup of G.

(iii) $A = \bigcup_U A^U$ where U runs over the open subgroups of G.

Proof. $(i) \Rightarrow (ii)$: If $G \times A \to A$ is continuous, then for $a \in A$ its preimage

$$\{(\sigma, b) \in G \times A \mid \sigma b = a\}$$

is open. The intersection with the open set $G \times \{a\}$ is $G_a \times \{a\}$. Since the projection map $G \times A \to G$ is open, it follows that G_a is open in G.

$(ii) \Rightarrow (iii)$: For $a \in A$ we have $a \in A^U$ where $U = G_a$ is an open subgroup of G by assumption.

$(iii) \Rightarrow (i)$: Let $a \in A$ and $(\sigma, b) \in G \times A$ such that $\sigma b = a$. If U is an open subgroup of G with $b \in A^U$, then $\sigma U \times \{b\}$ is an open neighbourhood of (σ, b) mapping to a. Therefore the action $G \times A \to A$ is continuous.

□

Definition 1.7. Let G be a profinite group. A **discrete G-module** is an abstract G-module A such that the equivalent conditions from lemma 1.6 are satisfied.

Note that for a finite group G with the discrete topology every abstract G-module is discrete. Since we will mainly deal with discrete G-modules, it will be understood that by G-modules we always mean discrete G-modules, unless stated otherwise. Note that submodules, quotients and direct sums of discrete G-modules are again discrete.

Examples 1.8.

- For every profinite group G, any abelian group A becomes a G-module with the **trivial action** $\sigma(a) = a$.
- For every profinite group G, the group ring $\mathbb{Z}[G]$ is a G-module with the obvious action.
- For a Galois extension $L|K$, the additive group L and the multiplicative group $L^\times$ are $G(L|K)$-modules (we will see these in section 2).

1.3 The Cohomology Groups $H^0(G, A)$ and $H^1(G, A)$

We will now define the cohomology groups $H^0(G, A)$ and $H^1(G, A)$ of a G-module A.

Definition 1.9. Let G be a finite group and A a G-module. The **fixed module** of A is

$$A^G := \{a \in A \mid \sigma a = a \text{ for all } \sigma \in G\}.$$

A^G is an abelian group which we will also call the **zeroth cohomology group**

$$H^0(G, A) := A^G.$$

It is easily verified that the association $A \mapsto A^G$ from G-modules to abelian groups is functorial, i.e. every G-homomorphism $f : A \to B$ restricts to a group homomorphism $f^* : A^G \to B^G$ such that $(1_A)^* = 1_{A^G}$ and $(gf)^* = g^* f^*$ for $f : A \to B$ and $g : B \to C$. The functor $G\text{-}\mathsf{Mod} \to \mathsf{Ab}$, $A \mapsto A^G$ is left-exact which means that an exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

of G-modules induces an exact sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G$$

of abelian groups. However, it does in general not preserve exactness at the right. For example, consider the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

of $\{\pm 1\}$-modules with the obvious action. Taking fixed modules gives the exact sequence

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z}/2\mathbb{Z}$$

but the right map is not surjective.

In situations like this (a functor between abelian categories that is left-exact but not right-exact), general homological algebra provides us (under the mild assumption that the first category has enough injectives, which is satisfied for the category of G-modules) with a way to measure the failure of right-exactness via so-called **right-derived functors**. Namely, there is a sequence of functors $H^i(G, -) : G\text{-}\mathsf{Mod} \to \mathsf{Ab}$ for $i \geq 0$ with $H^0(G, A) = A^G$, such that every exact sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

of G-modules induces an exact sequence

$$\begin{aligned}
0 \longrightarrow\ & H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, C) \\
\rightarrowtail\ & H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C) \\
\rightarrowtail\ & H^2(G, A) \longrightarrow H^2(G, B) \longrightarrow H^2(G, C) \\
\rightarrowtail\ & H^3(G, A) \longrightarrow \quad \dots
\end{aligned}$$

For the sake of concreteness, however, we will restrict ourselves to work only with H^0 and H^1 which is sufficient for the purposes of this essay. We already defined $H^0(G, A) = A^G$ above. Now we define $H^1(G, A)$ explicitly in terms of cocycles and coboundaries.

Definition 1.10. Let G be a profinite group and let A be a G-module. A **1-cochain** is a continuous map $G \to A$ (where as before A is equipped with the discrete topology). The set of all 1-cochains forms an abelian group under pointwise addition and is denoted by $C^1(G, A)$.

A **crossed homomorphism** (or **1-cocycle**) is a continuous map $f : G \to A$ such that

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau) \quad \text{for all } \sigma, \tau \in G.$$

The set of crossed homomorphisms $G \to A$ is clearly closed under addition, thus it forms a subgroup of $C^1(G, A)$. It is denoted by $Z^1(G, A)$.

A **principal crossed homomorphism** (or **1-coboundary**) is a map of the form

$$f : G \to A,\ \sigma \mapsto \sigma a - a$$

for some $a \in A$. A principal crossed homomorphism is indeed a crossed homomorphism since

$$\sigma\tau a - a = (\sigma a - a) + \sigma(\tau a - a)$$

and these maps are clearly continuous. The set of principal crossed homomorphisms is a subgroup of $Z^1(G, A)$ which we denote by $B^1(G, A)$. It is the image of the homomorphism

$$\partial : A \to Z^1(G, A),\ a \mapsto [\sigma \mapsto \sigma a - a].$$

We define the **first cohomology group** of the G-module A as

$$H^1(G, A) := \frac{\text{crossed homomorphisms}}{\text{principal crossed homomorphisms}} = \frac{\text{1-cocycles}}{\text{1-coboundaries}} = \frac{Z^1(G, A)}{B^1(G, A)}.$$

It is easily verified that the association $H^1(G, -) : G\text{-}\mathsf{Mod} \to \mathsf{Ab}$ is functorial. This follows from the fact that for a G-homomorphism $f : A \to B$ the natural map "post-composition with f" from $C^1(G, A)$ to $C^1(G, B)$ takes 1-cocycles to 1-cocycles and 1-coboundaries to 1-coboundaries.

Example 1.11. If A is a trivial G-module, then crossed homomorphisms are the same as continuous homomorphisms and all principal crossed homomorphisms are zero. Thus

$$H^1(G, A) = \mathrm{Hom}_{\mathrm{cts}}(G, A)$$

for trivial G-modules.

Theorem 1.12. *Let G be a profinite group and let*

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be an exact sequence of G-modules. Then there is an associated exact cohomology sequence

$$0 \longrightarrow A^G \longrightarrow B^G \longrightarrow C^G \xrightarrow{\delta} H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow H^1(G, C)$$

of abelian groups. The association from short exact sequences to their induced cohomology sequence is functorial in the sense that for a commutative exact diagram of G-modules

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

the induced diagram

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \xrightarrow{\delta} & H^1(G, A) & \longrightarrow & H^1(G, B) & \longrightarrow & H^1(G, C) \\ & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & A'^G & \longrightarrow & B'^G & \longrightarrow & C'^G & \xrightarrow{\delta} & H^1(G, A') & \longrightarrow & H^1(G, B') & \longrightarrow & H^1(G, C') \end{array}$$

is also commutative. The homomorphism $\delta : C^G \to H^1(G, A)$ is called the ***connecting homomorphism****.*

The existence of the cohomology sequence essentially follows from the snake lemma which we state without proof.

Theorem 1.13 (Snake lemma)**.** *Given a commutative exact diagram*

$$\begin{array}{ccccccccc} & & A & \xrightarrow{i} & B & \xrightarrow{j} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' & & \end{array}$$

of G-modules (or more general of objects in any abelian category), there is an induced exact sequence

$$\begin{array}{l} \ker(i) \longrightarrow \ker(\alpha) \longrightarrow \ker(\beta) \longrightarrow \ker(\gamma) \\ \qquad\qquad \longrightarrow \operatorname{coker}(\alpha) \longrightarrow \operatorname{coker}(\beta) \longrightarrow \operatorname{coker}(\gamma) \longrightarrow \operatorname{coker}(j') \end{array}$$

The induced exact sequence behaves functorially in the sense that given another diagram of the given shape together with compatible homomorphisms between corresponding objects, there are homomorphisms between the two induced exact sequences making the resulting squares commute.

The proof of the snake lemma can be found in any standard textbook on homological algebra which is why we omit it here. The definitions of the maps in the induced exact sequence are all obvious except for the connecting homomorphism $\delta : \ker(\gamma) \to \operatorname{coker}(\alpha)$. It is constructed as follows: Given $c \in C$ with $\gamma(c) = 0$, pick any $b \in B$ with $j(b) = c$. Then $\beta(b)$ is in the kernel of j', so there exists an $a' \in A'$ with $i'(a') = \beta(b)$. Now $\delta(c)$ is defined as the class of a' in $\operatorname{coker}(\alpha)$. It can be checked that $\delta(c)$ is independent of the choices made and that δ is a homomorphism.

Proof of theorem 1.12. Consider the commutative and exact diagram

$$\begin{array}{ccccccccc} & & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \partial_A} & & \downarrow{\scriptstyle \partial_B} & & \downarrow{\scriptstyle \partial_C} & & \\ 0 & \longrightarrow & Z^1(G, A) & \longrightarrow & Z^1(G, B) & \longrightarrow & Z^1(G, C). & & \end{array}$$

Note that

$$\ker(\partial_A) = \{a \in A \mid \sigma a - a = 0 \text{ for all } \sigma \in G\} = A^G$$

and $\operatorname{coker}(\partial_A) = H^1(G, A)$, and similarly for B and C. Thus the snake lemma gives the desired exact sequence. The functoriality of this association now follows from the functoriality of H^0 and H^1 and the assertions in the snake lemma. □

1.4 Inflation and Restriction

We have seen that the cohomology groups $H^i(G, A)$ are functorial in the second argument. Now we will look at what happens if we pass from G to subgroups and quotients.

If G is a profinite group and $H \subseteq G$ is a closed subgroup, then H is also a profinite group. Any G-module A is naturally an H-module by restricting the action from G to H. Every crossed homomorphism $G \to A$ restricts to a crossed homomorphism $H \to A$, and principal crossed homomorphism resrict to principal crossed homomorphisms. Therefore, there is a natural map

$$\begin{aligned} \mathrm{res} : H^1(G, A) &\longrightarrow H^1(H, A), \\ [f] &\longmapsto \left[f\big|_H\right], \end{aligned}$$

called **restriction**. For two closed subgroups $H_1 \subseteq H_2 \subseteq G$ the restriction map $H^1(G, A) \to H^1(H_1, A)$ is clearly equal to the composite of the restriction maps $H^1(G, A) \to H^1(H_2, A)$ and $H^1(H_2, A) \to H^1(H_1, A)$.

Now suppose $H \trianglelefteq G$ is a closed normal subgroup. Then the quotient G/H is also a profinite group, and for any G-module A the H-fixed module A^H is naturally a G/H-module with the action $(\sigma H)a := \sigma a$. Every crossed homomorphism $G/H \to A^H$ induces a crossed homomorphism $G \to A$ via the projection $\pi : G \to G/H$ and the inclusion $\iota : A^H \to A$. The resulting homomorphism $Z^1(G/H, A^H) \to Z^1(G, A)$ takes principal crossed homomorphisms to principal crossed homomorphisms, therefore it induces a homomorphism

$$\begin{aligned} \inf : H^1(G/H, A^H) &\longrightarrow H^1(G, A), \\ [f] &\longmapsto [\iota \circ f \circ \pi], \end{aligned}$$

called **inflation**. For two closed normal subgroups $H_1 \subseteq H_2 \subseteq G$ the inflation map $H^1(G/H_1, A^{H_1}) \to H^1(G, A)$ is clearly equal to the composite of the inflation maps $H^1(G/H_1, A^{H_1}) \to H^1(G/H_2, A^{H_2})$ and $H^1(G/H_2, A^{H_2}) \to H^1(G, A)$.

Theorem 1.14 (Inflation-restriction sequence)**.** *Let G be a profinite group, A a G-module and $H \trianglelefteq G$ a closed normal subgroup. Then the sequence*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\inf} H^1(G, A) \xrightarrow{\mathrm{res}} H^1(H, A)$$

is exact.

Proof. For the injectivity of the inflation map, let $x \in Z^1(G/H, A^H)$ be a cocycle such that $\inf x$ is a coboundary, say $(\inf x)(\sigma) = \sigma a - a$ for some $a \in A$. For all $\tau \in H$ we have

$$0 = (\inf x)(1) = (\inf x)(\tau) = \tau a - a,$$

therefore $a \in A^H$, and $x(\sigma H) = (\sigma H)a - a$ is a coboundary.

For the exactness in the middle, let $x \in Z^1(G/H, A^H)$ be a 1-cocycle. Then for $\tau \in H$ we have

$$(\mathrm{res} \circ \inf x)(\tau) = x(\tau H) = x(1H) = 0,$$

so $\operatorname{res} \circ \inf = 0$. Now let $x \in Z^1(G, A)$ be a cocycle such that $\operatorname{res} x$ is a coboundary, say $(\operatorname{res} x)(\tau) = \tau a - a$ for some $a \in A$ and all $\tau \in H$. The 1-cocycle $x'(\sigma) = x(\sigma) - (\sigma a - a)$ on G defines the same cohomology class as x and satisfies $x'(\tau) = 0$ for $\tau \in H$. So we have

$$x'(\sigma\tau) = x'(\sigma) + \sigma x'(\tau) = x'(\sigma) \quad \text{for } \sigma \in G, \tau \in H$$

and also

$$x'(\tau\sigma) = x'(\tau) + \tau x'(\sigma) = \tau x'(\sigma) \quad \text{for } \sigma \in G, \tau \in H.$$

Since $x'(\sigma)$ does only depend on the class of σ modulo H, we can define $y : G/H \to A$, $y(\sigma H) := x'(\sigma)$. Then in fact $y(\sigma H) \in A^H$ because for $\tau \in H$ we have

$$\tau y(\sigma H) = y(\tau\sigma H) = y(\sigma H)$$

where we used that $H \trianglelefteq G$ is a normal subgroup. Therefore, y is a 1-cocycle with $\inf y = x'$. □

A profinite group G is made up in a simple way from its (finite) quotients G/U by open normal subgroups, namely G is naturally isomorphic to the inverse limit $G \cong \varprojlim_U G/U$. If A is a discrete G-module and $U \subseteq V \subseteq G$ are open normal subgroups, the cohomology groups $H^1(G/V, A^V)$ and $H^1(G/U, A^U)$ are connected by the inflation map

$$\inf : H^1(G/V, A^V) \longhookrightarrow H^1(G/U, A^U).$$

With these maps, the cohomology groups $H^1(G/U, A^U)$ form a direct system, indexed by the open normal subgroups U of G. The following theorem makes precise the idea that $H^1(G, A)$ should be made up from the subgroups $H^1(G/U, A^U)$.

Theorem 1.15. *Let G be a profinite group and A a discrete G-module. Then there is a natural isomorphism*

$$H^1(G, A) \cong \varinjlim_U H^1(G/U, A^U)$$

where U runs over the open normal subgroups of G.

Proof. For every open normal subgroup U of G, there is an inflation map $H^1(G/U, A^U) \to H^1(G, A)$, and for two open normal subgroups $U \subseteq V \subseteq G$ the diagram

$$\begin{array}{ccc} H^1(G/V, A^V) & \xrightarrow{\quad\inf\quad} & H^1(G/U, A^U) \\ & {\scriptstyle\inf}\searrow \quad \swarrow{\scriptstyle\inf} & \\ & H^1(G, A) & \end{array}$$

commutes, thus we get a natural homomorphism

$$\varphi : \varinjlim_U H^1(G/U, A^U) \longrightarrow H^1(G, A).$$

We show that φ is an isomorphism. The injectivity follows from theorem 1.14. For the surjectivity, let $x : G \to A$ be a 1-cocycle. Since x is continuous and G is compact, the

image of x is also compact. But A is discrete, so x takes only finitely many values. Let $U \subseteq G$ be an open subgroup such that $x(G) \subseteq A^U$ and $x(U) = 0$ (this is possible since A is a discrete G-module). Since the unit element of G has a basis of neighbourhoods of open normal subgroups, we may assume that U is normal. The restriction of x to U is zero, hence by theorem 1.14 there is an element $y \in H^1(G/U, A^U)$ such that $\inf y$ is the cohomology class of x. This shows that φ is surjective. □

Now we show that taking cohomology commutes with direct products in the second argument.

Proposition 1.16. *Let G be a profinite group and let $(A_i)_{i\in I}$ be a family of discrete G-modules. Assume that G or I is finite. Then $\prod_{i\in I} A_i$ is also discrete and there is a natural isomorphism*

$$H^1\big(G, \prod_{i\in I} A_i\big) \cong \prod_{i\in I} H^1(G, A_i).$$

Proof. Write $A := \prod_{i\in I} A_i$. If G is finite, A is trivially a discrete G-module. If I is finite then the stabiliser of $(a_i) \in \prod_{i\in I} A_i$ is the intersection of the stabilisers of the a_i, therefore a finite intersection of open subgroups of G, hence itself open. Thus A is a discrete G-module.

The projections $A \to A_i$ induce maps $H^1(G, A) \to H^1(G, A_i)$ on the cohomology level which together give a homomorphism

$$\varphi : H^1\big(G, \prod_{i\in I} A_i\big) \longrightarrow \prod_{i\in I} H^1(G, A_i).$$

We show that φ is an isomorphism. For the injectivity, let $x : G \to A$ be a 1-cocycle such that the composite $G \to A \to A_i$ is a coboundary for all $i \in I$, say $x(\sigma) = (\sigma a_i - a_i)_{i\in I}$ with $a_i \in A_i$. Then $x(\sigma) = \sigma a - a$ where $a = (a_i)_{i\in I} \in A$, so x is a coboundary.

For the surjectivity, let $x_i : G \to A_i$ be 1-cocycles for $i \in I$. Then $x = (x_i)_{i\in I} : G \to A$ is a 1-cocycle whose composition with the projections $A \to A_i$ gives the x_i. □

Now let G be a finite cyclic group of order n, generated by an element σ. The **norm** of G is defined as

$$N := \sum_{\tau\in G} \tau = 1 + \sigma + \sigma^2 + \ldots + \sigma^{n-1} \in \mathbb{Z}[G].$$

Furthermore, we define

$$D := \sigma - 1 \in \mathbb{Z}[G].$$

Note that $ND = DN = 0$. For a G-module A the two elements define linear maps $D : A \to A$ and $N : A \to A$ with $DA \subseteq {}_NA$ where ${}_NA = \ker(N : A \to A)$.

Theorem 1.17. *Let $G = \langle \sigma \mid \sigma^n = 1\rangle$ be a cyclic group of order n, and let A be a G-module. Then there is an isomorphism*

$$H^1(G, A) \cong \frac{{}_NA}{DA}.$$

Proof. For a 1-cocycle $x \in Z^1(G, A)$ we have

$$0 = x(1) = x(\sigma^n) = x(\sigma) + \sigma x(\sigma^{n-1}) = \ldots = \sum_{i=0}^{n-1} \sigma^i x(\sigma) = Nx(\sigma),$$

so we have a homomorphism

$$\begin{aligned} Z^1(G, A) &\longrightarrow {}_N A, \\ x &\longmapsto x(\sigma). \end{aligned}$$

We show that it is an isomorphism. The injectivity follows from the fact that a 1-cocycle x is completely determined by $x(\sigma)$. For the surjectivity, let $a \in A$ be given with $Na = 0$. We define $x : G \to A$, $x(\sigma^k) = \sum_{i=0}^{k-1} \sigma^i a$. This is well-defined since $\sum_{i=0}^{n-1} \sigma^i a = Na = 0$, and it satisfies the cocycle property since

$$\begin{aligned} x(\sigma^k \sigma^l) &= \sum_{i=0}^{k+l-1} \sigma^i a = (1 + \sigma + \ldots \sigma^{k-1})a + \sigma^k (1 + \sigma + \ldots + \sigma^{l-1})a \\ &= x(\sigma^k) + \sigma^k x(\sigma^l). \end{aligned}$$

By definition of $\partial : A \to Z^1(G, A)$, the diagram

$$\begin{array}{ccc} A & = & A \\ \downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle D} \\ Z^1(G, A) & \longrightarrow & {}_N A \end{array}$$

is commutative which implies that our isomorphism $Z^1(G, A) \to {}_N A$ induces an isomorphism $H^1(G, A) \cong {}_N A / DA$. □

1.5 The Conjugation Action

Let G be a profinite group, $H \subseteq G$ a closed subgroup and A a discrete G-module. For $\sigma, \tau \in G$ we write $\tau^\sigma = \sigma^{-1}\tau\sigma$ and ${}^\sigma H = \sigma H \sigma^{-1}$. Every $\sigma \in G$ induces a map on the cocycle groups

$$\begin{aligned} Z^1(H, A) &\xrightarrow{\sigma_*} Z^1({}^\sigma H, A) \\ x &\longmapsto [\sigma_* x : \tau \mapsto \sigma x(\tau^\sigma)]. \end{aligned}$$

Indeed $\sigma_* x : {}^\sigma H \to A$ is a 1-cocycle since for $\tau, \rho \in {}^\sigma H$ we have

$$\begin{aligned} \sigma_* x(\tau\rho) &= \sigma x(\tau^\sigma \rho^\sigma) \\ &= \sigma(x(\tau^\sigma) + \tau^\sigma x(\rho^\sigma)) \\ &= \sigma x(\tau^\sigma) + \tau\sigma x(\rho^\sigma) \\ &= \sigma_* x(\tau) + \tau \sigma_* x(\rho). \end{aligned}$$

It is easily checked that $1_* = 1$ and $(\sigma\tau)_* = \sigma_* \tau_*$, so σ_* is an isomorphism with inverse $(\sigma^{-1})_*$. Moreover, the upper square in the following exact diagram commutes

$$\begin{array}{ccc}
A & \xrightarrow{\quad\sigma\quad} & A \\
\downarrow{\scriptstyle\partial} & & \downarrow{\scriptstyle\partial} \\
Z^1(H,A) & \xrightarrow{\sigma_*} & Z^1({}^{\sigma}H,A) \\
\downarrow & & \downarrow \\
H^1(H,A) & \dashrightarrow^{\sigma_*} & H^1({}^{\sigma}H,A) \\
\downarrow & & \downarrow \\
0 & & 0
\end{array}$$

since for $a \in A$ and $\tau \in {}^{\sigma}H$ we have

$$\begin{aligned}
(\partial \circ \sigma)(a)(\tau) &= \tau\sigma a - \sigma a, \\
(\sigma_* \circ \partial)(a)(\tau) &= \sigma(\tau^{\sigma} a - a) = \tau\sigma a - \sigma a,
\end{aligned}$$

inducing the dashed isomorphism between the cohomology groups, which we also denote by σ_*.

Now consider the case that σ normalises H (e.g. this is the case if $\sigma \in H$ or H is normal). Then ${}^{\sigma}H = H$ and G acts on $H^1(H,A)$ via

$$\begin{aligned}
G \times H^1(H,A) &\longrightarrow H^1(H,A) \\
(\sigma, x) &\longmapsto \sigma_* x.
\end{aligned}$$

We say, G acts on $H^1(H,A)$ by **conjugation**.

Proposition 1.18. *In the above situation, the action of H on $H^1(H,A)$ by conjugation is trivial.*

Proof. Let $x : H \to A$ be a 1-cocycle. For $\sigma, \tau \in H$ we have

$$\begin{aligned}
\sigma_* x(\tau) &= \sigma x(\sigma^{-1}\tau\sigma) = \sigma x(\sigma^{-1}) + x(\tau\sigma) \\
&= x(\sigma\sigma^{-1}) - x(\sigma) + x(\tau) + \tau x(\sigma) \\
&= x(\tau) + \tau x(\sigma) - x(\sigma) \\
&= x(\tau) + (\partial x(\sigma))(\tau),
\end{aligned}$$

hence $\sigma_* x$ is equal to x up to a coboundary. □

A consequence of the proposition is that σ_* commutes with restrictions, i.e. the diagram

$$\begin{array}{ccc}
H^1(G,A) & \xrightarrow{\text{res}} & H^1(H,A) \\
\| & & \downarrow{\scriptstyle\sigma_*} \\
H^1(G,A) & \xrightarrow{\text{res}} & H^1({}^{\sigma}H,A)
\end{array}$$

is commutative for all $\sigma \in G$.

Another consequence is that $\sigma_* x$ depends only the the left coset σH of σ. In particular, if H is a closed normal subgroup of G, then $H^1(H, A)$ is a G/H-module. In this case, the compatibility of σ_* and res implies the following proposition.

Proposition 1.19. *Let G be a profinite group, $H \subseteq G$ a closed normal subgroup and A a G-module. Then the restriction* $\mathrm{res} : H^1(G, A) \to H^1(H, A)$ *maps into the fixed module $H^1(H, A)^{G/H}$.* □

2 Some Galois Cohomology

We will now see some applications of group cohomology to number-theoretic questions. Here the group G will be the Galois group $G(K|k)$ of a finite or infinite Galois extension $K|k$, which is always a profinite group, namely $G(K|k) = \varprojlim_L G(L|k)$ where L runs over all finite Galois extensions $L|k$ contained in K, and the transition maps $G(L_2|k) \to G(L_1|k)$ for $L_1 \subseteq L_2$ are given by the restriction of automorphisms of L_2 to L_1. The open subgroups of $G(K|k)$ are precisely the groups $G(K|L)$ for $L|k$ a finite intermediate extension.

Let us introduce some notation. For field k we denote by $\overline{k}$ a fixed separable closure. For our purposes k will usually be a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$, so that separability is automatic and $\overline{k}$ is in fact an algebraic closure of k. The absolute Galois group of k is denoted by $G_k := G(\overline{k}|k)$. If $K|k$ is a Galois extension and A is a $G(K|k)$-module we use the abbreviation

$$H^1(K|k, A) := H^1(G(K|k), A).$$

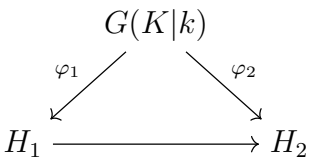
In the case where $K = \overline{k}$ we just write

$$H^1(k, A) := H^1(\overline{k}|k, A) = H^1(G(\overline{k}|k), A).$$

2.1 Galois Extensions as Homomorphisms

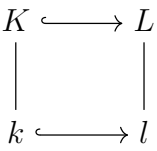
We start with a few remarks on how Galois extensions of a field k correspond to certain group homomorphisms since we will use this idea at several places in this essay. Let $K|k$ be a Galois extension. Then, given a group homomorphism $\varphi : G(K|k) \to H$ (for any group H), we form the field $E_\varphi := K^{\ker \varphi}$, the fixed field in K under the kernel of φ. This is a normal intermediate extension of $K|k$ with Galois group isormorphic to $G(K|k)/\ker\varphi \cong \operatorname{im}\varphi$. Every normal intermediate extension E of $K|k$ arises in this way from a homomorphism defined on $G(K|k)$, namely we can take the restriction map $G(K|k) \to G(E|k)$. Of course, different homomorphisms can give rise to the same field extension, even if H is fixed; for example composing $\varphi : G(K|k) \to H$ with an automorphism of H yields a φ' with $E_\varphi = E_{\varphi'}$.

The construction just described is functorial in the sense that for a commutative diagram

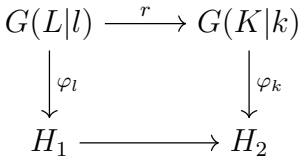


we have $\ker \varphi_1 \subseteq \ker \varphi_2$ and thus $E_{\varphi_2} \subseteq E_{\varphi_1}$.

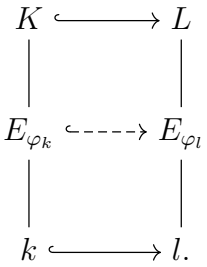
More general, for two Galois extensions $K|k$ and $L|l$ with commutative embeddings



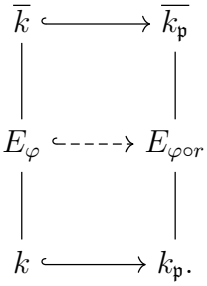
one has a restriction homomorphism $r : G(L|l) \to G(K|k)$ and every commutative square



induces a commutative diagram of field extensions



One interesting example of this situation is where k is a number field, l is the completion $k_\mathfrak{p}$ at one of its primes, $K = \overline{k}$ and $L = \overline{k_\mathfrak{p}}$. If we fix an embedding $\overline{k} \hookrightarrow \overline{k_\mathfrak{p}}$ (or equivalently, an extension of $\mathfrak{p}$ to $\overline{k}$), we get a commutative diagram as above. The restriction homomorphism r from above is then the injection $G(\overline{k_\mathfrak{p}}|k_\mathfrak{p}) \hookrightarrow G(\overline{k}|k)$. Every homomorphism $\varphi : G_k \to H$ induces a homomorphism $\varphi \circ r : G(\overline{k_\mathfrak{p}}|k_\mathfrak{p}) \to H$ and thus a commutative diagram of field extensions



From the equality $\ker(\varphi \circ r) = G(\overline{k_\mathfrak{p}}|k_\mathfrak{p}) \cap \ker \varphi$ follows that $E_{\varphi \circ r}$ is the smallest subfield of $\overline{k_\mathfrak{p}}$ containing $k_\mathfrak{p}$ and E_φ, i.e. $E_{\varphi \circ r} = E_\varphi k_\mathfrak{p}$. This is called the **localisation** of E_φ at the prime defined by the embedding $E_\varphi \hookrightarrow \overline{k} \hookrightarrow \overline{k_\mathfrak{p}}$ (see [Neu99], II.§8). If $E_\varphi|k$ is finite, then this is the same as the completion of E_φ at this prime. In general, it is the union of the completions of all finite subextensions.

2.2 Hilbert's Theorem 90

A Galois group $G(K|k)$ naturally acts on the additive group $(K, +)$ and the multiplicative group $(K^\times, \cdot)$. Both are discrete $G(K|k)$-modules since for $\alpha \in K$ the stabiliser

$$G(K|k)_a = \{\sigma \in G(K|k) \mid \sigma\alpha = \alpha\} = G(K|k(\alpha))$$

is an open subgroup of $G(K|k)$. For the cohomology of the additive group one has $H^i(K|k, K) = 0$ for all $i \geq 1$, but since we don't need this and we didn't introduce the higher cohomology groups anyway, we will not prove this here. But it is a fundamental fact that $H^1(K|k, K^\times)$ is trivial. This is known as Hilbert's theorem 90.

Theorem 2.1 (Hilbert's theorem 90)**.** *Let $K|k$ be a Galois extension. Then*

$$H^1(K|k, K^\times) = 0.$$

Proof. By theorem 1.15, $H^1(K|k, K^\times) = \varinjlim_L H^1(L|k, L^\times)$ where L ranges over the finite Galois extensions $L|k$ inside K, so we may assume that $K|k$ is finite. Put $G = G(K|k)$ and let $x : G \to K^\times$ be a 1-cocycle. Note that $K^\times$ is a $G(K|k)$-module under multiplication, whereas earlier we used an additive notation for general G-modules. Thus the cocycle property reads

$$x(\sigma\tau) = x(\sigma) \cdot \sigma x(\tau) \quad \text{for all } \sigma, \tau \in G.$$

For $c \in K^\times$ we put

$$b = \sum_{\sigma \in G} x(\sigma)\sigma(c).$$

Since the automorphisms $\sigma \in G$ are linearly independent in the vector space of functions $K^\times \to K$ (see [Lan02], Thm. VI.4.1), we can choose $c \in K^\times$ such that $b \neq 0$. For $\tau \in G$ we get

$$\tau(b) = \sum_{\sigma \in G} \tau(x(\sigma))\tau\sigma c = \sum_{\sigma \in G} x(\tau)^{-1}x(\tau\sigma)\tau\sigma c = x(\tau)^{-1} \sum_{\sigma \in G} x(\sigma)\sigma c = x(\tau)^{-1}b,$$

thus $x(\tau) = b/\tau(b)$ for all $\tau \in G$. Therefore, x is a coboundary. □

In the case where $K|k$ is a finite Galois extension with cyclic Galois group, generated by σ, say, theorem 1.17 tells us that ${}_N K^\times = DK^\times$. Here $N(x) = \prod_{\tau \in G(K|k)} \tau(x) = N_{K|k}(x)$ is the field-theoretic norm, and $D(y) = \sigma(y)/y$. Thus every element $x \in K^\times$ with $N_{K|k}(x) = 1$ is of the form $x = \sigma(y)/y$ for some $y \in K^\times$. This is the classical statement of Hilbert's theorem 90 of which the cohomological version given above is a generalisation.

2.3 Kummer Theory

Another application of Hilbert's theorem 90 is Kummer theory, i.e. the study of extensions of k that one obtains by adjoining mth roots.

Theorem 2.2. *Let k be a field and let $m \in \mathbb{N}$ be a natural number prime to the characteristic of k. Then*

$$H^1(k, \mu_m) \cong k^\times / k^{\times m}.$$

Under this isomorphism, an element $a \bmod k^{\times m}$ corresponds to the cohomology class represented by the cocycle $x : G(\overline{k}|k) \to \mu_m$, $x(\sigma) = \sigma(\sqrt[m]{\alpha})/\sqrt[m]{\alpha}$ where $\sqrt[m]{\alpha}$ is any fixed mth root of α in $\overline{k}$.

Proof. Consider the exact sequence of $G(\overline{k}|k)$-modules

$$1 \longrightarrow \mu_m \longrightarrow \overline{k}^\times \xrightarrow{m} \overline{k}^\times \longrightarrow 1$$

where the surjectivity of the right map follows from the fact that $\sqrt[m]{\alpha}$ is separable for $\alpha \in \overline{k}^\times$ as long as m is prime to the characteristic of k. We get an exact cohomology sequence

$$k^\times \xrightarrow{m} k^\times \xrightarrow{\delta} H^1(\overline{k}|k, \mu_m) \longrightarrow 0,$$

the zero on the right following from Hilbert's theorem 90. Therefore, $H^1(\overline{k}|k, \mu_m) \cong k^\times / k^{\times m}$. The given isomorphism follows from the explicit description of the connecting homomorphism $\delta : k^\times \to H^1(\overline{k}|k, \mu_m)$ which we get from applying the snake lemma to the diagram

$$\begin{array}{ccccccccc}
 & & & & & & k^\times & & \\
 & & & & & & \downarrow & & \\
 & & \mu_m & \longrightarrow & \overline{k}^\times & \xrightarrow{m} & \overline{k}^\times & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle \partial} & & \downarrow{\scriptstyle \partial} & & \\
1 & \longrightarrow & Z^1(\overline{k}|k, \mu_m) & \longrightarrow & Z^1(\overline{k}|k, \overline{k}^\times) & \xrightarrow{m} & Z^1(\overline{k}|k, \overline{k}^\times) & & \\
 & & \downarrow & & & & & & \\
 & & H^1(\overline{k}|k, \mu_m) & & & & & &
\end{array}$$

□

In the case where k contains the mth roots of unity, G_k acts trivially on μ_m and hence $H^1(k, \mu_m) = \mathrm{Hom}_{\mathrm{cts}}(G_k, \mu_m)$. The isomorphism $\mathrm{Hom}_{\mathrm{cts}}(G_k, \mu_m) \cong k^\times / k^{\times m}$ gives a one-to-one correspondence between the finite subgroups of $\mathrm{Hom}_{\mathrm{cts}}(G_k, \mu_m)$ and the finite subgroups of $k^\times / k^{\times m}$. One can show that the finite subgroups of $\mathrm{Hom}_{\mathrm{cts}}(G_k, \mu_m)$ are precisely the groups $\mathrm{Hom}(G(L|k), \mu_m)$ where $L|k$ is a finite abelian extension of exponent m. Thus one obtains classical Kummer theory, i.e. the one-to-one correspondence

$$\left\{ \begin{array}{c} \text{finite abelian extensions} \\ L|k \text{ of exponent } m \end{array} \right\} \rightleftarrows \left\{ \begin{array}{c} \text{finite subgroups of} \\ k^\times/k^{\times m} \end{array} \right\}$$
$$L \longmapsto k^\times \cap L^{\times m} \bmod k^{\times m}$$
$$k(\sqrt[m]{\Delta}) \longleftarrow\!\shortmid \Delta.$$

3 The Hasse Principle for mth Powers

In this section we will deal with a local-to-global principle for mth powers. Namely, we will show that an element of a number field k that is an mth power in the completions $k_\mathfrak{p}$ for almost all primes $\mathfrak{p}$ of k, is in fact already an mth power in k (except in one very special case involving the prime 2). A local-to-global principle of this kind is also called **Hasse principle** after the classical theorem of Hasse-Minkowski, which says that a quadratic polynomial equation over k that has a solution in all completions $k_\mathfrak{p}$ of k already has a solution in k.

Most results in this section hold for general global fields, i.e. number fields and fields of the form $\mathbb{F}_q(t)$, but for simplicity we will only consider the number field case to avoid technicalities araising from working in positive characteristic that otherwise would have to be treated separately at some places. In some of the lemmas k is allowed to be any field of characteristic zero, but we always have the number field case in mind.

3.1 The Localisation Homomorphism

So let k be a number field, and just as before denote by $\overline{k}$ a fixed algebraic closure of k, and by $G_k = G(\overline{k}|k)$ the absolute Galois group of k. For every prime $\mathfrak{p}$ of k we fix an embedding $i_\mathfrak{p} : \overline{k} \hookrightarrow \overline{k_\mathfrak{p}}$. This is equivalent to fixing an extension of $|\cdot|_\mathfrak{p}$ to $\overline{k}$ by setting $|x|_\mathfrak{p} := |i_\mathfrak{p}(x)|_\mathfrak{p}$, i.e. we fix a prime of $\overline{k}$ lying over $\mathfrak{p}$. We consider all algebraic extensions $K|k$ as embedded into $\overline{k}$, so that we have a distinguished prime $\mathfrak{P}$ of K lying over $\mathfrak{p}$. We agree on the notation

$$K_\mathfrak{p} := i_\mathfrak{p}(K)k_\mathfrak{p};$$

this is the localisation of K at the distinguished prime $\mathfrak{P}$, which for finite extensions $K|k$ coincides with the completion of K at $\mathfrak{P}$ (see [Neu99], II.§8). Similarly, if $K|k$ is Galois, we write $G_\mathfrak{p}(K|k)$ for the decomposition group $G_\mathfrak{P}(K|k) \subseteq G(K|k)$. Recall that $G(K_\mathfrak{p}|k_\mathfrak{p})$ is isomorphic to $G_\mathfrak{p}(K|k)$ via the restriction homomorphism (see [Neu99], II.§9). We usually identify the two groups and use $G_\mathfrak{p}(K|k)$ and $G(K_\mathfrak{p}|k_\mathfrak{p})$ interchangeably. In particular we view $G(K_\mathfrak{p}|k_\mathfrak{p})$ as a subgroup of $G(K|k)$. Thereby, we obtain for every $G(K|k)$-module A a restriction homomorphism

$$\mathrm{res}_\mathfrak{p} : H^1(K|k, A) \longrightarrow H^1(K_\mathfrak{p}|k_\mathfrak{p}, A).$$

One might think that this definition is non-canonical due to the choice of the embedding $i_\mathfrak{p} : \overline{k} \hookrightarrow \overline{k_\mathfrak{p}}$ and thus of the prime $\mathfrak{P}$ of K lying over $\mathfrak{p}$, but it is in fact independent

of these choices up to canonical isomorphism. Indeed, any other prime of K lying over $\mathfrak{p}$ is of the form $\sigma\mathfrak{P}$ for some $\sigma \in G(K|k)$, and σ is unique up to multiplication from the right with an element of $G_{\mathfrak{P}}(K|k)$. The decomposition groups are then conjugated by σ:

$$G_{\sigma\mathfrak{P}}(K|k) = \sigma G_{\mathfrak{P}}(K|k)\sigma^{-1},$$

so we are in the situation treated earlier in the section on the conjugation action. Thus we have an isomorphism

$$H^1(K_{\mathfrak{P}}|k_{\mathfrak{p}}, A) \xrightarrow{\sigma_*} H^1(K_{\sigma\mathfrak{P}}|k_{\mathfrak{p}}, A).$$

This isomorphism does not depend on the choice of σ since the conjugation action of $G_{\mathfrak{P}}(K|k)$ on the left group is trivial. We have a commutative diagram

$$\begin{array}{ccc} H^1(K|k, A) & \xrightarrow{\mathrm{res}_{\mathfrak{P}}} & H^1(K_{\mathfrak{P}}|k_{\mathfrak{p}}, A) \\ \| & & \downarrow{\scriptstyle \sigma^*} \\ H^1(K|k, A) & \xrightarrow{\mathrm{res}_{\sigma\mathfrak{P}}} & H^1(K_{\sigma\mathfrak{P}}|k_{\mathfrak{p}}, A) \end{array}$$

with a canonical isomorphism at the right, justifying the notation defined above where we fixed a distinguished prime $\mathfrak{P}$ of K lying above $\mathfrak{p}$.

Now let T be a set of primes of k. For every $\mathfrak{p} \in T$ we have a restriction homomorphism

$$H^1(K|k, A) \xrightarrow{\mathrm{res}_{\mathfrak{p}}} H^1(K_{\mathfrak{p}}|k_{\mathfrak{p}}, A)$$

and putting all of these together we obtain a localisation homomorphism

$$H^1(K|k, A) \xrightarrow{\mathrm{res}} \prod_{\mathfrak{p}\in T} H^1(K_{\mathfrak{p}}|k_{\mathfrak{p}}, A).$$

The idea of a Hasse principle for the $G(K|k)$-module A is that if T is big enough, then knowing all the local restrictions $\mathrm{res}_{\mathfrak{p}}\, x \in H^1(K_{\mathfrak{p}}|k_{\mathfrak{p}}, A)$ for $\mathfrak{p} \in T$ is enough to recover the the global cohomology class $x \in H^1(K|k, A)$, i.e. the localisation homomorphism is injective. We are thus interested in the vanishing of its kernel which we denote by

$$Ш^1(K|k, T, A) := \ker\left(H^1(K|k, A) \longrightarrow \prod_{\mathfrak{p}\in T} H^1(K_{\mathfrak{p}}|k_{\mathfrak{p}}, A)\right).$$

We will in particular consider the case $K = \overline{k}$ where we note that $(\overline{k})_{\mathfrak{p}} = \overline{k_{\mathfrak{p}}}$, i.e. $i_{\mathfrak{p}}(\overline{k})k_{\mathfrak{p}} = \overline{k_{\mathfrak{p}}}$. This is a consequence of Krasner's lemma (see [NSW08], Prop. 8.1.5). So, if A is a G_k-module, we have for every prime $\mathfrak{p}$ of k a restriction map

$$H^1(k, A) \xrightarrow{\mathrm{res}_{\mathfrak{p}}} H^1(k_{\mathfrak{p}}, A).$$

As for cohomology groups we use the notation $Ш^1(k, T, A) := Ш^1(\overline{k}|k, T, A)$, i.e.

$$Ш^1(k, T, A) = \ker\left(H^1(k, A) \longrightarrow \prod_{\mathfrak{p}\in T} H^1(k_{\mathfrak{p}}, A)\right).$$

In this section we will prove a Hasse principle for the G_k-module $A = \mu_m$ where by Kummer theory (theorem 2.2) the homomorphism in question becomes

$$k^\times/k^{\times m} \longrightarrow \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times m}.$$

The injectivity of this map (i.e. the vanishing of $Ш^1(k, T, \mu_m)$) is equivalent to the assertion that a number $\alpha \in k^\times$ which is an mth power in $k_\mathfrak{p}^\times$ for all $\mathfrak{p} \in T$ is already an mth power globally. We show that this holds if T omits only finitely many primes and we are not in a special case involving the prime 2. First, we need some lemmas.

Lemma 3.1. *Let T be a set of primes of k, let $K|k$ be a Galois extension and A and B two $G(K|k)$-modules. Then*

$$Ш^1(K|k, T, A \times B) \cong Ш^1(K|k, T, A) \times Ш^1(K|k, T, B).$$

Proof. Using proposition 1.16, the projections $A \times B \to A$ and $A \times B \to B$ induce a commutative diagram

$$\begin{array}{ccc} H^1(K|k, A \times B) & \xrightarrow{\text{res}} & \prod_T H^1(K_\mathfrak{p}|k_\mathfrak{p}, A \times B) \\ \wr\downarrow & & \wr\downarrow \\ H^1(K|k, A) \times H^1(K|k, B) & \xrightarrow{\text{res}} & \prod_T H^1(K_\mathfrak{p}|k_\mathfrak{p}, A) \times \prod_T H^1(K_\mathfrak{p}|k_\mathfrak{p}, B). \end{array}$$

This induces an isomorphism between the kernel of the upper map, which by definition is $Ш^1(K|k, T, A \times B)$, and the kernel of the lower map, which is $Ш^1(K|k, T, A) \times Ш^1(K|k, T, B)$. □

3.2 The Cohomology of $(\mathbb{Z}/p^m\mathbb{Z})^\times$

Lemma 3.2. *Let p be a prime, m a natural number and $\alpha = 1 + p^s u \in U^s$ a principal unit in $\mathbb{Z}_p$, $s \geq 1$, $u \in (\mathbb{Z}_p)^\times$. If p is odd or $s \geq 2$, then $v_p(\alpha^m - 1) = s + v_p(m)$.*

Proof. We have

$$\alpha^m - 1 = (1 + p^s u)^m - 1 = mp^s u + \binom{m}{2} p^{2s} u^2 + \ldots + p^{ms} u^m$$

and the first summand has valuation $v_p(mp^s u) = s + v_p(m)$. Thus it is enough to show

$$v_p\left(\binom{m}{k} p^{ks} u^k\right) > s + v_p(m) \quad \text{for } 2 \leq k \leq m.$$

We use the well-known fact

$$v_p(k!) = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \ldots < \sum_{i=1}^{\infty} \frac{k}{p^i} = \frac{k}{p-1}$$

which implies $v_p(k!) \leq \frac{k-1}{p-1}$ since $(p-1)v_p(k!)$ is an integer. We get

$$v_p\left(\binom{m}{k}p^{ks}u^k\right) \geq v_p(m) + ks - \frac{k-1}{p-1} = v_p(m) + s + (k-1)\left(s - \frac{1}{p-1}\right)$$

which is $> v_p(m) + s$ if $k \geq 2$ and $p > 2$ or $s \geq 2$. □

Lemma 3.3. *Let $m \geq 2$ be a natural number. Denote by U^i the image of $1 + 2^i\mathbb{Z}_2$ in $(\mathbb{Z}/2^m\mathbb{Z})^\times$ under the projection $\mathbb{Z}_2 \to \mathbb{Z}/2^m\mathbb{Z}$. Then the subgroups of $(\mathbb{Z}/2^m\mathbb{Z})^\times = \langle -1\rangle \times U^2$ are precisely the groups*

(a) $G = \langle -1\rangle \times \langle \alpha\rangle$ with $\alpha \in U^2$,

(b) $G = \langle \alpha\rangle$ with $\alpha \in U^2$,

(c) $G = \langle \alpha\rangle$ with $-\alpha \in U^2$, $-\alpha \neq 1$.

Proof. Let G be a subgroup of $(\mathbb{Z}/2^m\mathbb{Z})^\times$. If G is cyclic, either $G = \langle -1\rangle$ or G is of the form (b) or (c). If G is non-cyclic, G is a direct sum of at least two cyclic groups whose order is a power of 2, so G contains at least four elements of order dividing 2. But $(\mathbb{Z}/2^m\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{m-2}\mathbb{Z}$ contains at most four elements of order dividing 2. So G contains all of them, in particular $-1 \in G$. Thus G is of the form (a). □

Lemma 3.4. *Let p be a prime number, $m \geq 1$ a natural number, $G \subseteq (\mathbb{Z}/p^m\mathbb{Z})^\times$ a subgroup, and let A be the G-module $\mathbb{Z}/p^m\mathbb{Z}$ on which G acts by multiplication. Then*

$$H^1(G, A) = 0$$

unless $p = 2$, $m \geq 2$ and $-1 \in G$ in which case

$$H^1(G, A) \cong \mathbb{Z}/2\mathbb{Z}.$$

Proof. The case $G = 1$ is trivial, so assume $G \neq 1$. First consider the case where p is odd. In this case $(\mathbb{Z}/p^m\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{m-1}\mathbb{Z}$ is cyclic, so $G = \langle\alpha\rangle$ for some $\alpha \in (\mathbb{Z}/p^m\mathbb{Z})^\times$. By theorem 1.17 it suffices to show $DA = {}_NA$ where $D = \alpha - 1$ and $N = 1 + \alpha + \ldots + \alpha^{\mathrm{ord}(\alpha)-1}$. If $\alpha - 1$ is a unit, we have $A = DA \subseteq {}_NA \subseteq A$, hence $DA = {}_NA$. Otherwise we can write $\alpha = 1 + p^s u$ with $u \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ and $1 \leq s < m$. Then we have $DA = (\alpha - 1)A = p^sA$. By lemma 3.2, α has order p^{m-s}. Writing α also for a preimage of α in $\mathbb{Z}_p$, we have

$$\begin{aligned} v_p(1 + \alpha + \ldots + \alpha^{p^{m-s}-1}) &= v_p(\alpha^{p^{m-s}} - 1) - v_p(\alpha - 1) \\ &= (s + (m-s)) - s = m - s \end{aligned}$$

and therefore

$${}_NA = \left\{a \in A \;\middle|\; p^{m-s}a = 0\right\} = p^sA = DA.$$

Now consider the case $p = 2$. We may assume $m \geq 2$, otherwise $G = 1$. By lemma 3.3 G is of the form (a), (b) or (c) described above. In case (b) the same proof as for odd p using lemma 3.2 applies.

Case (c): Write $\alpha = -1 + 2^s u$ with $u \in (\mathbb{Z}/2^m\mathbb{Z})^\times$ and $2 \leq s < m$. Then we have $DA = (\alpha - 1)A = (-2 - 2^s u)A = 2A$. Since the order of G is even, α has the same order as $-\alpha = 1 - 2^s u$, which is 2^{m-s} by lemma 3.2. Now, again using the same letter α for a preimage in $\mathbb{Z}_2$,

$$\begin{aligned} v_2(1 + \alpha + \ldots + \alpha^{2^{m-s}-1}) &= v_2(\alpha^{2^{m-s}} - 1) - v_2(\alpha - 1) \\ &= v_2((-\alpha)^{2^{m-s}} - 1) - v_2(\alpha - 1) \\ &= (s + (m - s)) - 1 = m - 1. \end{aligned}$$

Hence

$$ {}_N A = \left\{ a \in A \;\middle|\; 2^{m-1} a = 0 \right\} = 2A = DA. $$

Case (a): Assume $G = \langle -1 \rangle \times \langle \alpha \rangle$ with $\alpha \in U^2$. This is the special case, so we have to show $H^1(G, A) \cong \mathbb{Z}/2\mathbb{Z}$. First consider the case $\alpha = 1$, i.e. $G = \langle -1 \rangle$. Then $D = -2$ and $N = 0$, so $DA = 2A$ and ${}_N A = A$, hence $H^1(G, A) \cong A/2A \cong \mathbb{Z}/2\mathbb{Z}$.

Now suppose $G = \langle -1 \rangle \times \langle \alpha \rangle$ with $\alpha \in U^2$, $\alpha \neq 1$. There is an inflation-restriction sequence

$$ 0 \longrightarrow H^1(\langle -1 \rangle, A^{\langle \alpha \rangle}) \xrightarrow{\text{inf}} H^1(G, A) \xrightarrow{\text{res}} H^1(\langle \alpha \rangle, A) $$

where the right cohomology group is trivial by case (b). Thus $H^1(G, A) \cong H^1(\langle -1 \rangle, A^{\langle \alpha \rangle})$. Writing $\alpha = 1 + 2^s u$ as above, $2 \leq s < m$, we have $A^{\langle \alpha \rangle} = \{a \in A \mid (\alpha - 1)a = 0\} = 2^{m-s} A \cong \mathbb{Z}/2^s\mathbb{Z}$ and are reduced to the case $\alpha = 1$ which we treated above. □

3.3 The Special Case

For a field k and a natural number m which is prime to $\mathrm{char}(k)$ the cyclotomic extension $k(\mu_m)|k$ is a finite Galois extension generated by any primitive mth root of unity ζ. For every automorphism $\sigma \in G(k(\mu_m)|k)$, the conjugate $\sigma(\zeta)$ of ζ is of the form ζ^i with $\gcd(m, i) = 1$, and σ is completely determined by i. Thus we have an injective homomorphism

$$\begin{aligned} \chi_{\text{cycl}} : G(k(\mu_m)|k) &\hookrightarrow (\mathbb{Z}/m\mathbb{Z})^\times \\ \sigma &\longmapsto i \text{ such that } \sigma(\zeta) = \zeta^i, \end{aligned}$$

which is called the **cyclotomic character**.

Definition 3.5. Let k be a field with $\mathrm{char}\, k = 0$ and $m = 2^r m'$, $m' odd$, a natural number. We say that we are in the **special case** (k, m) if $r \geq 2$ and -1 is in the image of the cyclotomic character $\chi_{\text{cycl}} : G(k(\mu_{2^r})|k) \to (\mathbb{Z}/2^r\mathbb{Z})^\times$.

Example 3.6. If $k = \mathbb{Q}$, we are in the special case $(\mathbb{Q}, 2^r)$ for all $r \geq 2$. In this case the cyclotomic character is an isomorphism $G(\mathbb{Q}(\mu_{2^r})|\mathbb{Q}) \cong (\mathbb{Z}/2^r\mathbb{Z})^\times$, depending on a choice of a primitive root of unity ζ. The automorphism defined by $\zeta \mapsto \zeta^{-1}$ is complex conjugation.

An immediate consequence of lemma 3.4 is the following proposition.

Proposition 3.7. *Let k be a field with* $\operatorname{char} k = 0$*, let p be a prime number and $r \in \mathbb{N}$. Then*

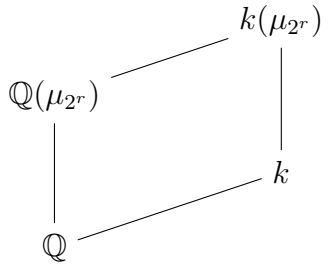
$$H^1(k(\mu_{p^r})|k, \mu_{p^r}) = 0,$$

unless $p = 2$ and we are in the special case $(k, 2^r)$. In this case

$$H^1(k(\mu_{2^r})|k, \mu_{2^r}) \cong \mathbb{Z}/2\mathbb{Z}.$$

□

Let us describe the special case more explicitly. For a field k with $\operatorname{char} k = 0$ and $r \in \mathbb{N}$, the extension $k(\mu_{2^r})|k$ is a translation of $\mathbb{Q}(\mu_{2^r})|\mathbb{Q}$ as shown in the following diagram:



We have a restriction homomorphism $G(k(\mu_{2^r})|k) \to G(\mathbb{Q}(\mu_{2^r})|\mathbb{Q})$ which is injective since an automorphism $\sigma \in G(k(\mu_{2^r})|k)$ is completely determined by what it does on μ_{2^r}. The image of this homomorphism corresponds to a subfield E of $\mathbb{Q}(\mu_{2^r})$, namely E is the fixed field

$$\begin{aligned} E &= \left\{ x \in \mathbb{Q}(\mu_{2^r}) \;\middle|\; \sigma\big|_{\mathbb{Q}(\mu_{2^r})}(x) = x \text{ for all } \sigma \in G(k(\mu_{2^r})|k) \right\} \\ &= \{ x \in \mathbb{Q}(\mu_{2^r}) \mid \sigma(x) = x \text{ for all } \sigma \in G(k(\mu_{2^r})|k) \} \\ &= \mathbb{Q}(\mu_{2^r}) \cap k. \end{aligned}$$

So we have an isomorphism

$$G(K(\mu_{2^r})|k) \cong G(\mathbb{Q}(\mu_{2^r})|k \cap \mathbb{Q}(\mu_{2^r})).$$

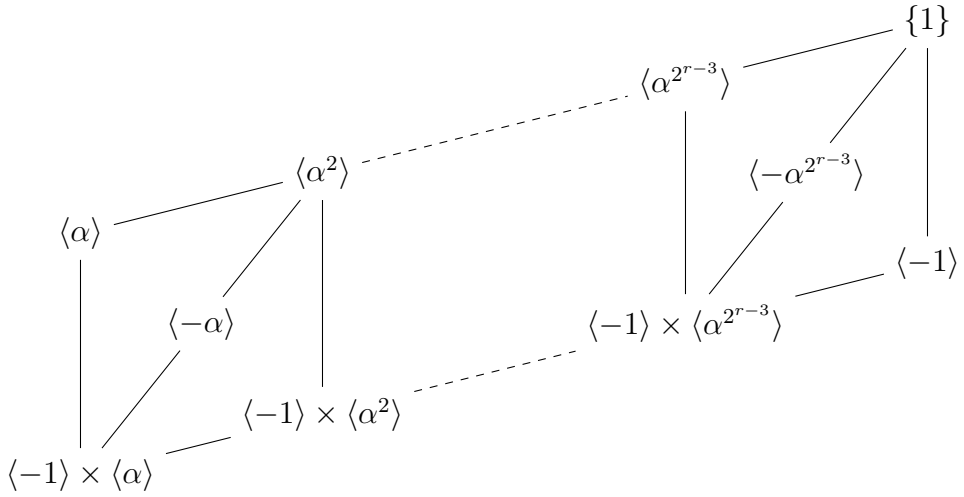
The cyclotomic character $\chi_{\text{cycl}} : G(k(\mu_{2^r})|k) \to (\mathbb{Z}/2^r\mathbb{Z})^\times$ is the composite homomorphism

$$G(K(\mu_{2^r})|k) \xrightarrow{\sim} G(\mathbb{Q}(\mu_{2^r})|k \cap \mathbb{Q}(\mu_{2^r})) \hookrightarrow G(\mathbb{Q}(\mu_{2^r})|\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/2^r\mathbb{Z})^\times.$$

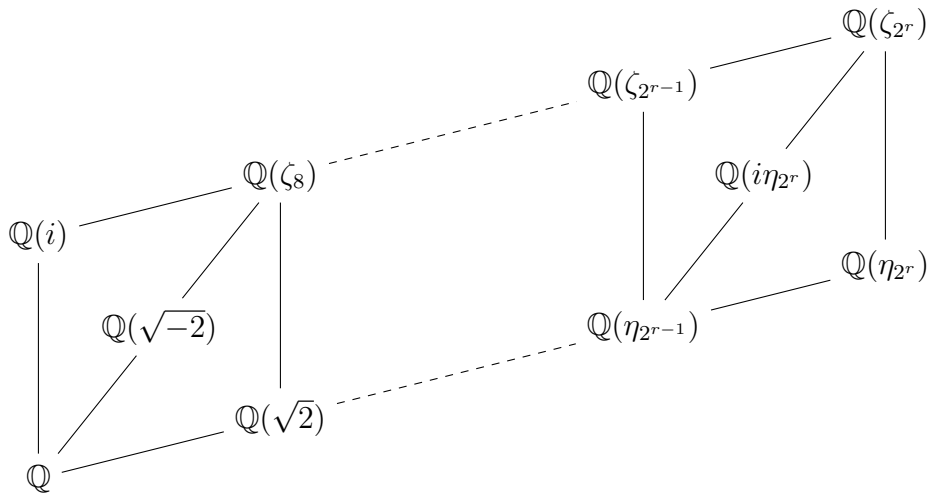
If $r \geq 2$, the element $-1 \in (\mathbb{Z}/2^r\mathbb{Z})^\times$ corresponds to complex conjugation in $G(\mathbb{Q}(\mu_{2^r})|\mathbb{Q})$ and fixes $k \cap \mathbb{Q}(\mu_{2^r})$ if and only if this field is real. This proves the following proposition:

Proposition 3.8. *Let k be a field with* $\operatorname{char} k = 0$ *and $m = 2^r m'$, m' odd, a natural number. Then we are in the special case (k, m) if and only if $r \geq 2$ and $k \cap \mathbb{Q}(\mu_{2^r})$ is real.* □

Let us look at the subfields of $\mathbb{Q}(\mu_{2^r})$. They correspond bijectively to the subgroups of $G(\mathbb{Q}(\mu_{2^r})|\mathbb{Q}) \cong (\mathbb{Z}/2^r\mathbb{Z})^\times$ which we already listed in lemma 3.3. Writing $(\mathbb{Z}/2^r\mathbb{Z})^\times = \langle -1\rangle \times \langle \alpha\rangle$ (one can choose $\alpha = 5$), the subgroup lattice looks like this (note that inclusions are reversed to correspond with the field diagram):



The corresponding subfield lattice of $\mathbb{Q}(\mu_{2^r})$ is the following, denoting by ζ_n a primitive nth root of unity and setting $\eta_n = \zeta_n + \zeta_n^{-1}$:



Note that the real fields are the ones in the bottom row, corresponding to the subgroups of $(\mathbb{Z}/2^r\mathbb{Z})^\times$ containing -1. For a field k with $\operatorname{char} k = 0$, the isomorphism $G(k(\mu_{2^r})|k) \cong G(\mathbb{Q}(\mu_{2^r})|k \cap \mathbb{Q}(\mu_{2^r}))$ implies that the intermediate fields of $k(\mu_{2^r})|k$ correspond bijectively to the intermediate fields of $\mathbb{Q}(\mu_{2^r})|k \cap \mathbb{Q}(\mu_{2^r})$. The bijection is given by intersecting with $\mathbb{Q}(\mu_{2^r})$ in one direction, and taking the composite with k in

the other:

$$\left\{ \begin{array}{c} \text{intermediate fields} \\ \mathbb{Q}(\mu_{2^r}) \cap k \subseteq E \subseteq \mathbb{Q}(\mu_{2^r}) \end{array} \right\} \rightleftarrows \left\{ \begin{array}{c} \text{intermediate fields} \\ k \subseteq k' \subseteq k(\mu_{2^r}) \end{array} \right\}$$
$$E \longmapsto Ek$$
$$k' \cap \mathbb{Q}(\mu_{2^r}) \longmapsfrom k'$$

We will need this later in a proof.

Without proof we state the following theorem which is a consequence of Chebotarev's density theorem (see [Neu99], Cor. VII.13.7).

Theorem 3.9. *Let $K|k$ be a finite extension of number fields. If almost all primes of k split completely in $K|k$, then in fact $K = k$.*

Definition 3.10. Let k be a number field, $m = 2^r m'$, m' odd, a natural number, and T a set of primes of k. We say that we are in the **special case** (k, m, T) if we are in the special case (k, m) and all primes $\mathfrak{p} \in T$ decompose in $k(\mu_{2^r})|k$.

Lemma 3.11. *Let k be a number field and T a set of primes of k, containing all but finitely many primes. If $k(\mu_{2^r})|k$ is cyclic, then we are not in the special case $(k, 2^r, T)$.*

Proof. Consider $G = G(k(\mu_{2^r})|k)$ as a subgroup of $(\mathbb{Z}/2^r\mathbb{Z})^\times$ via the cyclotomic character $\chi_{\text{cycl}} : G \hookrightarrow (\mathbb{Z}/2^r\mathbb{Z})^\times$. If we are in the special case $(k, 2^r)$, then $-1 \in G$, and since G is cyclic, we have $G = \{\pm 1\}$ and thus $[k(\mu_{2^r}) : k] = 2$. In view of theorem 3.9 there must be a prime $\mathfrak{p} \in T$ that is not completely split in $k(\mu_{2^r})|k$. Then $\mathfrak{p}$ does not decompose, so we are not in the special case $(k, 2^r, T)$. □

Proposition 3.12. *Let k be a number field, T a set of primes of k containing all but finitely many primes, and $m \in \mathbb{N}$ a natural number. Then we are in the special case (k, m, T) if and only if*

- *$m = 2^r m'$ with m' odd and $r \geq 3$,*
- *$k(\mu_{2^r})|k$ is not cyclic, and*
- *all primes $\mathfrak{p} \in T$ dividing 2 decompose in $k(\mu_{2^r})|k$*

Proof. Suppose we are in the special case (k, m, T). Writing $m = 2^r m'$ with m' odd, all primes $\mathfrak{p} \in T$ decompose in $k(\mu_{2^r})|k$ and lemma 3.11 implies that $k(\mu_{2^r})|k$ is not cyclic, in particular $r \geq 3$.

Now suppose that $r \geq 3$, $k(\mu_{2^r})|k$ is not cyclic and all primes $\mathfrak{p} \in T$ dividing 2 decompose in $k(\mu_{2^r})|k$. A subgroup of $(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \{\pm 1\} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$ which does not contain -1 is cyclic, so we must have $-1 \in G$. A finite prime $\mathfrak{p} \in T$ not dividing 2 is unramified in $k(\mu_{2^r})|k$, so has a cyclic decomposition group which then must be a proper subgroup of G. So $\mathfrak{p}$ is decomposed in $k(\mu_{2^r})|k$. The same holds for archimedean primes in T. Therefore, all primes in T decompose and we are in the special case (k, m, T). □

Example 3.13. Let $k = \mathbb{Q}$ and let T be the set of all prime numbers except 2. Then we are in the special case $(\mathbb{Q}, 2^r, T)$ for all $r \geq 3$. This follows from proposition 3.12. Alternatively, we can argue as follows:

To show that all odd primes decompose in $\mathbb{Q}(\mu_{2^r})$ it suffices to show this for $r = 3$. The minimal polynomial of ζ_8 is the cyclotomic polynomial $\Phi_8 = X^4 + 1$. It has the factorisations

$$\begin{aligned} X^4 + 1 &= (X^2 - \sqrt{-1})(X^2 + \sqrt{-1}) \\ &= (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1) \\ &= (X^2 + \sqrt{-2}X - 1)(X^2 - \sqrt{-2}X - 1). \end{aligned}$$

The multiplicativity of the Legendre symbol implies that for every odd prime p at least one of $-1, 2, -2$ is a square mod p. Therefore, by Hensel's lemma $\mathbb{Q}_p$ contains at least one of $\sqrt{-1}, \sqrt{2}, \sqrt{-2}$ for every odd prime p. So $X^4 + 1$ splits over all $\mathbb{Q}_p$ and thus all odd primes decompose in $\mathbb{Q}(\zeta_8)$.

3.4 The Hasse Principle for mth Powers

Lemma 3.14. *Let k be a number field, T a set of primes of k containing all but finitely many primes and let A be a trivial G_k-module. Then*

$$Ш^1(k, T, A) = 0.$$

Proof. We have to show that the homomorphism

$$\mathrm{Hom}_{\mathrm{cts}}(G_k, A) \longrightarrow \prod_{\mathfrak{p} \in T} \mathrm{Hom}_{\mathrm{cts}}(G_{k_\mathfrak{p}}, A)$$

is injective. Let $\varphi : G_k \to A$ be in the kernel, and let K be the fixed field K of $\ker(\varphi)$. Then $K|k$ is a Galois extension with Galois group $G/\ker(\varphi)$ which is finite since $\ker(\varphi)$ is open. The composite maps $G_{k_\mathfrak{p}} \hookrightarrow G_k \to A$ for $\mathfrak{p} \in T$ are all zero, so $G(K_\mathfrak{p}|k_\mathfrak{p}) = 1$ for all $\mathfrak{p} \in T$. Therefore, $K|k$ is completely decomposed at T. Now theorem 3.9 implies $K = k$, hence $\varphi = 0$. □

Theorem 3.15. *Let k be a number field, T a set of primes of k containing all but finitely many primes, and $m \in \mathbb{N}$ a natural number. Then*

$$Ш^1(k, T, \mu_m) = 0$$

except we are in the special case (k, m, T) where

$$Ш^1(k, T, \mu_m) \cong \mathbb{Z}/2\mathbb{Z}.$$

Proof. By lemma 3.1 we may assume $m = p^r$. Let $K = k(\mu_{p^r})$, so that μ_{p^r} is a trivial $G(\overline{k}|K)$-module. The set $T(K)$ of all primes of K lying over a prime $\mathfrak{p} \in T$ contains all but finitely many primes of K. We have a commutative and exact diagram

$$\begin{array}{ccccc}
0 & \longrightarrow & Ш^1(\overline{k}|K, T(K), \mu_{p^r}) & \longrightarrow & H^1(\overline{k}|K, \mu_{p^r}) \longrightarrow \prod_{T(K)} H^1(K_\mathfrak{p}, \mu_{p^r}) \\
 & & \uparrow{\scriptstyle \text{res}} & & \uparrow{\scriptstyle \text{res}} \qquad \uparrow{\scriptstyle \text{res}} \\
0 & \longrightarrow & Ш^1(\overline{k}|k, T, \mu_{p^r}) & \longrightarrow & H^1(\overline{k}|k, \mu_{p^r}) \longrightarrow \prod_{T} H^1(k_\mathfrak{p}, \mu_{p^r}) \\
 & & \uparrow{\scriptstyle \text{inf}} & & \uparrow{\scriptstyle \text{inf}} \qquad \uparrow{\scriptstyle \text{inf}} \\
0 & \longrightarrow & Ш^1(K|k, T, \mu_{p^r}) & \longrightarrow & H^1(K|k, \mu_{p^r}) \longrightarrow \prod_{T} H^1(K_\mathfrak{p}|k_\mathfrak{p}, \mu_{p^r}) \\
 & & \uparrow & & \uparrow \qquad \uparrow \\
 & & 0 & & 0 \qquad 0
\end{array}$$

By lemma 3.14 the group $Ш^1(\overline{k}|K, T, \mu_{p^r})$ is trivial, hence

$$Ш^1(\overline{k}|k, T, \mu_{p^r}) \cong Ш^1(K|k, T, \mu_{p^r}).$$

If we are not in the special case (k, p^r) then by proposition 3.7 we have $H^1(K|k, \mu_{p^r}) = 0$ and thus $Ш^1(K|k, T, A) = 0$. If $p = 2$ and there is a prime $\mathfrak{p} \in T$ that does not decompose in $K = k(\mu_{2^r})$ then $G(K|k) = G(K_\mathfrak{p}|k_\mathfrak{p})$ and therefore $Ш^1(K|k, T, \mu_{2^r}) = 0$ as well.

So assume we are in the special case $(k, 2^r)$ and all primes $\mathfrak{p} \in T$ decompose in K. We have to show $Ш^1(K|k, \mu_{2^r}) \cong \mathbb{Z}/2\mathbb{Z}$. Since $H^1(K|k, \mu_{2^r}) \cong \mathbb{Z}/2\mathbb{Z}$ by proposition 3.7, this is equivalent to showing that the restriction maps $\text{res}_\mathfrak{p} : H^1(K|k, \mu_{2^r}) \to H^1(K_\mathfrak{p}|k_\mathfrak{p}, \mu_{2^r})$ are the zero map for all $\mathfrak{p} \in T$. So let $\mathfrak{p} \in T$, then the decomposition group $G(K_\mathfrak{p}|k_\mathfrak{p})$ is a proper subgroup of $G(K|k)$ and we denote its fixed field by k'. The exact sequence

$$0 \longrightarrow H^1(k'|k, \mu_{2^r} \cap k') \xrightarrow{\text{inf}} H^1(K|k, \mu_{2^r}) \xrightarrow{\text{res}_\mathfrak{p}} H^1(K|k', \mu_{2^r}) = H^1(K_\mathfrak{p}|k_\mathfrak{p}, \mu_{2^r})$$

shows $\ker(\text{res}_\mathfrak{p}) \cong H^1(k'|k, \mu_{2^r} \cap k')$, so we have to prove that this is $\cong \mathbb{Z}/2\mathbb{Z}$. Recall that k' corresponds to an intermediate field of $\mathbb{Q}(\mu_{2^r})|k \cap \mathbb{Q}(\mu_{2^r})$ and that $k \cap \mathbb{Q}(\mu_{2^r})$ is real since we are in the special case $(k, 2^r)$. Looking at the subfield lattice of $\mathbb{Q}(\mu_{2^r})$ we see that either $k' \cap \mu_{2^r} = \{\pm 1\}$ or $k' = k(\mu_{2^t})$ for some $t \geq 2$. In the former case

$$H^1(k'|k, \mu_{2^r} \cap k') = \text{Hom}(G(k'|k), \{\pm 1\}) \neq 0$$

since $k' \neq k$, and in the latter case $k \cap \mathbb{Q}(\mu_{2^t}) \subseteq k \cap \mathbb{Q}(\mu_{2^r})$ is real, so we are in the special case $(k, 2^t)$ and

$$H^1(k'|k, \mu_{2^r} \cap k') = H^1(k(\mu_{2^t}), \mu_{2^t}) \cong \mathbb{Z}/2\mathbb{Z}$$

using proposition 3.7 again. In either case $H^1(k'|k, \mu_{2^r} \cap k') \cong \mathbb{Z}/2\mathbb{Z}$, so we are finished. □

Lemma 3.16. *Let k be a field, and let a and b be coprime integers. Then*

$$k^{\times ab} = k^{\times a} \cap k^{\times b}.$$

Proof. The inclusion "$\subseteq$" is trivial. For "$\supseteq$" write $am + bn = 1$ with integers m and n. If $x = x_1^a = x_2^b \in k^{\times a} \cap k^{\times b}$, then

$$x = x^{am}x^{bn} = x_2^{abm}x_1^{abn} \in k^{\times ab}.$$

□

Now we are able two prove our Hasse principle for mth powers.

Theorem 3.17. *Let k be a number field, m a natural number and T a set of primes of k containing all but finitely many primes. Then the localisation homomorphism*

$$k^\times/k^{\times m} \longrightarrow \prod_{\mathfrak{p}\in T} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times m}$$

is injective except in the special case

- *$m = 2^r m'$ with m' odd and $r \geq 3$,*
- *$k(\mu_{2^r})|k$ is not cyclic, and*
- *all primes $\mathfrak{p} \in T$ dividing 2 decompose in $k(\mu_{2^r})|k$*

where the kernel is of order 2. In any case, if $\alpha \in k^\times$ is a $2m$-th power in $k_\mathfrak{p}^\times$ for all $\mathfrak{p} \in T$, then α is an mth power in $k^\times$.

Proof. By Kummer theory (theorem 2.2), the localisation homomorphism above is

$$H^1(k, \mu_m) \longrightarrow \prod_{\mathfrak{p}\in T} H^1(k_\mathfrak{p}, \mu_m)$$

and its kernel is $Ш^1(k, T, \mu_m)$. Therefore, the first statement follows from theorem 3.15 together with the characterisation of the special case we proved in proposition 3.12.

Now assume that $\alpha \in k^\times$ is a $2m$-th power in $k_\mathfrak{p}$ for all $\mathfrak{p} \in T$. We want to show that α is an mth power in k. By lemma 3.16 we may assume that m is a power of 2, say $m = 2^r$. If we are not in the special case $(k, 2^r, T)$ then this is clear from what we proved above, so assume otherwise. By proposition 3.8 the field $k \cap \mathbb{Q}(\mu_{2^r})$ is real, in particular $\sqrt{-1} \notin k$. Let $K = k(\mu_{2m}) = k(\mu_{2^{r+1}})$. Then, since $K(\mu_{2m})|K$ is trivially cyclic, we are not in the special case $(K, 2m, T(K))$ and the homomorphism

$$K^\times/K^{\times 2m} \longrightarrow \prod_{T(K)} K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2m}$$

is injective. Now α is a $2m$-th power in $K_\mathfrak{p}$ for all $\mathfrak{p} \in T(K)$, hence it is already a $2m$-th power in K. This means that α is in the kernel of the homomorphism

$$k^\times/k^{\times 2m} \longrightarrow K^\times/K^{\times 2m}.$$

But in view of the Kummer isomorphism (theorem 2.2), this is the restriction homomorphism in the exact sequence

$$0 \longrightarrow H^1(K|k, \mu_{2m}) \xrightarrow{\text{inf}} H^1(\overline{k}|k, \mu_{2m}) \xrightarrow{\text{res}} H^1(\overline{k}|K, \mu_{2m})$$

and its kernel $H^1(K|k, \mu_{2m})$ has order two by proposition 3.7. Therefore, $\alpha^2 = \beta^{2m}$ for some $\beta \in k^\times$. Hence $\alpha = \pm\beta^m$. Suppose $\alpha = -\beta^m$. Since α is an mth power in $k_\mathfrak{p}^\times$ for all $\mathfrak{p} \in T$, the same is true for -1. In particular $\sqrt{-1} \in k_\mathfrak{p}$ for all $\mathfrak{p} \in T$ as m is even. The decomposition groups $G_\mathfrak{p}(k(\sqrt{-1})|k) = G(k_\mathfrak{p}(\sqrt{-1})|k_\mathfrak{p})$ are thus trivial for all $\mathfrak{p} \in T$, which means that the extension $k(\sqrt{-1})|k$ is completely decomposed at all $\mathfrak{p} \in T$. By lemma 3.9, this implies $k(\sqrt{-1}) = k$, contradicting $\sqrt{-1} \notin k$. Thus we must have $\alpha = +\beta^m \in k^{\times m}$. □

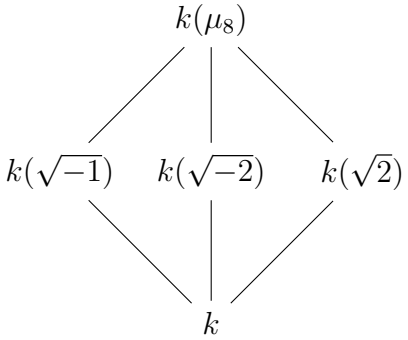
Remark. The result is still true if we loosen the hypothesis that T contains all but finitely many primes by only requiring that is has Dirichlet density $\delta(T) = 1$ (see [NSW08], 9.1.2, for the definition of the Dirichlet density of a set of primes).

Example 3.18. Let $k = \mathbb{Q}$ and let T be the set of all odd primes. Since we are in the special case $(\mathbb{Q}, 8, T)$, the theorem predicts that there should be a number $\alpha \in \mathbb{Q}^\times$ that is an eighth power in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all odd primes p, but not in $\mathbb{Q}$ (it must be a rational fourth power, however). The number 16 is such a number. Indeed, we have the following polynomial factorisation:

$$\begin{aligned} X^8 - 16 &= (X^4 - 4)(X^4 + 4) \\ &= (X^2 - 2)(X^2 + 2)(X^2 - 2X + 2)(X^2 + 2X + 2) \end{aligned}$$

In example 3.13 we saw that for every odd prime p at least one of $\sqrt{-1}$, $\sqrt{2}$, $\sqrt{-2}$ is contained in $\mathbb{Q}_p$, thus 16 is an eight power in all $\mathbb{Q}_p$ (the third and fourth factor have discriminant $-4 = (-1) \cdot 2^2$). However, $\sqrt[8]{16} = \sqrt{2} \notin \mathbb{Q}^\times$.

Example 3.19. Here is an example where an element is an mth power in *all* completions, but not globally: Consider $k = \mathbb{Q}(\sqrt{7})$, $m = 8$ and $T = \mathcal{P}(k) = \{\text{all primes of } k\}$. Since $7 \equiv 3 \bmod 4$, the discriminant of k is $28 = 4 \cdot 7$, so 2 and 7 are ramified in k. However, 7 is unramified in $\mathbb{Q}(\mu_8)$ and therefore $k \cap \mathbb{Q}(\mu_8) = \mathbb{Q}$. So we have globally the field diagram



Locally, however, $\mathbb{Q}_2(\sqrt{7})$ coincides with $\mathbb{Q}_2(\sqrt{-1})$ since $\sqrt{-7} \in \mathbb{Q}_2$, as can be seen by an application of Hensel's lemma together with the fact that $-7 \equiv 1 \bmod 8$ (see [Eis95], Thm. 7.3 for the suitable variant of Hensel's lemma). Writing $\mathfrak{p}$ for the unique prime ideal of k lying over 2, we have $k_\mathfrak{p} = \mathbb{Q}_2(\sqrt{7})$ and $k_\mathfrak{p}(\mu_8) = k_\mathfrak{p}(\sqrt{2})$ and thus $[k_2(\mu_8) : k] = 2$. This implies that $\mathfrak{p}$ decomposes into 2 different prime ideals in $k(\mu_2)$, thus we are in the special case $(k, 8, \mathcal{P}(k))$. Indeed, 16 is an eighth power in $\mathbb{Q}_2(\sqrt{-7})$ since this field contains $\sqrt{-1}$ (see the factorisation of $X^8 - 16$ in the previous example). Moreover, 16 is in eighth power in all completions of k at archimedean primes and at prime ideals lying over an odd prime p since this is already true in $\mathbb{Q}_p$. However, the global field $\mathbb{Q}(\sqrt{7})$ contains none of $\pm\sqrt{2}, \pm\sqrt{-2}$, so 16 is not an eighth power globally.

4 Local Class Field Theory

Our aim is to derive from the Hasse principle for mth powers the Grunwald-Wang theorem. To this end we need some local and global class field theory whose main results are summaried in this and the next section. For the proofs the reader is referred to [Neu13] and Chapter V in [Neu99].

4.1 The Maximal Abelian Extension

Recall that a Galois extension $K|k$ inside $\overline{k}$ is abelian if and only if the quotient $G(\overline{k}|k)/G(\overline{k}|K)$ is abelian, i.e. if and only if the first derived subgroup $G(\overline{k}|k)'$ (the closed subgroup generated by all commutators) is contained in $G(\overline{k}|K)$. Thus, there is a **largest abelian extension** of k, namely the fixed field of $G(\overline{k}|k)'$. It is denoted by k^{ab} and its Galois group is the abelianised absolute Galois group

$$G(k^{\mathrm{ab}}|k) = G(\overline{k}|k)/G(\overline{k}|k)' = G(\overline{k}|k)^{\mathrm{ab}}.$$

4.2 The Maximal Unramified Extension

For a Galois extension $K|k$ of non-archimedean local fields (i.e. finite extensions of $\mathbb{Q}_p$ for some prime number p) there is a surjective homomorphism

$$G(K|k) \twoheadrightarrow G(K(\mathfrak{P})|k(\mathfrak{p}))$$

where $\mathfrak{P}$ denotes the prime of K, $\mathfrak{p}$ the prime of k, and $K(\mathfrak{P})$ and $k(\mathfrak{p})$ are the respective residue fields. Its kernel is the **inertia subgroup** $I(K|k) \subseteq G(K|k)$. The extension $K|k$ is **unramified** if the inertia subgroup $I(K|k)$ is trivial, i.e. if $G(K|k) \twoheadrightarrow G(K(\mathfrak{P})|k(\mathfrak{p}))$ is an isomorphism. For a normal intermediate extension $k \subseteq K' \subseteq K$ with prime ideal $\mathfrak{P}'$ there is a commutative and exact diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I(K|K') & \longrightarrow & G(K|K') & \longrightarrow & G(K(\mathfrak{P})|K'(\mathfrak{P}')) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I(K|k) & \longrightarrow & G(K|k) & \longrightarrow & G(K(\mathfrak{P})|k(\mathfrak{p})) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & I(K'|k) & \longrightarrow & G(K'|k) & \longrightarrow & G(K'(\mathfrak{P}')|k(\mathfrak{p})) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

where the exactness of the first column follows from the nine lemma. This implies that $K'|k$ is unramified if and only if it is fixed under the action of the inertia group $I(K|k)$. Therefore, the fixed field of $I(K|k)$ is the **largest unramified intermediate extension** of $K|k$. In the case $K = \overline{k}$ it is denoted by k^{nr}.

If $\mathbb{F}_q$ is the residue field of k, then the residue field of k^{nr} is its algebraic closure $\overline{\mathbb{F}_q}$. The finite extensions of $\mathbb{F}_q$ are the fields $\mathbb{F}_{q^n}$ for $n \in \mathbb{N}$, and the Galois group $G(\mathbb{F}_{q^n}|\mathbb{F}_q)$ is cyclic of order n, generated by the Frobenius automorphism $x \mapsto x^q$. Thus, the absolute Galois group $G(\overline{\mathbb{F}_q}|\mathbb{F}_q)$ is

$$G(\overline{\mathbb{F}_q}|\mathbb{F}_q) \cong \varprojlim_n \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}.$$

Here, the projective system is indexed by the natural numbers and ordered by divisibility; the transition maps are the natural projections $\mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}$ for $m|n$. The group $\hat{\mathbb{Z}}$ is called the **profinite completion of the integers**. It contains $\mathbb{Z}$ as a dense subgroup. In fact, it is the completion of $\mathbb{Z}$ with respect to the **profinite topology**, in which the arithmetic progressions $n\mathbb{Z}$ ($n \in \mathbb{N}$) form a neighbourhood basis of 0. Under the isomorphism $G(\overline{\mathbb{F}_q}|\mathbb{F}_q) \cong \hat{\mathbb{Z}}$, the element $1 \in \hat{\mathbb{Z}}$ corresponds to the Frobenius automorphism $x \mapsto x^q$. The isomorphism $G(k^{\mathrm{nr}}|k) \cong G(\overline{\mathbb{F}_q}|\mathbb{F}_q)$ shows that there is a unique automorphism $\varphi_k \in G(k^{\mathrm{nr}}|k)$ that satisfies

$$\varphi_k(x) \equiv x^q \pmod{\mathfrak{p}_{k^{\mathrm{nr}}}} \quad \text{for all } x \in \mathcal{O}_{k^{\mathrm{nr}}}.$$

This automorphism φ_k is called the **Frobenius automorphism** of $k^{\mathrm{nr}}|k$. Note that $k^{\mathrm{nr}} \subseteq k^{\mathrm{ab}}$ since $G(k^{\mathrm{nr}}|k) \cong \hat{\mathbb{Z}}$ is abelian.

4.3 The Local Norm Residue Symbol

The main theorem of local class field theory asserts that for every finite abelian extension $K|k$ of non-archimedean local fields there is a surjective homomorphism of topological groups

$$k^\times \xrightarrow{(\quad,K|k)} G(K|k),$$

called the (local) **norm residue symbol**. Its kernel is the **norm group** $N_{K|k}K^\times \subseteq k^\times$, so the norm residue symbol induces an isomorphism

$$G(K|k) \cong k^\times / N_{K|k}K^\times.$$

If $K'|k$ is a normal intermediate extension of $K|k$, there is a commutative diagram

$$\begin{array}{ccc} k^\times & \xrightarrow{(\quad,K|k)} & G(K|k) \\ \| & & \downarrow \\ k^\times & \xrightarrow{(\quad,K'|k)} & G(K'|k). \end{array}$$

If $K|k$ is an arbitrary abelian extension (not necessarily finite), we have $G(K|k) = \varprojlim_{K'} G(K'|k)$ where K' runs over the finite Galois extensions $K'|k$ contained in K. For $a \in k^\times$ the elements $(a, K'|k)$ form a compatible set with respect to this projective system, i.e. they define an element in $G(K|k)$. Thus, the norm residue symbol extends to infinite abelian extensions $K|k$ by setting $(a, K|k) = \varprojlim_{K'}(a, K'|k)$, and its kernel is $\bigcap_{K'} N_{K'|k}K'^\times$. In particular, for $K = k^{\mathrm{ab}}$ there is an **absolute norm residue symbol**

$$\begin{aligned} k^\times &\xrightarrow{(\quad,k^{\mathrm{ab}}|k)} G(k^{\mathrm{ab}}|k), \\ (a, k^{\mathrm{ab}}|k) &= \varprojlim_{K'}(a, K'|k). \end{aligned}$$

We will see later that $k^{\times m}$ is the norm group of the maximal abelian extension of exponent m, and since $\bigcap_{m\geq 1} k^{\times m} = \{1\}$, it follows that the absolute norm residue symbol $(\quad, k^{\mathrm{ab}}|k)$ is injective. However, it cannot be an isomorphism since $G(k^{\mathrm{ab}}|k)$ is a profinite group, whereas $k^\times$ is not even compact. One can show that the cokernel is isomorphic to $\hat{\mathbb{Z}}/\mathbb{Z}$.

There is an explicit description for the norm residue symbol of the maximal unramified extension k^{nr}. Namely, for $x \in k^\times$, we have

$$(x, k^{\mathrm{nr}}|k) = \varphi_k^{v(x)} \in G(k^{\mathrm{nr}}|k)$$

where $v : k^\times \twoheadrightarrow \mathbb{Z}$ is the normalised discrete valuation on k. In particular, the kernel of $(\quad, k^{\mathrm{nr}}|k)$ is the unit group $U_k = \mathcal{O}_k^\times$.

4.4 The Existence Theorem of Local Class Field Theory

For every finite abelian extension $K|k$ there is an associated subgroup of $k^\times$, the norm group $N_{L|k}L^\times$. The following proposition shows that L is completely determined by $N_{L|k}L^\times$. We use the notation

$$N_L := N_{L|k}L^\times.$$

Proposition 4.1. *Let L_1 and L_2 be two finite abelian extensions of k. Then we have*

$$N_{L_1L_2} = N_{L_1} \cap N_{L_2}, \quad N_{L_1 \cap L_2} = N_{L_1} \cdot N_{L_2}.$$

In other words, the association $L \mapsto N_L$ from finite abelian extensions of k to subgroups of $k^\times$ is an order-reversing lattice homomorphism and in particular injective.

Proof. Since the Galois group $G(L_1L_2|k)$ embeds into $G(L_1|k) \times G(L_2|k)$, the extension $L_1L_2|k$ is also finite and abelian. The inclusion $N_{L_1L_2} \subseteq N_{L_1} \cap N_{L_2}$ follows from

$$N_{L_1L_2|k} = N_{L_i|k} \circ N_{L_1L_2|L_i}, \quad (i = 1, 2).$$

For the reverse inclusion, let $a \in N_{L_1} \cap N_{L_2}$. Then $(a, L_1L_2|k)\big|_{L_i} = (a, L_i|k) = 1$ for $i = 1, 2$, hence $(a, L_1L_1|k) = 1$, i.e. $a \in N_{L_1L_2}$. This shows $N_{L_1L_2} = N_{L_1} \cap N_{L_2}$.

Now we have

$$\begin{aligned} L_1 \subseteq L_2 &\iff L_1L_2 = L_2 \\ &\iff N_{L_1} \cap N_{L_2} = N_{L_2} \\ &\iff N_{L_1} \supseteq N_{L_2}, \end{aligned}$$

so the association $L \mapsto N_L$ is an order-reversing embedding of partially ordered sets, in particular injective. Since $L_1 \cap L_2$ is the largest field contained in both L_1 and L_2, it follows that $N_{L_1 \cap L_2}$ is the smallest subgroup of $k^\times$ containing both N_{L_1} and N_{L_2}, i.e. $N_{L_1 \cap L_2} = N_{L_1} \cdot N_{L_2}$. □

This shows that the structure of the finite abelian extensions of k is reflected in the subgroup structure of $k^\times$. It is now natural to ask which subgroups of $k^\times$ occur as norm groups N_L of an extension $L|k$. The norm group N_L is the kernel of the norm residue symbol $k^\times \longrightarrow G(L|k)$, which is continuous, thus N_L is always a closed subgroup of finite index in $k^\times$. The existence theorem of local class field theory states that in fact *every* closed subgroup of finite index in $k^\times$ is the norm group N_L of some finite abelian extension $L|k$.

Theorem 4.2 (Existence theorem of local class field theory)**.** *The association $L \mapsto N_L$ is an order-reversing lattice isomorphism between the finite abelian extensions of k and the closed subgroups of finite index in $k^\times$.* □

For a closed subgroup N of finite index in $k^\times$, the abelian extension $L|k$ with $N_L = N$ is called the **class field** of N. Note that every closed subgroup of finite index is automatically open as its complement is a finite union of closed cosets.

4.5 The Structure of the Multiplicative Group

Let k be a finite extension of $\mathbb{Q}_p$. By the existence theorem, the finite abelian extensions of k are reflected in the subgroup structure of $k^\times$, so we are naturally led to the question what it looks like. The exposition given here roughly follows chapter II.§5 in [Neu99].

Let π be a uniformiser of k. Then every element $a \in k^\times$ can be uniquely written as $a = \pi^n u$ with $n \in \mathbb{Z}$ and $u \in U_k$, so we have

$$k^\times \cong \mathbb{Z} \times U_k,$$

algebraically and topologically (the valuation $v : k^\times \to \mathbb{Z}$ is locally constant, thus continuous for the discrete topology on $\mathbb{Z}$). Let $f = [k(\mathfrak{p}) : \mathbb{F}_p]$ be the residue field degree, so the residue field of k is $k(\mathfrak{p}) = \mathbb{F}_q$ where $q = p^f$. The group $\mathbb{F}_q^\times$ is the full group of $(q-1)$-th roots of unity. By Hensel's lemma, the $(q-1)$-th roots of unity are already present in $k^\times$, so the exact sequence

$$1 \longrightarrow U_k^{(1)} \longrightarrow U_k \longrightarrow \mathbb{F}_q^\times \longrightarrow 1$$

splits, i.e. $U_k = \mu_{q-1} \times U_k^{(1)}$. We are thus reduced to the study of the group $U_k^{(1)}$ of principal units. It is a profinite group since it is isomorphic to the projective limit

$$U_k^{(1)} \cong \varprojlim_n U_k^{(1)}/U_k^{(n)}.$$

The isomorphism

$$\begin{aligned} U_k^{(n)}/U_k^{(n+1)} &\xrightarrow{\sim} k(\mathfrak{p}), \\ 1 + \pi^n a \bmod U_k^{(n+1)} &\longmapsto a \bmod \mathfrak{p} \end{aligned}$$

implies $(U_k^{(1)} : U_k^{(n+1)}) = q^n$, so the quotient $U_k^{(1)}/U_k^{(n+1)}$ is a module over $\mathbb{Z}/q^n\mathbb{Z}$. Passing to the projective limits

$$U_k^{(1)} \cong \varprojlim_n U_k^{(1)}/U_k^{(n+1)}, \quad \mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/q^n\mathbb{Z},$$

$U_k^{(1)}$ becomes naturally a $\mathbb{Z}_p$-module. The module operation can be seen as the usual operation of $\mathbb{Z}$ extended to $\mathbb{Z}_p$ by continuity, i.e. for $x \in \mathfrak{p}$, $a = \lim_{i\to\infty} a_i \in \mathbb{Z}_p$, $a_i \in \mathbb{Z}$ we have

$$(1+x)^a = \lim_{i\to\infty} (1+x)^{a_i}.$$

The higher unit groups $U_k^{(n)}$ are closed subgroups of $U_k^{(1)}$, hence $\mathbb{Z}_p$-submodules.

Theorem 4.3. *Let $e = v_k(p)$ be the ramification index of $k|\mathbb{Q}_p$. For $n > \frac{e}{p-1}$, the power series*

$$\begin{aligned} \exp(X) &= 1 + X + \frac{X^2}{2} + \frac{X^3}{6} + \dots \quad \textit{and} \\ \log(1+Y) &= Y - \frac{Y^2}{2} + \frac{Y^3}{3} - \frac{Y^4}{4} + \dots \end{aligned}$$

define mutually inverse isomorphisms

$$U_k^{(n)} \underset{\log}{\overset{\exp}{\rightleftarrows}} \mathfrak{p}^n$$

of topological $\mathbb{Z}_p$-modules. □

The equalities $\exp(\log(1+Y)) = 1+Y$ and $\log(\exp(X)) = X$ hold already in the ring of power series, so the only thing that needs to be checked is that the series converge on the given domains and map to the right set. The details can be found in [Neu99], Thm. II.5.5.

So by the theorem we have

$$U_k^{(n)} \cong \mathfrak{p}^n = \pi^n \mathcal{O}_k \cong \mathcal{O}_k$$

for large n. The valuation ring $\mathcal{O}_k$ is also the ring of integers of k and has therefore an integral basis over $\mathbb{Z}_p$, i.e. $\mathcal{O}_k \cong \mathbb{Z}_p^d$ where $d := [k : \mathbb{Q}_p]$. So $U_k^{(n)}$ is a free $\mathbb{Z}_p$-module of rank d. Since it has finite index in $U_k^{(1)}$, the structure theorem for modules over principal ideal domains implies that $U_k^{(1)}$ is also a finitely generated $\mathbb{Z}_p$-module of rank d. More precisely, $U_k^{(1)}$ is the direct sum of its torsion subgroup and a subgroup isomorphic to $\mathbb{Z}_p^d$. The torsion part is the group of roots of unity of p-power order in $k^\times$, say μ_{p^a}. Let V be the free part and let $\varepsilon_1, \ldots, \varepsilon_d$ be a free generating set. Then V is the image of the continuous map

$$\mathbb{Z}_p^d \longrightarrow U_k^{(1)},\ (a_1, \ldots, a_d) \longmapsto \varepsilon_1^{a_1} \cdots \varepsilon_d^{a_d},$$

hence compact and thus closed (as $U_k^{(1)}$ is Hausdorff). So the decomposition $U_k^{(1)} = \mu_{p^a} \times V$ is topological.

Putting everything together, we have proved

$$k^\times \cong \mathbb{Z} \oplus \mathbb{Z}/(q-1)\mathbb{Z} \oplus \mathbb{Z}/p^a\mathbb{Z} \oplus \mathbb{Z}_p^d,$$

topologically and algebraically.

Corollary 4.4. *Let m be a natural number and let $L|k$ be the maximal abelian extension of exponent m. Then $L|k$ is finite and its norm group is $N_L = k^{\times m}$.*

Proof. A finite abelian extension $K|k$ has exponent m if and only if $G(K|k) \cong k^\times/N_K$ has exponent m, i.e. if $k^{\times m} \subseteq N_K$. By our description of the multiplicative group $k^\times$, the subgroup $k^{\times m}$ is closed and has finite index, so it has a class field L', i.e. a finite abelian extension with $N_{L'} = k^{\times m}$. Now $k^{\times m}$ is smallest closed finite-index subgroup containing $k^{\times m}$, so L' is the largest finite abelian extension of exponent m. Thus we have $L' = L$. □

5 Global Class Field Theory

Global class field theory is concerned with abelian extensions of number fields. There is a norm residue symbol analogous to the local case, however the role of the multiplicative group of the ground field is now taken by the idele class group which we will define now. In this section, k is always a number field.

5.1 The Idele Class Group

Definition 5.1. Let $(X_i)_{i\in I}$ be a family of Hausdorff abelian topological groups, and $(Y_i)_{i\in I}$ a family of open subgroups $Y_i \subseteq X_i$. The **restricted product**

$$\prod_{i\in I}(X_i, Y_i)$$

is the subgroup of $\prod_{i\in I} X_i$ consisting of all $(x_i)_{i\in I}$ such that $x_i \in Y_i$ for almost all i. It carries a topology with a neighbourhood basis of the identity given by the subsets

$$\prod_{j\in J} U_j \times \prod_{i\in I\setminus J} Y_i$$

where J runs over the finite subsets of I and U_j runs over the open subsets of X_j.

If it is clear from the context what the Y_i are we will drop them from the notation and simply write $\prod_{i\in I} X_i$. If all X_i are locally compact and almost all Y_i are compact, then the restricted product $\prod_{i\in I}(X_i, Y_i)$ is again locally compact.

Definition 5.2. Let k be a number field. The **idele group** of k is

$$I_k = \prod_{\mathfrak{p}} k_{\mathfrak{p}}^{\times}$$

where $\mathfrak{p}$ runs over all primes of k and the restricted product is taken with respect to the unit groups $U_{k_\mathfrak{p}}$ for the non-archimedean primes. (There is no restriction at the archimedean primes since there is only a finite number of them anyway).

The multiplicative group $k^\times$ is embedded diagonally into the idele group

$$\begin{aligned} k^\times &\hookrightarrow I_k \\ a &\longmapsto (\ldots, a, a, a, \ldots). \end{aligned}$$

The image of $k^\times$ in I_k is a discrete and thus closed subgroup of I_k. The quotient $C_k := I_k/k^\times$ is called the **idele class group** of k. It is an abelian locally compact topological group.

If $L|k$ is a finite extension and $\mathfrak{P}$ is a non-archimedean prime of L lying over $\mathfrak{p}$, the norm $N_{L|k} : L^\times \to k^\times$ maps units to units, thus it induces a norm map on the idele groups

$$\begin{aligned} N_{L|k} : I_L &\longrightarrow I_k, \\ (a_\mathfrak{P}) &\longmapsto \big(\prod_{\mathfrak{P}|\mathfrak{p}} N_{L_\mathfrak{P}|k_\mathfrak{p}}(a_\mathfrak{P})\big)_\mathfrak{p} \end{aligned}$$

This norm on ideles commutes with the inclusions $k^\times \hookrightarrow I_k$ and $L^\times \hookrightarrow I_L$ and therefore induces a norm map between the idele class groups

$$N_{L|k} : C_L \longrightarrow C_k.$$

5.2 The Global Norm Residue Symbol

The main theorem of global class field theory states that for every finite abelian Galois extension $L|k$ of number fields there is a surjective homomorphism of topological groups

$$C_k \xrightarrow{(\quad,L|k)} G(L|k)$$

whose kernel is the norm group $N_{L|k}C_L$. This map is called the (global) **norm residue symbol**. It induces an isomorphism

$$G(L|k) \cong C_k/N_{L|k}C_L.$$

As in the local case, we have for every normal intermediate extension $E|k$ of $L|k$ a commutative square

$$\begin{array}{ccc} C_k & \xrightarrow{(\quad,L|k)} & G(L|k) \\ \| & & \downarrow \\ C_k & \xrightarrow{(\quad,E|k)} & G(E|k), \end{array}$$

so the norm residue symbol extends to infinite abelian Galois extensions $L|k$ via

$$\begin{aligned} C_k &\xrightarrow{(\quad,L|k)} G(L|k) \\ (\alpha, L|k) &= \varprojlim_E (\alpha, E|k), \end{aligned}$$

E running over the finite Galois extensions $E|k$ inside L. Unlike the local norm residue symbol, it is also surjective for infinite extensions. Its kernel is the intersection

$$\ker\left[C_k \xrightarrow{(\quad,L|k)} G(L|k)\right] = \bigcap_E N_{E|k}C_E.$$

The global norm residue symbol can be explicitly expressed in terms of the local norm residue symbols. Namely, for $\alpha = (a_\mathfrak{p}) \in I_k$ we have

$$(\alpha, L|k) = \prod_\mathfrak{p} (a_\mathfrak{p}, L_\mathfrak{p}|k_\mathfrak{p})$$

where $L_\mathfrak{p}$ denotes the localisation of L at any prime lying over $\mathfrak{p}$, and the local Galois group $G(L_\mathfrak{p}|k_\mathfrak{p})$ is embedded into $G(L|k)$ as the decomposition group of that prime. The product on the right side is finite since for almost all primes $\mathfrak{p}$ the component $a_\mathfrak{p}$ is a unit and $L_\mathfrak{p}|k_\mathfrak{p}$ is unramified, and we have $(a_\mathfrak{p}, L_\mathfrak{p}|k_\mathfrak{p}) = 1$ for those primes. This describes the norm residue symbol as a map $I_k \to G(L|k)$, but the fact that it factors over $I_k/k^\times$ implies that we have the product formula

$$\prod_\mathfrak{p} (a, L_\mathfrak{p}|k_\mathfrak{p}) = 1$$

for all $a \in k^\times$.

Now consider the maximal abelian extension k^{ab} of k. It can be shown that the kernel D_k of the norm residue symbol $(\quad, k^{\mathrm{ab}}|k)$ is the connected component of 1 in C_k and that it is uniquely divisible (see [NSW08],VIII.§2). This implies, by looking at the cokernels of the vertical maps in commutative exact diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & D_k & \longrightarrow & C_k & \xrightarrow{(\quad, k^{\mathrm{ab}}|k)} & G(k^{\mathrm{ab}}|k) & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} & & \\ 1 & \longrightarrow & D_k & \longrightarrow & C_k & \xrightarrow{(\quad, k^{\mathrm{ab}}|k)} & G(k^{\mathrm{ab}}|k) & \longrightarrow & 1 \end{array}$$

that for the maximal abelian extension $L|k$ of exponent m we have

$$G(L|k) \cong C_k/C_k^m.$$

5.3 The Existence Theorem of Global Class Field Theory

Just as in the local case a finite abelian extension $L|k$ is completely determined by its norm group $N_L := N_{L|k}C_L$ and there is an existence theorem which states that every closed subgroup of finite index in C_k is the norm group of some finite abelian extension.

Theorem 5.3 (Existence theorem of global class field theory)**.** *The association $L \mapsto N_L$ is an order-reversing lattice isomorphism between the finite abelian extensions of k and the closed subgroups of finite index in C_k.* □

6 The Grunwald-Wang Theorem

As before, let k be a number field and let S be a set of primes of k. The set of all primes of k is denoted by $\mathcal{P}(k)$. For a G_k-module A we have a localisation homomorphism

$$H^1(k, A) \longrightarrow \prod_{\mathfrak{p} \in S} H^1(k_\mathfrak{p}, A)$$

which enables us to study the interplay between global and local cohomology. In section 3 we dealt (for $A = \mu_m$) with the question whether global cohomology classes are completely determined by their local restrictions if S is "big enough" in some sense. One can also ask a dual question: If S is "small enough" (finite, for example), can we, given a local cohomology class for each $\mathfrak{p} \in S$, always find a global cohomology class with the given local restrictions? While the former question is about the injectivity of the localisation map, the latter is about its surjectivity. Our aim is to derive for a finite set of primes S the surjectivity of

$$H^1(k, \mathbb{Z}/m\mathbb{Z}) \longrightarrow \prod_{\mathfrak{p} \in S} H^1(k_\mathfrak{p}, \mathbb{Z}/m\mathbb{Z})$$

from the injectivity of

$$H^1(k,\mu_m) \longrightarrow \prod_{\mathfrak{p}\notin S} H^1(k_\mathfrak{p},\mu_m)$$

that we proved in section 3, provided that we are not in the special case $(k,m,\mathcal{P}(k)\setminus S)$. Recalling that elements of $H^1(k,\mathbb{Z}/m\mathbb{Z}) = \mathrm{Hom}_{\mathrm{cts}}(G(\overline{k}|k),\mathbb{Z}/m\mathbb{Z})$ correspond to Galois extensions of k of exponent m, this will help us to prove the Grunwald-Wang theorem which states that under suitable conditions one can, for finitely many given local extensions $K_\mathfrak{p}|k_\mathfrak{p}$, find a global extension $K|k$ with the given completions. One way to translate injectivity statements to surjectivity statements is Pontryagin duality, and this is what we will use here, together with the class field theory from the previous sections. It should however be remarked that there are also arithmetic duality theorems such as Poitou-Tate duality which are much deeper and provide a more general context for the kind of questions we are treating here. Our approach is essentially a special case of them, but it might give some idea of how the more general duality theorems are proved. The crucial step where class field theory comes into play is the following lemma.

Lemma 6.1. *Let m be a natural number and S a finite set of primes of k. Let $L|k$ be the maximal abelian extension of exponent m and for $\mathfrak{p}\in S$ let $M_\mathfrak{p}|k_\mathfrak{p}$ be the maximal abelian extension of exponent m for $k_\mathfrak{p}$. If we are not in the special case $(k,m,\mathcal{P}(k)\setminus S)$, then the natural homomorphism*

$$\prod_S G(M_\mathfrak{p}|k_\mathfrak{p}) \longrightarrow G(L|k)$$

is injective. In the special case, the kernel is of order 1 or 2.

Proof. The homomorphism above is induced by the restrictions

$$G(M_\mathfrak{p}|k_\mathfrak{p}) \twoheadrightarrow G(L_\mathfrak{p}|k_\mathfrak{p}) \hookrightarrow G(L|k).$$

By local and global class field theory, they fit into a commutative diagram

$$\begin{array}{ccc}
k_\mathfrak{p}^\times & \xrightarrow{(\quad,M_\mathfrak{p}|k_\mathfrak{p})} & G(M_\mathfrak{p}|k_\mathfrak{p}) \\
\| & & \downarrow\!\!\downarrow \\
k_\mathfrak{p}^\times & \xrightarrow{(\quad,L_\mathfrak{p}|k_\mathfrak{p})} & G(L_\mathfrak{p}|k_\mathfrak{p}) \\
\downarrow & & \downarrow \\
C_k & \xrightarrow{(\quad,L|k)} & G(L|k)
\end{array}$$

where the second vertical map on the left is given by

$$\begin{aligned} k_\mathfrak{p}^\times &\longrightarrow C_k, \\ a_\mathfrak{p} &\longmapsto (\ldots,1,1,a_\mathfrak{p},1,1\ldots) \bmod k^\times. \end{aligned}$$

We have seen in section 4 and 5 that the norm residue symbols induce isomorphisms $k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times m} \cong G(M_\mathfrak{p}|k_\mathfrak{p})$ and $C_k/C_k^m \cong G(L|k)$, so we get a commutative diagram

$$\begin{array}{ccc} \prod_S k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times m} & \xrightarrow{\sim} & \prod_S G(M_\mathfrak{p}|k_\mathfrak{p}) \\ \downarrow & & \downarrow \\ C_k/C_k^m & \xrightarrow{\sim} & G(L|k). \end{array}$$

Thus, in order to prove the lemma, we can equivalently show that the left vertical map is injective if we are not in the special case, and has a kernel of order 1 or 2 otherwise.

First, from the commutative exact diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & k^\times & \longrightarrow & I_k & \longrightarrow & C_k & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} & & \downarrow{\scriptstyle m} & & \\ 1 & \longrightarrow & k^\times & \longrightarrow & I_k & \longrightarrow & C_k & \longrightarrow & 1 \end{array}$$

we get the exact cokernel sequence

$$k^\times/k^{\times m} \longrightarrow I_k/I_k^m \longrightarrow C_k/C_k^m \longrightarrow 1.$$

Now from the diagram

$$\begin{array}{ccccccccc} & & k^\times/k^{\times m} & & \longrightarrow & & I_k/I_k^m & \longrightarrow & C_k/C_k^m & \longrightarrow & 1 \\ & & \downarrow & & & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \prod_{\mathfrak{p}\notin S} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times m} & & \xrightarrow{\text{id}} & & \prod_{\mathfrak{p}\notin S} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times m} & \longrightarrow & 1 & & \end{array}$$

we get an exact sequence of kernels (the first half of the snake lemma)

$$1 \longrightarrow Ш^1(k, \mathcal{P}(k), \mu_m) \longrightarrow Ш^1(k, \mathcal{P}(k) \setminus S, \mu_m) \longrightarrow \prod_S k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times m} \longrightarrow C_k/C_k^m.$$

In section 3 we proved that the group

$$Ш^1(k, \mathcal{P}(k) \setminus S, \mu_m) = \ker\left[k^\times/k^{\times m} \longrightarrow \prod_{\mathfrak{p}\notin S} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times m}\right]$$

is trivial if we are not in the special case $(k, m, \mathcal{P}(k) \setminus S)$, and of order 2 otherwise. This proves the lemma. □

Remark 6.2. From the proof we see that even in the special case $(k, m, \mathcal{P}(k) \setminus S)$ the map

$$\prod_S G(M_\mathfrak{p}|k_\mathfrak{p}) \longrightarrow G(L|k)$$

may still be injective, and this is the case if and only if

$$Ш^1(k, \mathcal{P}(k) \setminus S, \mu_m) = Ш^1(k, \mathcal{P}(k), \mu_m),$$

i.e. if every element of $k^\times$ that is an mth power in $k_\mathfrak{p}$ for all $\mathfrak{p} \notin S$ is in fact an mth power in *all* completions $k_\mathfrak{p}$.

Looking at the lemma, one might wonder whether $M_\mathfrak{p}$, the maximal abelian extension of exponent m over $k_\mathfrak{p}$, is the same as the localisation $L_\mathfrak{p}$ ($= Lk_\mathfrak{p}$) of the maximal abelian extension L of exponent m over k. One might then make some unsuccessful attempts to prove this (at least the author did), until one realizes that this fails to hold in a very special case. Indeed, noting that $G(M_\mathfrak{p}|L_\mathfrak{p})$ is the kernel of $G(M_\mathfrak{p}|k_\mathfrak{p}) \to G(L|k)$, we can take $S = \{\mathfrak{p}\}$ in lemma 6.1, and get an isomorphism

$$G(M_\mathfrak{p}|L_\mathfrak{p}) \cong \frac{Ш^1(k, \mathcal{P}(k) \setminus \{\mathfrak{p}\}, \mu_m)}{Ш^1(k, \mathcal{P}(k), \mu_m)}.$$

This shows the following proposition.

Proposition 6.3. *Let m be a natural number and $\mathfrak{p}$ and prime of k. Let $L|k$ and $M_\mathfrak{p}|k_\mathfrak{p}$ be the global and local maximal abelian extensions of exponent m. Then $L_\mathfrak{p} = M_\mathfrak{p}$, except in the special case*

- *$m = 2^r m'$ with m' odd and $r \geq 3$,*
- *$k(\mu_{2^r})|k$ is not cyclic,*
- *all primes $\mathfrak{q} \neq \mathfrak{p}$ dividing 2 decompose in $k(\mu_{2^r})|k$, and*
- *there exists $a \in k^\times$ such that a is an mth power in $k_\mathfrak{q}$ for all $\mathfrak{q} \neq \mathfrak{p}$, but not in $k_\mathfrak{p}$,*

in which case we have $[M_\mathfrak{p} : L_\mathfrak{p}] = 2$. □

In example 3.18 we have seen that $k = \mathbb{Q}$, $m = 8$ and $\mathfrak{p} = 2$ satisfies all conditions of this special case. Here, $a = 16$ is an 8-th power in $\mathbb{R}$ and $\mathbb{Q}_p$ for all $p \neq 2$, but not in $\mathbb{Q}_2$. So the localisation of the maximal abelian extension of exponent 8 over $\mathbb{Q}$ at a prime dividing 2 is not equal to the maximal abelian extension of exponent 8 over $\mathbb{Q}_2$. In contrast, it is always true that $(k^{\mathrm{ab}})_\mathfrak{p} = (k_\mathfrak{p})^{\mathrm{ab}}$ (this is VI.§5, Ex. 2 in [Neu99]).

Now in order to prove the Grunwald-Wang theorem, we would like to show that every homomorphism $\prod_S G(M_\mathfrak{p}|k_\mathfrak{p}) \longrightarrow \mathbb{R}/\mathbb{Z}$ can be extended to a continuous homomorphism $G(L|k) \longrightarrow \mathbb{R}/\mathbb{Z}$. This follows from a general theorem related to Pontryagin duality.

Definition 6.4. The group

$$\mathbb{T} := \mathbb{R}/\mathbb{Z}$$

is called the **circle group**. With the quotient topology from $\mathbb{R}$ it is a Hausdorff and locally compact abelian topological group.

For any Hausdorff locally compact abelian topological group G,

$$G^\vee := \mathrm{Hom}_{\mathrm{cts}}(G, \mathbb{T})$$

is called the **Pontryagin dual** of G.

Theorem 6.5. *Let G be a Hausdorff locally compact abelian topological group and $H \subseteq G$ a compact subgroup. Then every continuous homomorphism $f : H \to \mathbb{T}$ can be extended to a continuous homomorphism $\tilde{f} : G \to \mathbb{T}$ with $\tilde{f}|_H = f$.* □

The theorem can also be expressed by saying that the restriction homomorphism $G^\vee \to H^\vee$ is surjective. It is not difficult to show that every homomorphism $H \to \mathbb{T}$ can be extended to a homomorphism $G \to \mathbb{T}$ (the proof uses Zorn's lemma and the fact that $\mathbb{T}$ is divisible), but it is not obvious that this can be done in such a way that the extension is still *continuous*. A proof can be found for example in [Mor77].

Corollary 6.6. *Let k be a number field, S a finite set of primes of k and A a finite abelian group. If we are not in the special case $(k, \exp(A), \mathcal{P}(k) \setminus S)$, then the map*

$$\mathrm{Hom}_{\mathrm{cts}}(G(\overline{k}|k), A) \longrightarrow \prod_S \mathrm{Hom}_{\mathrm{cts}}(G(\overline{k_\mathfrak{p}}|k_\mathfrak{p}), A)$$

is surjective.

Proof. Writing A as a product of cyclic groups, $A = \prod_i A_i$, and noting that

$$\mathrm{Hom}_{\mathrm{cts}}(G, \prod_i A_i) = \prod_i \mathrm{Hom}_{\mathrm{cts}}(G, A_i)$$

for every topological group G, we may assume that A is cyclic, say $A = \mathbb{Z}/m\mathbb{Z}$. Let $L|k$ and $M_\mathfrak{p}|k_\mathfrak{p}$ be the global and local maximal abelian extension of exponent m. By Galois correspondence, $G(\overline{k}|L)$ is the smallest closed subgroup of $G(\overline{k}|k)$ containing all commutators and $G(\overline{k}|k)^m$, therefore $G(\overline{k}|L)$ is annihilated by every continuous homomorphism $G(\overline{k}|k) \to \mathbb{Z}/m\mathbb{Z}$. Thus

$$\begin{aligned}\mathrm{Hom}_{\mathrm{cts}}(G(\overline{k}|k), \mathbb{Z}/m\mathbb{Z}) &\cong \mathrm{Hom}_{\mathrm{cts}}(G(L|k), \mathbb{Z}/m\mathbb{Z}) \\ &\cong \mathrm{Hom}_{\mathrm{cts}}(G(L|k), \tfrac{1}{m}\mathbb{Z}/\mathbb{Z}) \\ &= G(L|k)^\vee\end{aligned}$$

and similarly $\mathrm{Hom}_{\mathrm{cts}}(G(\overline{k_\mathfrak{p}}|k_\mathfrak{p}), \mathbb{Z}/m\mathbb{Z}) \cong G(M_\mathfrak{p}|k_\mathfrak{p})^\vee$. Thus we have to show that

$$G(L|k)^\vee \longrightarrow \prod_S G(M_\mathfrak{p}|k_\mathfrak{p})^\vee$$

is surjective. But this follows directly from theorem 6.5 and lemma 6.1 (note that $\prod_S G(M_\mathfrak{p}|k_\mathfrak{p})$ is compact since it is finite). □

Theorem 6.7 (Grunwald-Wang)**.** *Let k be a number field, S a finite set of primes of k and A a finite abelian group. Assume further that for every prime $\mathfrak{p} \in S$ we are given a finite abelian extension $K_\mathfrak{p}|k_\mathfrak{p}$ such that $G(K_\mathfrak{p}|k_\mathfrak{p})$ may be embedded into A. If we are not in the special case $(k, \exp(A), \mathcal{P}(k) \setminus S)$, then there exists a finite abelian extension $K|k$ with Galois group A such that K has the given local completions $K_\mathfrak{p}$.*

Proof. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_s$ be primes not contained in S and not dividing 2, and let

$$\varphi_i : G(\overline{k_{\mathfrak{q}_i}}|k_{\mathfrak{q}_i}) \to A$$

be continuous homomorphisms whose images together generate A (this can be done for example by writing A as a product of cyclic groups, and using that for every $n \in \mathbb{N}$ there is a unique unramified extension of $k_{\mathfrak{q}_i}$ of degree n, which has Galois group isomorphic to $\mathbb{Z}/n\mathbb{Z}$). Put $S' = S \cup \{\mathfrak{q}_1, \dots, \mathfrak{q}_s\}$. Since we are not in the special case $(k, \exp(A), \mathcal{P}(k) \setminus S)$ and the $\mathfrak{q}_i$ do not divide 2, we are also not in the special case $(k, \exp(A), \mathcal{P}(k) \setminus S')$, thus by proposition 6.6 the homomorphism

$$\mathrm{Hom}_{\mathrm{cts}}(G(\overline{k}|k), A) \longrightarrow \prod_{\mathfrak{p} \in S'} \mathrm{Hom}_{\mathrm{cts}}(G(\overline{k_{\mathfrak{p}}}|k_{\mathfrak{p}}), A)$$

is surjective. The given extensions $K_{\mathfrak{p}}|k_{\mathfrak{p}}$ with embeddings $G(K_{\mathfrak{p}}|k_{\mathfrak{p}}) \hookrightarrow A$ define continuous homomorphisms $\varphi_{\mathfrak{p}} : G(\overline{k_{\mathfrak{p}}}|k_{\mathfrak{p}}) \to G(K_{\mathfrak{p}}|k_{\mathfrak{p}}) \hookrightarrow A$ with kernel $G(\overline{k_{\mathfrak{p}}}|K_{\mathfrak{p}})$, and together with the φ_i we get an element of the right hand side. Let $\varphi \in \mathrm{Hom}_{\mathrm{cts}}(G_k, A)$ be a preimage, i.e. $\varphi : G_k \to A$ is a continuous homomorphism such that the diagrams

$$\begin{array}{ccc} G(\overline{k_{\mathfrak{p}}}|k_{\mathfrak{p}}) & \hookrightarrow & G(\overline{k}|k) \\ \downarrow{\scriptstyle \varphi_{\mathfrak{p}}} & & \downarrow{\scriptstyle \varphi} \\ A & = & A \end{array} \qquad \begin{array}{ccc} G(\overline{k_{\mathfrak{q}_i}}|k_{\mathfrak{q}_i}) & \hookrightarrow & G(\overline{k}|k) \\ \downarrow{\scriptstyle \varphi_i} & & \downarrow{\scriptstyle \varphi} \\ A & = & A \end{array}$$

commute for all $\mathfrak{p} \in S$ and $i = 1, \dots, s$. Let $K|k$ be the extension corresponding to φ, i.e. $K = \overline{k}^{\ker \varphi}$. The right squares together with the choice of the φ_i imply that φ is surjective, hence $G(K|k) \cong A$. Recalling our remarks in section 2.1, the commutativity of the left squares implies that K has the given completions $K_{\mathfrak{p}}$ for $\mathfrak{p} \in S$. □

References

[Eis95] D. Eisenbud. *Commutative Algebra: With a View Toward Algebraic Geometry.* Graduate Texts in Mathematics. Springer, 1995.

[Lan02] S. Lang. *Algebra.* Graduate Texts in Mathematics Series. Springer London, Limited, 2002.

[Mor77] S.A. Morris. *Pontryagin Duality and the Structure of Locally Compact Abelian Groups.* London Mathematical Society Lecture Note Series. Cambridge University Press, 1977.

[Neu99] J. Neukirch. *Algebraic Number Theory.* Grundlehren der mathematischen Wissenschaften. Springer, 1999.

[Neu13] J. Neukirch. *Class Field Theory*. Springer, 2013.

[NSW08] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Grundlehren der mathematischen Wissenschaften. Springer, 2008.