Algebraic number theory II

Uwe Jannsen

Contents

1 Infinite Galois theory

An algebraic field extension L/K is called **Galois**, if it is normal and separable. For this, L/K does not need to have finite degree. For example, for a finite field $\mathbb{F}_p$ with p elements (p a prime number), the algebraic closure $\overline{\mathbb{F}_p}$ is Galois over $\mathbb{F}_p$, and has infinite degree. We define in this general situation

Definition 1.1 Let L/K be a Galois extension. Then the Galois group of L over K is defined as $\mathrm{Gal}(L/K) := \mathrm{Aut}_K(L) = \{\sigma : L \to L \mid \sigma \text{ field automorphisms}, \sigma(x) = x \text{ for all } x \in K\}$.

But the main theorem of Galois theory (correspondence between all subgroups of $\mathrm{Gal}(L/K)$ and all intermediate fields of L/K) only holds for finite extensions! To obtain the correct answer, one needs a topology on $\mathrm{Gal}(L/K)$:

Definition 1.2 Let L/K be a Galois extension. The **Krull topology** on $G = Gal(L/K)$ is defined by the fact that for every element $\sigma \in G$ the cosets

$$\sigma \cdot \mathrm{Gal}(L/K') \quad , \quad K'/K \text{ finite},$$

form a basis of neighborhoods of σ.

This gives in fact a topology: By standard definitions of topology we have to show: Let $\sigma\,\mathrm{Gal}(L/K')$ and $\tau\,\mathrm{Gal}(L/K'')$ be as given above, and let $\rho \in \sigma\,\mathrm{Gal}(L/K') \cap \tau\,\mathrm{Gal}(L/K'')$. Then there is a finite extension K'''/K with

$$\rho\,\mathrm{Gal}(L/K''') \subseteq \sigma\,\mathrm{Gal}(L/K') \cap \tau\,\mathrm{Gal}(L/K'')\,.$$

But this holds for $K''' = K' \cdot K''$ (the compositum), since we have $\mathrm{Gal}(L/K''') = \mathrm{Gal}(L/K') \cap \mathrm{Gal}(L/K'')$ and since $\rho \in \sigma\,\mathrm{Gal}(L/K')$, we have $\rho\,\mathrm{Gal}(L/K''') \subseteq \sigma\,\mathrm{Gal}(L/K')$, similarly we have $\rho\,\mathrm{Gal}(L/K''') \subseteq \tau\,\mathrm{Gal}(L/K'')$.

Lemma 1.3 With this topology, $G = \mathrm{Gal}(L/K)$ is a **topological** group, i.e., the multiplication

$$\mu : G \times G \to G\,, \quad (\sigma, \tau) \mapsto \sigma\tau$$

and forming the inverse

$$\iota : G \to G, \quad \sigma \mapsto \sigma^{-1}$$

are continuous maps.

Proof Left to the reader.

Theorem 1.4 Endowed with the Krull topology, $G = \mathrm{Gal}(L/K)$ is compact and totally disconnected (i.e., for every $\sigma \in G$, the connected component of σ is equal to $\{\sigma\}$).

For the proof we note:

Remarks 1.5 (a) Let H be a topological group (see 1.3). Then, for every $\tau \in H$ the left translation by τ

$$L_\tau : H \to H \quad , \quad \sigma \mapsto \tau\sigma$$

is a homeomorphism, and the same holds for the right translation by τ $R_\tau : \sigma \mapsto \sigma\tau$). In fact, $L_\tau = \mu(\tau, -)$ is continuous, with continuous inverse $L_{\tau^{-1}}$. Therefore τ establishes bijections

$$\begin{array}{rcl} U_1 = \{ \text{ neighborhoods of } 1 \ \} & \to & U_2 = \{ \text{ neighborhood of } \tau\} \\ C(1) & \to & C(\tau) \end{array}$$

where $C(\sigma)$ denotes the connected component of an element σ.

(b) If L/K is finite, then the Krull topology on $\mathrm{Gal}(L/K)$ is the discrete topology (since $\{\sigma\}$ is open for every $\sigma \in \mathrm{Gal}(L/K)$, therefore for every subset).

Lemma 1.6 The map

$$\begin{array}{rccc} h: & \mathrm{Gal}(L/K) & \to & \prod\limits_{\substack{K'/K \text{finite, normal} \\ K' \subseteq L}} \mathrm{Gal}(K'/K) \\ & \sigma & \mapsto & (\sigma_{|K'}) \end{array}$$

is injective with closed image

$$\tilde{G} := \{(\sigma_{K'}) \in \textstyle\prod \mathrm{Gal}(K'/K) \mid \text{for } K' \subseteq K'' \text{ we have } \sigma_{K''}|_{K'} = \sigma_{K'}\}\,.$$

Definition 1.7 We call a family $(\sigma_{K'})$ in $\mathrm{Gal}(L/K)$ **compatible**, if it lies in $\tilde{G}$.

The map

$$G \xrightarrow{h} \tilde{G}$$

is a homeomorphism. (Here $\prod \mathrm{Gal}(K'/K)$ carries the product topology with respect to the discrete topologies on the finite groups $\mathrm{Gal}(K'/K)$), and $\tilde{G}$ carries the subgroup topology in this group).

Recollection 1.8 Let $(X_i)_{i\in I}$ be a family of topological spaces. The product topology on

$$X = \prod_{i\in I} X_i$$

is the topology, for which the sets

$$U = \prod_{i\in I} U_i$$

with $U_i \subseteq X_i$ open for all i and $U_i = X_i$ for almost i form a basis (i.e., the open sets are unions of these sets). A subbasis is given by the sets

$$\prod_{\substack{i\in I \\ i\neq j}} X_i \times U_j$$

for $j \in I$ and $U_j \subseteq X_j$ open (i.e., finite intersections of these sets form a basis of the topology).

This product topology is the coarsest topology, for which all projections

$$p_i : X \to X_i$$

are continuous. If Y is a topological space, then a map $f : Y \to \prod_{i\in I} X_i$ is continuous if and only if all component maps $f_i = p_i \circ f : Y \to X_i$ are continuous. This gives the universal property

$$\mathrm{Abb}_{cont}(Y, \prod_{i\in I} X_i) \xrightarrow{\sim} \prod_{i\in I} \mathrm{Abb}_{cont}(Y, X_i)\,,$$

where $\mathrm{Abb}_{cont}(Y, X)$ denotes the set of continuous maps $f : Y \to X$.

Proof of Lemma 1.6: Let $(L_i)_{i\in I}$ be the family of the intermediate fields L_i of L/K with L_i/K finite and Galois. Hence we consider the map

$$h :\ G := \mathrm{Gal}(L/K) \to \prod_{i\in I} \mathrm{Gal}(L_i/K) =: H$$

(a) h is injective: If $\sigma_{|L_i} = id$ for all $i \in I$, then we have $\sigma_{|K'} = id$ for all subfields K' of L/K which are finitely over K (consider the smallest normal field $N(K') \supset K' \supset K$, which is one of the fields of L_i). Thus we have $\sigma = \mathrm{id}$.

(b) $h(G) = \tilde{G}$: The inclusion $h(G) \subseteq \tilde{G}$ is obvious. On the other hand, if (σ_{L_i}) is a compatible family, then we can define $\sigma \in \mathrm{Gal}(L/K)$ by setting $\sigma(x) = \sigma_{L_i}(x)$ for $x \in L_i$ (note that $\bigcup_{i\in I} L_i = L$, see above).

(c) To show that $\tilde{G}$ is closed, we show that the complement of $\tilde{G}$ is open. Let $(\sigma_i) \in \prod_{i\in I} \mathrm{Gal}(L_i/K)$, $(\sigma_i) \notin \tilde{G}$, hence not compatible. Therefore there are $j, k \in I$ with $L_j \subseteq L_k$, but $\sigma_k|_{L_j} \neq \sigma_j$. Then the set

$$\{(\tau_i) \in \prod_{i\in I} \mathrm{Gal}(L_i/K) \mid \tau_j = \sigma_j, \tau_k = \sigma_k\}$$

is an open neighborhood of (σ_i), which lies in the complement of $\tilde{G}$.

(d) h is continuous: The sets

$$U = U_{j,\sigma_j} = \prod_{i\neq j} \mathrm{Gal}(L_i/K) \times \{\sigma_j\}\,,$$

for $j \in I$ and $\sigma_j \in \mathrm{Gal}(L_i/K)$ form a subbasis of the product topology. If σ_j has no inverse image in $\mathrm{Gal}(L/K)$, then $h^{-1}(U)$ is empty, therefore open (later we will see that this case does not occur). If σ is a preimage of σ_j in $\mathrm{Gal}(L/K)$, then $h^{-1}(U) = \sigma \cdot \mathrm{Gal}(L/L_j)$ is open.

(e) h maps open onto the image: $h(\sigma \operatorname{Gal}(L/L_j)) = h(G) \cap U_{j,\sigma_j}$ is open for $\sigma_j = \sigma|_{L_j}$. Therefore h is a homeomorphism and we proved Lemma 1.6.

From this now follows the first claim in Theorem 1.4, since $\prod_{i \in I} \operatorname{Gal}(L_i/K)$ is compact by Tychonov's Theorem (see i.e. Lang 'Real Analysis' II §3 Theorem 3), and $\tilde{G}$ is closed in this. For the second claim it suffices to show that $H = \prod_{i \in I} \operatorname{Gal}(L_i/K)$ is totally disconnected.

For this we show that $Z(1)$, the connected component of 1 in H, is equal to $\{1\}$ (from this and 1.5 it follows that $Z(\sigma) = \sigma$ for all $\sigma \in G$). Obviously, $Z(1)$ lies in every set M which contains the unit and is simultaneously open and closed (from $Z(1) = (Z(1) \cap M) \cup (Z(1) \cap CM)$ it follows that $Z(1) \cap CM = \emptyset$, since $Z(1)$ is connected and $Z(1) \cap M \neq \emptyset$). Hence $Z(1)$ lies in the intersection of all subgroups $U_{j,1} = \prod_{i \neq j} \operatorname{Gal}(L_i/K) \times \{1\}$. But this intersection is $\{1\}$.

Now we obtain

Theorem 1.9 (Main theorem of Galois theory for infinite extensions)

(a) Let L/K be a Galois extension with Galois group $G = \operatorname{Gal}(L/K)$. Then the assignment

$$\Psi : K' \mapsto \operatorname{Gal}(L/K')$$

is a bijective, inclusion-inversing bijection between den intermediate fields of L/K and the *closed* subgroups of G. The inverse map is

$$\Phi : U \mapsto L^U$$

where $L^U = \{x \in L \mid ux = x \text{ for all } u \in U\}$ is the fixed field of U in L.

(b) The open subgroups of G correspond to the intermediate fields $K \subseteq K' \subseteq L$, for which K'/K is finite.

(c) For an intermediate field $K \subseteq K' \subseteq L$, K'/K is normal if and only if $\operatorname{Gal}(L/K')$ is a normal subgroup in $\operatorname{Gal}(L/K)$. In this case one has a canonical isomorphism of topological groups

$$\operatorname{Gal}(L/K)/\operatorname{Gal}(L/K') \xrightarrow{\sim} \operatorname{Gal}(K'/K)\,.$$

We need

Lemma 1.10 If a subgroup U of a topological group H is open, then it is also closed. If U is closed and of finite index, then U is also open.

Proof 1) For every $h \in H$ the coset hU is again open (1.5). Thus

$$H \smallsetminus U = \bigcup_{h \notin U} hU$$

is open.

2) If $\sigma_1, \ldots, \sigma_n$ is a system of representatives for H/U, with $\sigma_1 \in U$, then $H \smallsetminus U = \bigcup_{i=2}^{n} \sigma_i U$ is closed. $\square$

Lemma 1.11 If L/K is Galois and K' is an intermediate field which is again Galois over K is, then the homomorphism

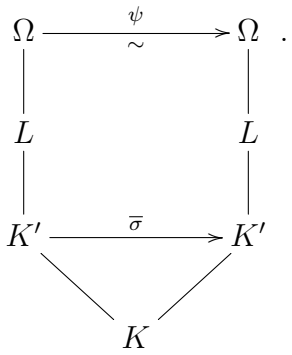
$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \to & \mathrm{Gal}(K'/K) \\ \sigma & \mapsto & \sigma|_{K'} \end{array}$$

is surjective.

Proof Let Ω be an algebraic closure of L and let $\overline{\sigma} \in \mathrm{Gal}(K'/K)$. The K-homomorphism

$$\varphi : K' \xrightarrow{\overline{\sigma}} K' \hookrightarrow L \hookrightarrow \Omega$$

can be extended to an isomorphism $\psi : \Omega \to \Omega$ by standard results of Algebra (see, e.g., my course Algebra I, Lemma 16.9), where we embed K' via $K' \hookrightarrow L \hookrightarrow \Omega$. Therefore we obtain a commutative diagram



Since L/K is normal, we have $\psi(L) \subseteq L$ (If $\alpha \in L$ and p is the minimal polynomial of α over K, then $\psi(\alpha)$ is again a root of p, therefore in L). By considering ψ^{-1} we see that $\sigma = \psi_{|L} : L \to L$ is an isomorphism, therefore we have $\sigma \in \mathrm{Gal}(L/K)$, and by construction we have $\sigma|_{K'} = \overline{\sigma}$.

Proof of Theorem 1.9:

(a): Well-definedness of the correspondence: If K'/K is a finite sub-extension of L/K, then $\mathrm{Gal}(L/K')$ is open by definition, and, by 1.9, also closed. If K'/K is an arbitrary sub-extension, then we have

$$\mathrm{Gal}(L/K') = \bigcap_{\nu} \mathrm{Gal}(L/K_\nu)\,,$$

where K_ν/K runs through the finite sub-extensions of K/K' (every $\alpha \in K$ is contained in the finite sub-extension $K(\alpha)/K$). Therefore, $\mathrm{Gal}(L/K')$ is closed.

Furthermore it is obvious that for intermediate fields $K' \subseteq K''$ of L/K we have the inclusion $\mathrm{Gal}(L/K'') \subseteq \mathrm{Gal}(L/K')$, and that for closed subgroups $U \leq V$ of $\mathrm{Gal}(L/K)$ we have the inclusion $L^V \subseteq L^U$.

(b): Bijectivity of the correspondence:

1) Let K' be an intermediate field, then we have $L^{\mathrm{Gal}(L/K')} = K'$, therefore $\Phi\Psi = id$:

The inclusion "$\supseteq$"is obvious. Assume there is an $\alpha \in L^{\mathrm{Gal}(L/K')}$ with $\alpha \notin K'$. Then there is a finite Galois extension N/K' in L/K' with $\alpha \in N$, and a $\overline{\sigma} \in \mathrm{Gal}(N/K')$ with $\overline{\sigma}\alpha \neq \alpha$ (hence $N^{\mathrm{Gal}(N/K')} = K'$ by classical Galois theory). But by 1.10 there is a $\sigma \in \mathrm{Gal}(L/K')$ with $\sigma|_N = \overline{\sigma}$, therefore $\sigma\alpha \neq \alpha$. Contradiction to the fact that $\alpha \in L^{\mathrm{Gal}(L/K')}$!

2) If $H \leq \mathrm{Gal}(L/K)$ is a closed subgroup, then we have $\mathrm{Gal}(L/L^H) = H$ therefore $\Psi\Phi = id$: We show more generally:

Lemma 1.12 If $H \leq \mathrm{Gal}(L/K)$ is an arbitrary subgroup and if $\overline{H}$ is its closure, then we have $\overline{H} = \mathrm{Gal}(L/L^H)$.

Proof Let again $(L_i)_{i\in I}$ be the family of the intermediate fields of L/K with L_i/K finite Galois. Let $f_i : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L_i/K)$ be the restriction map and $H_i = f_i(H)$. Since $L = \bigcup_{i\in I} L_i$, $\sigma \in \mathrm{Gal}(L/K)$ lies in $\mathrm{Gal}(L/L^H)$ if and only if $\sigma|_{L_i}$ for all $i \in I$ operates trivially on $L_i^H = L_i^{H_i}$. By finite Galois theory this holds if and only if $\sigma|_{L_i} \in H_i$, since $\mathrm{Gal}(L_i/L_i^{H_i}) = H_i$.

Therefore we have $\sigma \in \mathrm{Gal}(L/L^H)$

$\Leftrightarrow$ for all $i \in I$ if we have $f_i(\sigma) \in H_i$

$\Leftrightarrow$ for all $i \in I$ there is a $\tau_i \in H$ with $f_i(\tau_i) = f_i(\sigma)$

$\Leftrightarrow$ for all $i \in I$ there is a $\tau_i \in H$ with $\tau_i \in f_i^{-1}(f_i(\sigma)) = \sigma\ \mathrm{Gal}(L/L_i)$

$\Leftrightarrow$ for all $i \in I$, $\sigma\ \mathrm{Gal}(L/L_i) \cap H \neq \emptyset$

$\Leftrightarrow \sigma \in \overline{H}$,

since the sets $\sigma\ \mathrm{Gal}(L/L_i)$ form a basis of neighborhoods for σ (if K'/K is an intermediate field of L/K and $N(K')/K$ is the normal closure, then we have $\mathrm{Gal}(L/N(K')) \subseteq \mathrm{Gal}(L/K')$).

b) We show that the open subgroups $U \leq \mathrm{Gal}(L/K)$ correspond to the finite intermediate extensions:

If K'/K is a finite extension, $K' \subset L$, then, by definition the Krull topology $\mathrm{Gal}(L/K')$ is open. If conversely $U \leq \mathrm{Gal}(L/K)$ is an open subgroup, then there is an intermediate field $K \subseteq K' \subset L$ with K'/K finite, so that $\mathrm{Gal}(L/K') \subseteq U$. This follows since

$$K \subseteq L^U \subseteq L^{\mathrm{Gal}(L/K')} = K'$$

and from the finiteness of L^U/K.

c) If K'/K is an intermediate field of L/K and $\sigma \in \mathrm{Gal}(L/K)$, then obviously we have

$$\mathrm{Gal}(L/\sigma(K')) = \sigma\ \mathrm{Gal}(L/K)\sigma^{-1}\,.$$

If K'/K is normal, then we have $\sigma(K') = K'$, therefore $\mathrm{Gal}(L/\sigma(K')) = \mathrm{Gal}(L/K')$ for all σ, therefore this is a normal subgroup. Conversely, if $\mathrm{Gal}(L/K')$ is a normal subgroup, the Galois correspondence implies that $\sigma(K') = K'$ for all $\sigma \in \mathrm{Gal}(L/K)$. From this follows that K'/K is normal: If $\alpha \in K'$ and $\tilde{\alpha}$ is a conjugate of α in an algebraic closure $\overline{L}$ of L, i.e., another zero of the minimal polynomial of α over K, then, by Algebra I, Theorem 16.15, there is a K-embedding $\psi : L \to \overline{L}$ with $\psi(\alpha) = \tilde{\alpha}$. Since L/K is Galois, we have $\psi(L) \subseteq L$ and $\sigma = \psi|_L \in \mathrm{Gal}(L/K)$. Since $\sigma(K') = K'$ we have $\tilde{\alpha} \in K$!

By 1.11 we further have that

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(K'/K)$$

is surjective with kernel $\mathrm{Gal}(L/K')$. Hence the homomorphism theorem gives the isomorphism

$$\mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/K') \xrightarrow{\sim} \mathrm{Gal}(K'/K)\,.$$

Now we have to consider the topology. On the right hand side, we take the Krull topology. On the left hand side, we consider the quotient topology (with respect to the Krull topology on $\mathrm{Gal}(L/K)$ and the surjection $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(L/K)/\,\mathrm{Gal}(L/K')$).

Quite generally, if $f : X \to Y$ is a map, where X is a topological space, then there is a finest topology on Y, for which f is continuous: Define

$$V \subseteq Y \text{ open} \quad :\Leftrightarrow \quad f^{-1}(V) \subseteq X \text{ open}\,.$$

This topology is called the final topology with respect to f. If f is surjective, then this is called the quotient topology.

It now follows that, with these topologies, the above group homomorphism is a homeomorphism.

Exercise!

2 Projective and inductive limits

To describe Galois groups in a conceptual way, we introduce projective limits, which are also important in other fields of mathematics. The dual term (in the sense of category theory) is that of inductive limits.

Definition 2.1 A (partially) ordered set $(I, \leq)$ is called filtered (or directed, or inductively ordered), if the following holds:

For two elements $i, j \in I$ there is a $k \in I$ with $i \leq k$ and $j \leq k$.

Examples 2.2 (a) Every totally ordered set is filtered, for example $(\mathbb{N}, \leq)$.

(b) The power set $\mathfrak{P}(M)$ of a set M is filtered with respect to the inclusion $\subseteq$.

(c) Let L/K be a field extension. The set of all intermediate fields K' is filtered with respect to the inclusion.

(d) The same holds for all finite partial extensions K'/K, and as well for all finite normal partial extensions K''/K.

(e) $\mathbb{N}$ with the partial order $|$ is filtered.

Definition 2.3 Let be I a filtered ordered set. An inductive (respectively, projective) system of sets over I is a family

$$((X_i)_{i\in I}, (\alpha_{ij})_{i\leq j}) \quad (\text{resp. } ((X_i)_{i\in I}, (\beta_{ji})_{i\leq j}))$$

of sets X_i (for $i \in I$) and maps

$$\begin{array}{rcccl} & \alpha_{ij} & : & X_i & \to & X_j \quad (\text{for } i \leq j \text{ in } I) \\ (\text{resp.} & \beta_{ji} & : & X_j & \to & X_i \quad (\text{for } i \leq j \text{ in } I)) \end{array}$$

so that we have

$$\begin{array}{rcl} \alpha_{jk} \circ \alpha_{ij} & = & \alpha_{ik} \quad \text{for } i \leq j \leq k \\ (\text{resp.} \quad \beta_{ji} \circ \beta_{kj} & = & \beta_{ki} \quad \text{for } i \leq j \leq k)\,. \end{array}$$

The maps α_{ij} (β_{ji}, resp.) are called the transition maps of the system.

Therefore one obtains the term of the projective system from an inductive system by "reversing of the arrows". One has also projective and inductive systems of groups (the X_i are groups and the transition maps are homomorphisms) or rings (...) or topological spaces (....).

Examples 2.4 (a) Let R be a ring and let $\mathfrak{a} \subseteq R$ be an ideal. Then one obtains a projective system of rings over $(\mathbb{N}, \leq)$ by

$$\begin{array}{rcl} n & \mapsto & R/\mathfrak{a}^n \\ m \leq n & \mapsto & R/\mathfrak{a}^n \quad \to \quad R/\mathfrak{a}^m\,. \end{array}$$

In particular, one has the projective system

$$(\mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}$$

with transition maps

$$\ldots \to \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z} \to \ldots \to \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}\,.$$

(b) One obtains a **projective** system of abelian groups over $(\mathbb{N}, |)$ by

$$\begin{array}{rcl} n & \mapsto & \mathbb{Z}/n\mathbb{Z} \\ m \mid n & \mapsto & \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/m\mathbb{Z}\,. \end{array}$$

(c) One obtains an **inductive** system over $(\mathbb{N}, |)$ by

$$\begin{array}{rcccl} n & \mapsto & \mathbb{Z}/n\mathbb{Z} & & \\ m \mid n & \mapsto & \mathbb{Z}/m & \to & \mathbb{Z}/n\mathbb{Z} \\ & & \overline{a} & \mapsto & \frac{n}{m}\cdot\overline{a}\,. \end{array}$$

(d) Let L/K be a Galois extension. Then the set $\mathcal{K} = \mathcal{K}_{L/K}$ of the finite Galois field extensions K'/K is inductively ordered (2.2 (d)), and we obtain a projective system of finite groups over $\mathcal{K}$ by

$$\begin{array}{rcl} K' & \hookrightarrow & \mathrm{Gal}(K'/K) \\ K' \subseteq K'' & \mapsto & \mathrm{Gal}(K''/K) \twoheadrightarrow \mathrm{Gal}(K'/K)\,. \end{array}$$

Definition 2.5 (a) The projective limit $X = \varprojlim_{i\in I} X_i$ of a projective system (X_i, β_{ji}) of sets is defined as the set

$$\varprojlim_{i\in I} X_i \;:=\; \{(x_i) \in \prod_{i\in I} X_i \mid \beta_{ji}(x_j) = x_i \text{ for all } i \le j\}$$

of the **compatible families** in the product $\prod_{i\in I} X_i$.

(b) The inductive limit $\varinjlim_{i\in I} X_i$ of an inductive system (X_i, α_{ij}) of sets is defined as the quotient

$$\varinjlim_{i\in I} X_i \;:=\; \coprod_{i\in I} X_i/\sim$$

of the disjoint union $\coprod_{i\in I} X_i$ of the sets X_i by the following equivalence relation $\sim$: for $x_i \in X_i$ and $x_j \in X_j$ we have

$$x_i \sim x_j \;:\Leftrightarrow\; \exists\, k \in I,\; i,j \le k \text{ with } \alpha_{ik}(x_i) = \alpha_{jk}(x_j) \text{ in } X_k\,.$$

If the X_i have additional structures, then this usually carries over to the limits. E.g., if one has i.e. a projective (resp. inductive) system of groups, then the projective (resp. inductive) limit is again a group. This also holds for rings etc.

Examples 2.6 (compare 2.4) (a) Let R be a ring and let $\mathfrak{a}$ be an ideal. Then

$$\hat{R} := \varprojlim_n R/\mathfrak{a}^n$$

is called the $\mathfrak{a}$-adic completion of R and is a ring. The elements of $\hat{R}$ are compatible families $(\overline{a}_n)_{n\in\mathbb{N}}$ with $\overline{a}_n \in R/\mathfrak{a}^n$.

Compatibility means that for representatives a_n of $\overline{a}_n$ we have:

$$a_{n+1} \equiv a_n \mod \mathfrak{a}^n\,.$$

One has a ring homomorphism

$$\begin{array}{rccc} \varphi & : & R & \to & \hat{R} \\ & & a & \mapsto & (\overline{a})_{n\in\mathbb{N}}\,, \end{array}$$

which is in general neither injective nor surjective. Obviously we have

$$\ker\varphi = \bigcap_{n\geq 1} \mathfrak{a}^n\,.$$

For example, let $R = \mathbb{Z}$ and let $\mathfrak{a} = (p)$ be the principal ideal generated by a prime number p. Then

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

is called the **p-adic completion** of $\mathbb{Z}$. The map $\varphi : \mathbb{Z} \to \mathbb{Z}_p$ is injective, since we obviously have $\bigcap\limits_{n\geq 1}(p^n) = 0$. Every element $\overline{\alpha} \in \mathbb{Z}/p^n\mathbb{Z}$ will be represented by a uniquely determined element $\alpha \in \mathbb{Z}$ with $0 \leq \alpha < p^n$, and this can again be written in a unique way by

$$\alpha = \sum_{i=0}^{n-1} q_i\, p^i$$

with numbers $0 \leq q_i \leq p-1$ (p-adic expansion). Thus, every element $\alpha \in \mathbb{Z}_p$ can be written in a unique way as a formal series

$$(*) \qquad \alpha = \sum_{i=0}^{\infty} a_i\, p^i \quad (a_i \in \mathbb{Z}, 0 \leq a_i \leq p-1)$$

If we set

$$\alpha_n = \sum_{i=0}^{n-1} a_i\, p^i \in \mathbb{Z} \quad (n \geq 1)\,,$$

then $(*)$ means the compatible family

$$(\alpha_n \bmod (p^n))_{n\geq 1}\,.$$

This shows that there are uncountably many elements in $\mathbb{Z}_p$ (the set of the families $(a_i)_{i\geq 0}$ with $a_i \in \{0,\ldots,p-1\}$ is uncountable). In particular, $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ is not surjective. $\mathbb{Z}_p$ is also called the ring of the **(integral) p-adic numbers**.

(b) Define $\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}$. Here, the projective limit is over $(\mathbb{N}, |)$, indexed as in 2.4 (b). If $n \in \mathbb{N}$ and

$$n = p_1^{n_1} \dots p_r^{n_r}$$

is the the prime factor decomposition, then one has a canonical decomposition

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/p_1^{m_1}\mathbb{Z} \times \dots \times \mathbb{Z}/p_r^{m_r}\mathbb{Z} \tag{2.6.1}$$

(Chinese residue theorem). This is compatible with the transition maps: For $m \mid n$ we have

$$m = p_1^{m_1} \dots p_r^{m_r}$$

with $m_i \le n_i \quad (i = 1, \dots, r)$, and the diagram

$$\begin{array}{ccccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/p_1^{m_1}\mathbb{Z} & \times \cdots \times & \mathbb{Z}/p_r^{n_r}\mathbb{Z} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\sim} & \mathbb{Z}/p^{m_1}\mathbb{Z} & \times \cdots \times & \mathbb{Z}/p_r^{m_r}\mathbb{Z} \end{array} \tag{2.6.2}$$

is commutative. This gives a canonical ring isomorphism

$$\hat{\mathbb{Z}} \xrightarrow{\sim} \prod_p \mathbb{Z}_p \,,$$

where the product on the right hand side runs over all prime numbers. (For this it is best to write formally $n = \prod_p p^{n_p}$, where the product runs over all prime numbers and $n_p = 0$ for nearly all p, and to write the right hand side of (2.6.1) as

$$\prod_p \mathbb{Z}/p^{n_p}\mathbb{Z} \,,$$

correspondingly for (2.6.2)).

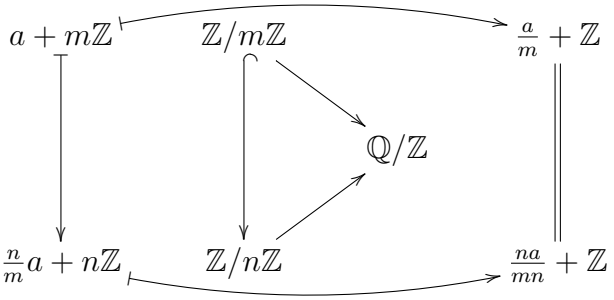
(c) For the inductive system $(\mathbb{Z}/n\mathbb{Z})_{n\in\mathbb{N}}$ of 2.4 (c) one obtains an isomorphism of abelian groups

$$\varinjlim_n \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z} \,,$$

which maps $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ to the residue class of $\frac{a}{n} \mod \mathbb{Z}$: For every fixed $n \in \mathbb{N}$, the map

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \hookrightarrow & \mathbb{Q}/\mathbb{Z} \\ a + n\mathbb{Z} & \mapsto & \frac{a}{n} + \mathbb{Z} \end{array}$$

is a well-defined, injective group homomorphism. This is compatible with the transition maps: For $m \mid n$ the diagram



is commutative. This implies the claim – exercise!

The group $\mathbb{Q}/\mathbb{Z}$ is also called the "Prüfer group". This is also isomorphic to the group $\mu(\mathbb{C})$ of all unit roots in $\mathbb{C}^\times$, via the map

$$\begin{array}{rcl} \mathbb{Q}/\mathbb{Z} & \xrightarrow{\sim} & \mu(\mathbb{C}) \\ \frac{p}{q}+\mathbb{Z} & \mapsto & e^{2\pi i \frac{p}{q}}\,. \end{array}$$

(d) If L/K is a Galois extension, then, by Lemma 1.6

$$\mathrm{Gal}(L/K) \xrightarrow{\sim} \varprojlim_{K'\in\mathcal{K}_{L/K}} \mathrm{Gal}(K'/K) \tag{2.6.3}$$

where $\mathcal{K}_{L/K}$ is the directed set of the finite normal sub-extensions K'/K of L/K.

(e) If $(X_i)_{i\in I}$ is a projective system of topological spaces, then

$$\varprojlim_{i\in I} X_i \;\subseteq\; \prod_{i\in I} X_i$$

is equipped with the subspace topology, with respect to the product topology on the product on the right hand side.

(f) If one applies this on the examples (a), (b) and (d), with respect to the discrete topologies on $R/\mathfrak{a}^n$, $\mathbb{Z}/n\mathbb{Z}$ resp., $\mathrm{Gal}(K'/K)$ resp., then one obtains topologies on $\hat{R} = \varprojlim R/\mathfrak{a}^n$, $\mathbb{Z}_p$, $\hat{\mathbb{Z}}$ and $\varprojlim \mathrm{Gal}(K'/K)$.

Furthermore one can easily see that, by this, one obtains topological groups, and for $\hat{R}$, $\mathbb{Z}_p$ and $\hat{\mathbb{Z}}$ one even obtains topological rings (the multiplication is again continuous). From Lemma 1.6 we get that the isomorphism (2.6.3) is also a homeomorphism, therefore an isomorphism of topological groups.

Now we can describe the absolute Galois group

$$G_{\mathbb{F}_q} = \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$$

of a finite field $\mathbb{F}_q$ with q elements.

Theorem 2.7 There is a canonical isomorphism of topological groups

$$\hat{\mathbb{Z}} \;\xrightarrow{\sim}\; G_{\mathbb{F}_q}\,.$$

Proof For every natural number n there is exactly one extension of degree n over $\mathbb{F}_q$, to wit: $\mathbb{F}_{q^n}$. This is Galois, and there is a canonical isomorphism

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \\ 1 \mod n\mathbb{Z} & \mapsto & Fr_q\,, \end{array}$$

where Fr_q is the Frobenius automorphism, given by

$$Fr_q(x) = x^q \quad (\text{for all } x \in \mathbb{F}_{q^n}).$$

This is compatible with the transition maps: One has $\mathbb{F}_{q^m} \subseteq \mathbb{F}_{q^n}$ if and only if $m \mid n$, and then the diagram

$$\begin{array}{ccccc} 1 & & \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) & & Fr_q \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ 1 & & \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q) & & Fr_q \end{array}$$

is commutative. The projective system $(\mathrm{Gal}(K'/\mathbb{F}_q))_{K' \in K_{\overline{\mathbb{F}}_q/\mathbb{F}_q}}$ therefore can be identified with the projective system $(\mathbb{Z}/n\mathbb{Z})_{n \in (\mathbb{N},|)}$ from 2.4 (b); accordingly one obtains an isomorphism

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z} \to \varprojlim_n \mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \varprojlim_{K'} \mathrm{Gal}(K'/\mathbb{F}_q)$$

of the projective limits, which maps a compatible family $(\overline{a}_n)_n$ on the left hand side to the compatible family $(Fr^{a_n}_{\mathbb{F}_{q^n}/\mathbb{F}_q})_n$ on the right hand side. The claim of the theorem now follows with 20.6 (d), (e) and (f).

Remark 2.8 We have the map

$$\begin{array}{ccccc} \mathbb{Z} & \to & \hat{\mathbb{Z}} & \xrightarrow{\sim} & \mathrm{Gal}(\overline{\mathbb{F}}_q, \mathbb{F}_q), \\ 1 & \mapsto & 1 & \mapsto & Fr_q \end{array}$$

where Fr_q is the Frobenius automorphism of $\overline{\mathbb{F}}_q$: $Fr_q(x) = x^q$. The first homomorphism is injective, but not surjective, since not even one of the compositions

$$\mathbb{Z} \to \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \to \mathbb{Z}_p$$

is surjective (20.6(a)). But we have that $\mathbb{Z}$ is dense in $\hat{\mathbb{Z}}$ (and thus dense in $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$) (Proof: left to the reader).

3 Cohomology of groups and pro-finite groups

The following definition is formulated in a parallel way for the case that topologies on G and A are given, and one considers continuous maps, or that there is no topology (equivalent: the topology is discrete, so that all maps are continuous).

Definition 3.1 Let G be a (topological) group and let A be a (continuous) G**-module**, i.e., an abelian group A together with a (continuous) composition

$$\begin{array}{rccc} \mu: & G \times A & \to & A \\ & (\sigma, a) & \mapsto & \sigma a \end{array}$$

for which we have

$$\begin{array}{rcl} \sigma(a+b) & = & \sigma a + \sigma b \\ \sigma_1(\sigma_2 a) & = & (\sigma_1\sigma_2)a \\ 1a & = & a \end{array}$$

for all $a, b \in A, \sigma, \sigma_1, \sigma_2 \in G$ and the unit element $1 \in G$. For $n \in \mathbb{N}_0$ define the group of the continuous n-**cochains** on G with coefficients in A by

$$X^n = X^n(G, A) = \{\text{continuous maps } x : G^{n+1} \to A\}.$$

X^n is in a natural way a continuous G-module by

$$(\sigma x)(\sigma_0, ..., \sigma_n) = \sigma x(\sigma^{-1}\sigma_0, \sigma^{-1}\sigma_1, ..., \sigma^{-1}\sigma_n).$$

The maps

$$d_i : X^{n+1} \longrightarrow X^n$$

given by

$$d_i x(\sigma_0, \sigma_1, ..., \sigma_n) = x(\sigma_0, ..., \hat{\sigma_i}, .., \sigma_n),$$

(where $\hat{\sigma_i}$ indicates that we have omitted σ_i from the $(n+1)$-tuple $(\sigma_0, ..., \sigma_n)$) induce G-homomorphisms $d_i^* : X^{n-1} \longrightarrow X^n$, and we form the alternating sum

$$\partial^n = \sum_{i=0}^{n} (-1)^i d_i^* : X^{n-1} \longrightarrow X^n.$$

We often just write ∂ instead of ∂^n. Hence, for $x \in X^{n-1}$, ∂x is the function

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

Moreover, we have a G-module homomorphism $\delta^0 : A \longrightarrow X$, which associates to $a \in A$ the constant function $x(\sigma_0) = a$,

Proposition 3.2 The sequence

$$0 \longrightarrow A \xrightarrow{\partial^0} X^0 \xrightarrow{\partial^1} X^1 \xrightarrow{\partial^2} X^2 \longrightarrow \dots$$

is exact, i.e., one has $\operatorname{im} \partial^n = \ker \partial^{n+1}$ at all places.

Proof We first show that the sequence is a complex, i.e., that $\partial\partial = 0$. It is clear that $\partial^1 \circ \partial^0 = 0$. Now let $x \in X^{n-1}$. Applying ∂ to 3.1, we get summands of the form $x(\sigma_0, ..., \hat{\sigma_j}, ..., \sigma_n)$ with certain signs. Each of these summands arise twice, once where first σ_j and then σ_i is omitted, and again where first σ_i and then σ_j is omitted. The first time the sign is $(-1)^i(-1)^j$, and the second time it is $(-1)^i(-1)^{j-1}$. Hence the summands add up to zero.

For the exactness, we consider the map $D^{-1} : X^0 \to A, D^{-1}x = x(1)$, and for $n \geq 0$ the maps

$$D^n : X^{n+1} \longrightarrow X^n, \ \ (D^n x)(\sigma_0, \ldots, \sigma_n) = x(1, \sigma_0, \ldots, \sigma_n).$$

These are homomorphisms of $\mathbb{Z}$-modules, and not of G-modules. An easy calculation shows that for $n \geq 0$ we have

$$D^n \circ \partial^{n+1} + \partial^n \circ D^{n-1} = id. \tag{3.2.1}$$

If $x \in \ker(\partial^{n+1})$, then $x = \partial^n D^{n-1} x$, i.e., $\mathrm{im}(\partial^n) \subseteq \ker(\partial^{n+1})$ and thus $\ker(\partial^{n+1}) = \mathrm{im}(\partial^n)$, because $\partial^{n+1} \circ \partial^n = 0$.

An exact sequence of G-modules $0 \to A \to X^0 \to X^1 \to X^2 \to \ldots$ is called a resolution of A, and a family $(D^n)_{n \geq -1}$ as above with the property 3.2.1 is called a **contracting homotopy**. The above resolution is called the **standard resolution** of A (by G-modules).

Now we apply the functor of taking the fixed modules under G. For any G-module A this is the module

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

Therefore we define, for $n \geq 0$,

Definition 3.3 Let

$$C^n(G, A) = X^n(G, A)^G.$$

$C^n(G, A)$ consists of the continuous functions $x : G^{n+1} \to A$ such that

$$x(\sigma\sigma_0, \ldots, \sigma\sigma_n) = \sigma x(\sigma_0, \ldots, \sigma_n)$$

for all $\sigma \in G$. These functions are called the homogeneous n-**cochains** of G with coefficients in A. From the standard resolution 3.2.1 we obtain a sequence

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

which is no longer exact. But it is still a complex, i.e., we have $\partial\partial = 0$, and this complex is called the **homogeneous cochain complex** of G with coefficients in A. We set

$$Z^n(G, A) = \ker(C^n(G, A) \xrightarrow{\partial^{n+1}} C^{n+1}(G, A)), B^n(G, A) = \mathrm{im}(C^{n-1} \xrightarrow{\partial^n} C^n(G, A))$$

and define

Definition 3.4 For $n \geq 0$ the cohomology groups of the complex $C^\bullet(G, A)$,

$$H^n(G, A) = Z^n(G, A)/B^n(G, A)$$

are called the n-th cohomology groups of G with coefficients in A.

For computational purposes, and for many applications, it is useful to pass to a modified definition of the cohomology groups, which reduces the number of variables in the homogeneous cochains $x(\sigma_0, \ldots, \sigma_n)$ by one. Let $\mathcal{C}^0(G, A) = A$ and $\mathcal{C}^n(G, A)$, for $n \geq 1$, be the abelian group of all continuous functions $y : G^n \longrightarrow A$. Then we have the isomorphism

$$C^0(G, A) \longrightarrow \mathcal{C}^0(G, A), x(\sigma) \mapsto x(1),$$

and for $n \geq 1$ the isomorphisms

$$C^n(G, A) \longrightarrow \mathcal{C}^n(G, A), x(\sigma_0, \ldots, \sigma_n) \mapsto y(\sigma_1, \ldots, \sigma_n) = x(1, \sigma_1, \sigma_1\sigma_2, \ldots, \sigma_1 \ldots \sigma_n),$$

whose inverse is given by

$$y(\sigma_1, \ldots, \sigma_n) \mapsto x(\sigma_0, \ldots, \sigma_n) = \sigma_0 y(\sigma_0^{-1}\sigma_1, \sigma_1^{-1}\sigma_2, \ldots, \sigma_{n-1}^{-1}\sigma_n).$$

With these isomorphisms the coboundary operators $\partial^{n+1} : C^n(G, A) \longrightarrow C^{n+1}(G, A)$ are transformed into the homomorphisms $\partial^{n+1} : \mathcal{C}^n(G, A) \longrightarrow \mathcal{C}^{n+1}(G, A)$ given by

$$\begin{aligned}
\partial^1(a)(\sigma) &= \sigma a - a, \text{ for a } \in A = \mathcal{C}^0 \\
\partial^2(f)(\sigma_1, \sigma_2) &= \sigma_1 f(\sigma_2) - f(\sigma_1\sigma_2) + f(\sigma_1), \\
\partial^{n+1}(f)(\sigma_1, \ldots, \sigma_{n+1}) &= \sigma_1 f(\sigma_2, \ldots, \sigma_n) \\
&\quad + \sum_{i=1}^{n} (-1)^i f(\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}, \sigma_{i+2}, \ldots, \sigma_{n+1}) \\
&\quad + (-1)^{n+1} f(\sigma_1, \ldots, \sigma_n) \text{ for } n \geq 1
\end{aligned}$$

Setting

$$\mathcal{Z}^n(G, A) = \ker(\mathcal{C}^n(G, A) \xrightarrow{\partial^{n+1}} \mathcal{C}^{n+1}(G, A)),$$

$$\mathcal{B}^n(G, A) = \mathrm{im}(\mathcal{C}^{n-1}(G, A) \xrightarrow{\partial^n} \mathcal{C}^n(G, A)),$$

the isomorphisms $C^n(G, A) \to \mathcal{C}^n(G, A)$ induce isomorphisms

$$H^n(G, A) \cong \mathcal{Z}^n(G, A)/\mathcal{B}^n(G, A).$$

The functions in $\mathcal{C}^n(G, A)$, $\mathcal{Z}^n(G, A)$ and $\mathcal{B}^n(G, A)$ are called the inhomogeneous $n-$ **cochains**, $n-$ **cocycles**, and $n-$ **coboundaries**, respectively.

We now consider the cohomology groups in small dimensions, $n = 0, 1, 2$.

$\mathbf{H^0(G, A)}$:

Lemma 3.5 There is a canonical isomorphism

$$H^0(G, A) \cong A^G,$$

where $A^G = \{a \in A \mid \sigma a = a \text{ for all } \sigma \in G\}$ denotes the **fixed module** of A under G.

Proof We have $H^0(G, A) = \ker \partial^0$, and ∂^0 is the map

$$\begin{array}{ccc} A & \xrightarrow{\partial^0} & \mathcal{C}^1(G, A) \\ a & \mapsto & f : G \to A \text{ with } f(\sigma) = \sigma a - a. \end{array}$$

Therefore we have $\ker \partial^0 = A^G$.

$\mathbf{H^1(G, A)}$:

$Z^1(G, A)$ is the group of the (continuous) maps $f : G \to A$ with

$$f(\sigma\tau) = f(\sigma) + \sigma f(\tau).$$

These are also called **crossed homomorphisms**. The group $B^1(G, A)$ of the $1-$ *coboundaries* is the group of maps $f : G \to A$ of the form

$$f(\sigma) = \sigma a - a$$

for a fixed $a \in A$. We immediately see:

Lemma 3.6 If G operates trivially on A (i.e., if $\sigma a = a$ for all $\sigma \in G, a \in A$), then

$$H^1(G, A) = Hom(G, A) \qquad , \qquad (\text{respectively}, Hom_{cont}(G, A))$$

is the group of homomorphisms from G to A (respectively, the continuous homomorphisms, if we have topologies on the group).

$\mathbf{H^2(G, A)}$:

$Z^2(G, A)$ is the group of (continuous) maps $f : G \times G \to A$ with

$$f(\sigma\tau, \rho) + f(\sigma, \tau) = f(\sigma, \tau\rho) + \sigma f(\tau, \rho).$$

These are also called **factor systems**. The 2-coboundaries are the functions of the form

$$f(\sigma, \tau) = g(\sigma) - g(\sigma\tau) + \sigma g(\tau)$$

for an arbitrary (continuous) map $g : G \to A$.

The factor systems are related to group extensions. We only describe this for groups without topology.

Definition 3.7 Let G and A be groups (not necessarily commutative). A **group extension** of G by A is an exact sequence

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1,$$

i.e., ι and π are group homomorphisms, ι is injective, π is surjective, and we have $\operatorname{im}\iota = \ker\pi$. In other words, E is a group which contains A as a normal subgroup, such that we have an isomorphism $E/A \xrightarrow{\sim} G$.

Lemma 3.8 Assume that A is abelian. Then A becomes a G-module by defining, for $a \in A$ and $g \in G$

$$g(a) = \hat{g}a\hat{(}g)^{-1},$$

where $\hat{g} \in E$ is a lift of g, i.e., a preimage of g under $\pi : E \twoheadrightarrow G$.

Proof Since A is a normal subgroup, we have $g(a) \in A$, and since A is commutative, $g(a)$ is independent of the choice of $\hat{g}$. In fact, if $\tilde{g}$ is another lift of g, then we have $\tilde{g} = \tilde{g}b$ for a $b \in A$ (since $\tilde{g}^{-1} \in \ker\pi = A$), and therefore we have

$$\tilde{g}a\tilde{g}^{-1} = \hat{g}bab^{-1}\hat{g}^{-1} = \hat{g}a\hat{g}^{-1},$$

since A is commutative.

A is a G-module: Obviously we have $1 \cdot a = a$. Moreover for $a, a' \in A$ we have

$$g(a \cdot a') = \hat{g}aa'\hat{g}^{-1} = \hat{g}a\hat{g}^{-1}\hat{g}a'\hat{g}^{-1} = g(a) \cdot g(a')$$

i.e., the operation of G is compatible with the group law of A (which is written multiplicatively here).

Definition 3.9 If

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle g} & & \| & & \\ 1 & \longrightarrow & A & \xrightarrow{\iota'} & E' & \xrightarrow{\pi'} & G & \longrightarrow & 1 \end{array}$$

is a commutative diagram, then the two extensions are called equivalent.

Now we attach a factor system to each group extension.

Let

$$s : G \to E$$

be a section of $\pi : E \to G$, i.e., a map with $\pi s = \mathrm{id}_G$ (This always exists, by the axiom of choice – obvious for finite groups). For $\sigma, \tau \in G$, the elements $s(\sigma) \cdot s(\tau)$ and $s(\sigma\tau)$ are both mapped to $\sigma\tau$ by π; hence they differ by an element in $\ker\pi = A$. Hence there is a unique $f(\sigma, \tau) \in A$ with

$$s(\sigma) \cdot s(\tau) = f(\sigma, \tau) \cdot s(\sigma\tau)\,.$$

Lemma 3.10 (i) The map $f : (\sigma, \tau) \mapsto f(\sigma, \tau)$ is a factor system, i.e., a 2-cocycle.

(ii) The associated cohomology class

$$[f] \in H^2(G, A)$$

is independent of the choice of a section s.

(iii) Two group extensions

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$$
$$1 \to A \xrightarrow{\iota'} E \xrightarrow{\pi'} G \to 1$$

are equivalent if and only if the associated classes $[f]$, $[f']$ in $H^2(G, A)$ are equal.

Exercise!

4 Basics about modules and homological Algebra

Let R be a ring with unit (not necessarily commutative).

Definition 4.1 (a) A (left) R-**module** is an abelian group $(M,+)$ together with a composition

$$\begin{array}{rcl} R\times M & \to & M \\ (r,m) & \mapsto & rm \end{array}$$

so that we have

$$\begin{array}{lrcl} \text{(i)} & r(m+n) & = & rm+rn \\ \text{(ii)} & (r+s)m & = & rm+sn \\ \text{(iii)} & (rs)m & = & r(sm) \\ \text{(iv)} & 1m & = & m \end{array}$$

for all $r,s\in R$ and $m,n\in M$.

(b) Let M and N be R-modules. A map $\varphi : M\to N$ is called a **homomorphism of R-modules** (or R-linear), if the following holds:

(i) $\varphi(m_1+m_2)=\varphi(m_1)+\varphi(m_2)$ for all $m_1,m_2\in M$ (i.e., φ is a group homomorphism of $(M,+)$ to $(N,+)$),

(ii) $\varphi(rm)=r\varphi(m)$ for all $m\in M, r\in R$.

Let $Hom_R(M,N)$ be the abelian group of the R-linear maps from M to N.

Remarks 4.2 (a) A right R-module M is defined similarly, but the property (iii) is replaced by

$$\text{(iii')} \qquad (rs)m = s(rm)\,.$$

If one writes the composition differently, namely

$$\begin{array}{rcl} M\times R & \to & M \\ (m,r) & \mapsto & mr\,, \end{array}$$

then one gets a more plausible relation

$$m(rs)=(mr)s\,.$$

(b) For a commutative ring, left- and right modules are the same.

(c) As usual, one calls an R-linear map $\varphi : M\to N$ a monomorphism (resp. epimorphism, resp. isomorphism), if it is injective (resp. surjective, resp. bijective).

(d) The composition of R-linear maps is again linear. The inverse of a R-module isomorphism is again R-linear.

Examples 4.3 (a) Every abelian group A becomes a $\mathbb{Z}$-module by the definition

$$na = a + \ldots + a \quad (n\text{-times}) \quad \text{for } n \in \mathbb{N}\,,$$

$$\begin{aligned} 0a &= 0 \\ (-n)a &= -(na) \quad \text{for } n \in \mathbb{N}\,. \end{aligned}$$

One can see that abelian groups and $\mathbb{Z}$-modules are the same.

(b) If $(M_i)_{i\in I}$ is a family of R-modules, then the abelian groups

$$\prod_{i\in I} M_i \quad \supseteq \quad \bigoplus_{i\in I} M_i$$

become R-modules by the definition $r(m_i)_{i\in I} := (rm_i)_{i\in I}$.

The first module is called the **direct product** of the R-modules M_i, and the second module is called the **direct sum** of the R-modules M_i.

(c) If K is a field , then a K-module is the same as a K-vectorspace.

Definition 4.4 An R-module M is called a free R-module, if there is a family $(m_i)_{i\in I}$ of elements $m_i \in M$, so that we have: Every element $m \in M$ has a unique representation

$$m = \sum_{i\in I} r_i m_i\,,$$

where $r_i \in R$ and $r_i = 0$ for almost all $i \in I$ (so that the right sum is finite, if we omit the summands with $r_i = 0$). Such a family $(m_I)_{i\in I}$ is called basis of M.

Examples 4.5 (a) Let I be a set. Then the R-module

$$F_R(I) := \bigoplus_{i\in I} R$$

is free with basis $(e_i)_{i\in I}$, where we have $e_i = (\delta_{ji})_{j\in I}$, with the Kronecker symbol

$$\delta_{ij} = \begin{cases} 1 & , \quad j = 1 \\ 0 & , \quad j \neq i \end{cases}$$

(with $0, 1 \in R$). $F_R(I)$ is also called the free R-module over I. Sometimes one identifies e_i with i and one writes the elements as formal linear combinations

$$\sum_{i\in I} r_i i\,,$$

with $r_i \in R, r_i = 0$ for nearly all i.

(b) The $\mathbb{Z}$-module $M = \mathbb{Z}/5\mathbb{Z}$ is not free, since for every $m \in \mathbb{Z}/5\mathbb{Z}$, we have $1 \cdot m = m = 6 \cdot m$. But M is a free module over the ring $\mathbb{Z}/5\mathbb{Z}$.

Lemma 4.6 (Universal property of the free module) Let M be an R-module and let $(m_i)_{i\in I}$ be a family of elements $m_i \in M$. Then there is a unique R-module-homomorphism

$$\varphi : F_R(I) \to M$$

with $\varphi(e_i) = m_i$ for all $i \in I$ (Therefore we have $\mathrm{Hom}_R(F_R(I), M) \xrightarrow{\sim} Abb(I, M)$ via $\varphi \mapsto (\varphi(e_i))_{i\in I}$).

Proof Let $\varphi((r_i)) = \sum\limits_{i\in I} r_i m_i$.

Definition 4.7 M is free with basis $(m_i)_{i\in I}$ if and only if the φ above is an isomorphism.

Definition 4.8 Let M be an R-module. An (R-)submodule of M is a subset $N \subseteq M$, for which we have:

(i) N is subgroup with respect to $+$,

(ii) for all $n \in N$ and $r \in R$ we have $rn \in N$.

Lemma 4.9 If $\varphi : M \to N$ is a homomorphism of R-modules, then $\ker\varphi$ is a submodule of M and $\mathrm{im}\,\varphi$ is a submodule of N.

Proof easy!

Theorem 4.10 If M is an R-module and $N \subseteq M$ is a submodule, then the quotient group

$$M/N$$

becomes an R-module by the definition

$$r(m + N) \;:=\; rm + N \quad \text{for } r \in R, m \in M$$

(Hence $r \cdot \overline{m} = \overline{rm}$, if $\overline{m}$ denotes the coset of $m \in M$). The surjection $\pi : M \to M/N$ is R-linear.

Proof Left to the reader!

Remarks 4.11 The homomorphism theorem and the first and the second isomorphism theorem hold for R-modules:

(a) An R-linear map $\varphi : M \to N$ induces an R-module-isomorphism

$$M/\ker\varphi \xrightarrow{\sim} \mathrm{im}\,\varphi\,.$$

(b) For submodules $N_1, N_2 \subset M$ one has an R-module-isomorphism

$$N_1/(N_1 \cap N_2) \xrightarrow{\sim} (N_1 + N_2)/N_2\,.$$

(c) For submodules $M_3 \subset M_2 \subset M_1$ one has an R-isomorphism

$$(M_1/M_3)/(M_2/M_3) \xrightarrow{\sim} M_1/M_2\,.$$

Now we consider the homological Algebra of R-modules.

Definition 4.12 We define complexes of R-modules again as sequences

$$\ldots \to M^{n-1} \stackrel{\partial^{n-1}}{\to} M^n \stackrel{\partial^n}{\to} M^{n+1} \stackrel{\partial^{n+1}}{\to} M^{n+2} \to \ldots\,,$$

where the M^n are R-modules and the maps ∂^n are linear maps with $\partial^n \partial^{n-1} = 0$. The elements in $\ker \partial^n$ are called the cycles in M^n, and the elements of $\operatorname{im} \partial^{n-1}$ are called the boundaries in M^n. Since $\partial^n \partial^{n-1} = 0$, we have $\operatorname{im} \partial^{n-1} \subseteq \ker \partial^n$. The n-th cohomology of the complex is the R-module

$$H^n(M^{\cdot}) = \ker \partial^n / \operatorname{im} \partial^{n-1}$$

and the complex is called exact at the place n, if $H^n(M^{\cdot}) = 0$, and exact, if it is exact at all places.

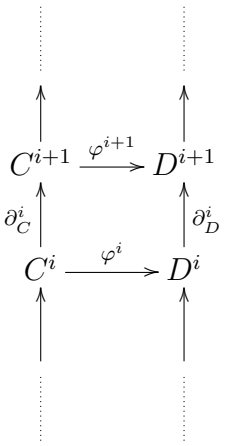
Definition 4.13 Let $C^{\cdot}$ and $D^{\cdot}$ be complexes of R-modules, where R is a ring (for $R = \mathbb{Z}$ we have simply complexes of abelian groups). A morphism of complexes (of R-modules)

$$\varphi : C^{\cdot} \to D^{\cdot}$$

is a collection of homomorphisms of R-modules

$$\varphi^i : C^i \to D^i\,,$$

which are compatible with den differentials, i.e., for which all squares



are commutative, where ∂^i_C and ∂^i_D are the differentials for $C^{\cdot}$ and $D^{\cdot}$), respectively. Therefore we have $\varphi^{i+1}\partial^i_C = \partial^i_D \varphi^i$ (simplified notation, without degrees: $\varphi\partial_C = \partial_D \varphi$).

Lemma 4.14 A morphism of complexes

$$\varphi : C^{\cdot} \to D^{\cdot}$$

induces homomorphisms

$$\varphi^i_* = H^i(\varphi) : H^i(C) \to H^i(D)$$

in the cohomology. For these we have $(\mathrm{id}_C)^i_* = \mathrm{id}_{H^i(C)}$ and $(\psi\varphi)_* = \psi_*\varphi_*$ for another morphism of complexes $\psi : D^{\cdot} \to E^{\cdot}$.

Proof By the compatibility with the differentials the map

$$\varphi^i : C^i \to D^i$$

induces maps

$$\begin{array}{rcl} \ker \partial^i_C & \to & \ker \partial^i_D \\ \mathrm{im}\, \partial^{i-1}_C & \to & \mathrm{im}\, \partial^{i-1}_B \end{array}$$

and thus a well-defined R-linear map

$$\begin{array}{rcl} \varphi^i_* : \quad H^i(C^{\cdot}) & \to & H^i(D^{\cdot}), \\ [a] := a \mod \mathrm{im}\, \partial^{-1}_C & \mapsto & \varphi^i(a) \mod \mathrm{im}\, \partial^{i-1}_D =: [\varphi^i(a)] \end{array}$$

(for $a \in \ker \partial^i_C$). The other claims are obvious.

In the following, $[a]$ denotes the cohomology class of a cycle a.

Definition 4.15 A sequence

$$C^{\cdot} \stackrel{\phi}{\to} D^{\cdot} \stackrel{\Psi}{\to} E^{\cdot}$$

of (morphisms of) complexes is called exact, if the sequence

$$C^i \stackrel{\phi^i}{\to} D^i \stackrel{\psi^i}{\to} E^i$$

is exact for all i.

Theorem 4.16 (long exact cohomology sequence) Let R be a ring and let

$$0 \to C^{\cdot} \stackrel{\phi}{\to} D^{\cdot} \stackrel{\Psi}{\to} E^{\cdot} \to 0$$

be a short exact sequence of complexes of R-modules. Then there are canonical R-module homomorphisms

$$\delta^i : H^i(E^{\cdot}) \to H^{i+1}(C^{\cdot})$$

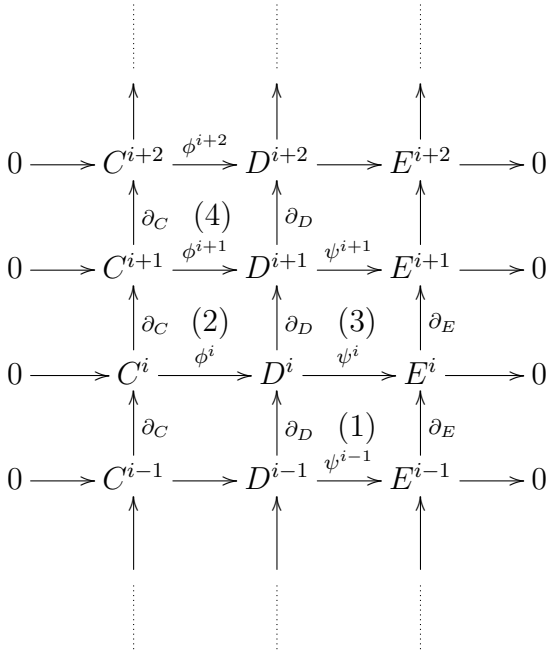
for all i (called connecting homomorphisms), such that the sequence

$$\ldots \to H^{i-1}(E^{\cdot}) \stackrel{\delta^{i-1}}{\to} H^i(C^{\cdot}) \stackrel{\phi^i_*}{\to} H^i(D^{\cdot}) \stackrel{\psi^i_*}{\to} H^i(E^{\cdot}) \stackrel{\delta^i}{\to} H^{i+1}(C^{\cdot}) \to \ldots$$

is exact.

Proof We have a commutative diagram

(4.15.1)



where the rows are short exact sequences.

1) **Exactness at** $H^i(D^\cdot)$: It is obvious that $\psi_*\phi_* = 0$ (since $\psi_*\phi_* = (\psi\phi)_* = 0_* = 0$). Let $[d^i] \in H^i(D^\cdot)$ with $\psi_*[d^i] = 0$. Then $\psi^i d^i$ is a boundary, i.e., there is an $e^{i-1} \in E^{i-1}$ with $\psi^i(d^i) = \partial_E e^{i-1}$. By the surjectivity of ψ^{i-1} there is a $d^{i-1} \in D^{i-1}$ with $\psi^{i-1}d^{i-1} = e^{i-1}$. Then we have

$$\psi^i(d^i - \partial_D d^{i-1}) = \partial_E e^{i-1} - \psi^i \partial_D d^{i-1} = \partial_E \psi^{i-1} d^{i-1} - \psi^i \partial_D d^{i-1} = 0$$

(commutativity of (1)). By the exactness of the i-th row there is a $c^i \in C^i$ with $\phi^i c^i = d^i - \partial_D d^{i-1}$. For this c_i we have

$$\phi^{i+1}\partial_C c^i = \partial_D \phi^i c^i = \partial_D d^i - \partial_D \partial_D d^{i-1} = 0$$

by the commutativity of (2), since $\partial_D \partial_D = 0$ and since d^i is a cycle. Since ϕ^{i+1} is injective, we get $\partial_C c^i = 0$, i.e., c^i is a cycle. Then we have

$$[d^i] = [d^i - \partial_D d^{i-1}] = [\phi^i c^i] = \phi^i_*[c^i] \in \operatorname{im} \phi^i_* \,.$$

2) **Definition of** δ^i: Let $[e^i] \in H^i(E^\cdot)$, i.e., let $e^i \in E^i$ with $\partial_E e^i = 0$. By the surjectivity of ψ^i there is a $d^i \in D^i$ with $\psi^i d^i = e^i$. Consider

$$\partial_D d^i \in D^{i+1} \,.$$

We have

$$\begin{aligned} \psi^{i+1}\partial_D d^i &= \partial_E \psi^i d^i \quad \text{commutativity of (3))} \\ &= \partial_E e^i = 0 \quad \text{(assumption)} \,. \end{aligned}$$

Hence, by the exactness of the $i+1$-th row, there is a $c^{i+1} \in C^{i+1}$ with $\phi^{i+1}c^{i+1} = \partial_D d^i$. For this element we have

$$\phi^{i+2}\partial_C c^{i+1} = \partial_D \phi^{i+1} c^{i+1} = \partial_D \partial_D d^i = 0$$

(commutativity of (4) and $\partial_D \partial_D = 0$), and we see that $\partial_C c^{i+1} = 0$, since ϕ^{i+2} is injective. Therefore c^{i+1} is a cycle. We set

$$\delta([e^i]) = [c^{i+1}] \in H^{i+1}(C^\cdot)\,. \tag{4.15.2}$$

Conclusion: The definition of δ^i can be visualized as:

$$\begin{array}{ccc} c^{i+1} & \overset{\phi^{i+1}}{\longmapsto} & \partial_D d^i \\ & & \uparrow{\scriptstyle \partial_D} \\ & & d^i \overset{\psi^i}{\longmapsto} e^i \end{array}$$

Well-definedness: Let $\widetilde{e^i} \in E^i$ be another cycle with $[\widetilde{e^i}] = [e^i]$, let $\widetilde{d^i} \in D^i$ with $\phi^i \widetilde{d^i} = \widetilde{e^i}$, and let $\widetilde{c^{i+1}} \in C^{i+1}$ with $\phi^{i+1}\widetilde{c^{i+1}} = \partial_D \widetilde{d^i})$ be chosen as above. We have to show that $[\widetilde{c^{i+1}}] = [c^{i+1}] \in H^{i+1}(C^\cdot)$.

By assumption, there is an $e^{i-1} \in E^{i-1}$ with

$$\widetilde{e^i} = e^i + \partial_E e^{i-1}\,,$$

and by the surjectivity of ψ^{i-1} there is a $d^{i-1} \in D^{i-1}$ with $\psi^{i-1}d^{i-1} = e^{i-1}$. We calculate

$$\begin{aligned} \psi^i(\widetilde{d^i} - d^i - \partial_D d^{i+1}) &= \widetilde{e^i} - e^i - \psi^i \partial_D d^{i-1} \\ &= \widetilde{e^i} - e^i - \partial_E \psi^{i-1} d^{i-1} \qquad \text{(commutativity of (1))} \\ &= \widetilde{e^i} - e^i - \partial_E e^{i-1} = 0\,. \end{aligned}$$

By the exactness of the i-th row there is a $c^i \in C^i$ with $\phi^i c^i = \widetilde{d^i} - d^i - \partial_D d^{i-1}$. We claim that

$$\widetilde{c^{i+1}} = c^{i+1} + \partial_C c^i\,, \tag{4.15.3}$$

which implies $[\widetilde{c^{i+1}}] = [c^{i+1}]$ as wished. But we have

$$\begin{aligned} \phi^{i+1}(\widetilde{c^{i+1}} - c^{i+1}) &= \partial_D \widetilde{d^i} - \partial_D d^i \\ &= \partial_D(\widetilde{d^i} - d^i - \partial_D d^{i-1}) \qquad \text{(since } \partial_D \partial_D = 0\text{)} \\ &= \partial_D \phi^i c^i = \phi^{i+1}\partial_C c^i \qquad \text{(commutativity of (2))} \end{aligned}$$

By the injectivity of ϕ^{i+1}, (4.15.3) follows.

Exactness at $H^i(E^\cdot)$: One can easily see that $\delta^i \psi^i_* = 0$: If $[e_i] \in \operatorname{im} \psi^i_*$, then we can choose $d^i \in Z^i(D^\cdot)$ above, i.e., choose it as a *cycle*. Then $\partial_D d^i = 0$, therefore $c^{i+1} = 0$,

by Definition (4.15.2) therefore $\delta([e^i]) = 0$. Conversely, let $\delta([e^i]) = 0$, therefore (with the notations above) $[c^{i+1}] = 0$, i.e.,

$$c^{i+1} = \partial_C c^i$$

for an $c^i \in C^i$. Then, again with the notations above, we have

$$\begin{aligned} \partial_D d^i &= \phi^{i+1} c^{i+1} = \phi^{i+1} \partial_C c^i \\ &= \partial_D \phi^i c^i \qquad \text{(commutativity of (2))}\,. \end{aligned}$$

Therefore for $\widetilde{d}^i = d^i - \phi^i c^i$ we have $\partial_D \widetilde{d}^i = 0$, i.e., $\widetilde{d}^i \in Z^i(D^\cdot)$ and $\psi^i \widetilde{d}^i = \psi^i d^i - \psi^i \phi^i c^i = \psi^i d^i = e^i$ (since $\psi^i \phi^i = 0$), therefore

$$\psi^i_* [\widetilde{d}^i] = [e^i]\,.$$

Exactness at $H^{i+1}(C^\cdot)$: Exercise!

The claim follows, since i was arbitrary.

Corollary 4.17 (Snake lemma) Let

(4.16.1)
$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & B' & \longrightarrow & C' & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \end{array}$$

be a commutative diagram of R-modules with exact rows. Then one has a canonical exact sequence

(4.16.2)
$$0 \to \ker f \to \ker g \to \ker h \xrightarrow{\delta} \operatorname{coker} f \to \operatorname{coker} g \to \operatorname{coker}\ h \to 0\,.$$

Here one defines:

Definition 4.18 Let $\varphi : M \to N$ is a homomorphism of R-modules. Then

$$\operatorname{coker} \varphi := N / \operatorname{im} \varphi$$

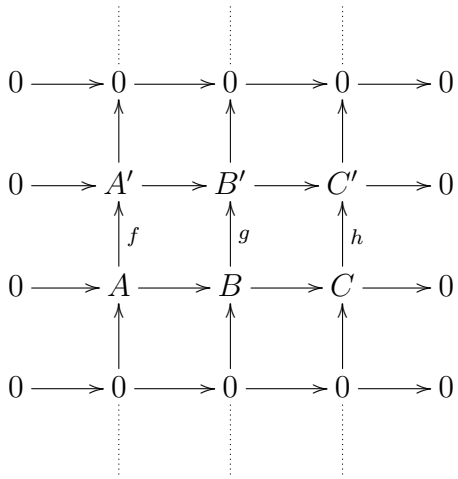
is called the **cokernel** of φ.

Remark 4.19 With this definition we always have an exact sequence

$$0 \to \ker \varphi \xrightarrow{i} M \xrightarrow{\varphi} N \xrightarrow{p} \operatorname{coker} \varphi \to 0$$

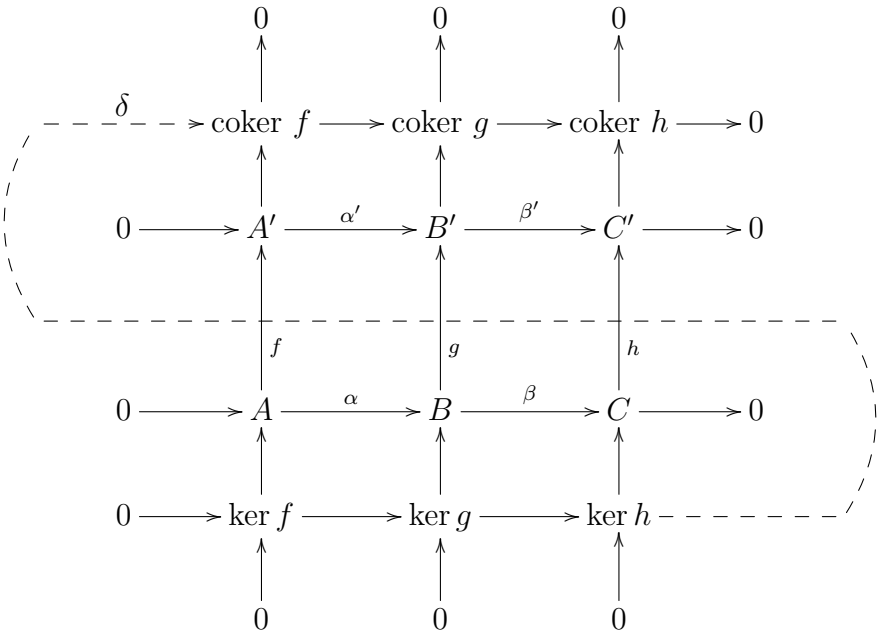
where i is the inclusion and p is the canonical projection.

Proof of the snake lemma: We regard (4.16.1) as a short exact sequence of complexes, where we complete with zeroes above and below:



The long exact cohomology sequence of 4.17 gives (4.16.2): The cohomology at A, B and C is just $\ker f, \ker g$ and $\ker h$, respectively, and the cohomology at A', B' and C' is just $A'/\operatorname{im} f$, $B'/\operatorname{im} g$ and $C'/\operatorname{im} h$. The homomorphism δ in (4.16.2) is just the connecting homomorphism. All other cohomology groups are zero.

Remarks 4.20 (a) The following diagram with exact rows *and columns* gives an explanation of the name and the definition of the maps (and – by 'diagram chase' – also a proof of the snake lemma)



The sequence of the kernel below is induced by α and β, the sequence of the cokernels above is induced by α' and β'. The homomorphism δ is defined as follows: For $c \in \ker h \subseteq C$

let b be a lift of c in B ($\beta(b) = c$) and $b' = g(b) \in B'$. Then "b' already lies in A'" (if we regard α' as inclusion), more precisely, there is an $a' \in A'$ with $\alpha(a') = b'$ (since $\beta'(b') = h(c) = 0$ and $\ker \beta' = \operatorname{im} \alpha'$). Then one has

$$\delta(c) = \text{ class of } a' \text{ in } \operatorname{coker} f\,.$$

This follows from the definitions in 4.16. On the other hand, with the indicated maps, one can easily prove the well-definedness of δ and the exactness of (4.16.2).

(b) In the literature the easy snake lemma is usually proven first, and the long exact cohomology sequence is derived from it.

Corollary 4.21 Let

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

be an exact sequence of abelian groups and let $n \in \mathbb{N}$. Then one has an exact sequence

$$0 \to A[n] \to B[n] \to C[n] \to A/n \to B/n \to C/n \to 0\,.$$

Here, for an abelian group D let

$$D[n] \;:=\; \{d \in D \mid n \cdot d = 0\}$$

be the group of the n-**torsions elements** and let

$$D/n \;:=\; D/nD\,,$$

with $nD = \{nd \mid d \in D\} \subseteq D$.

Proof Apply the snake lemma to

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle n} & & \uparrow{\scriptstyle n} & & \uparrow{\scriptstyle n} & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0\,, \end{array}$$

where $\overset{n}{\to}$ denotes the n-multiplication $x \mapsto nx$.

Corollary 4.22 (compare example 20.6 (c))

$$\mathbb{Q}/\mathbb{Z}[n] \;\cong\; \mathbb{Z}/n\mathbb{Z}$$

Proof Apply 4.21 to the exact sequence

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

where $\mathbb{Q}[n] = 0$ and $\mathbb{Q}/n\mathbb{Q} = 0$.

5 Applications to group cohomology

Let G be a group or a topological group.

Definition 5.1 Let A and B be two (continuous) G-modules. A map

$$\varphi : A \to B$$

is called a **(homo-)morphism of G-modules**, if φ is a (continuous) group homomorphism and if we have:

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

Lemma 5.2 A homomorphism $\varphi : A \to B$ of G-modules induces a canonical homomorphism of abelian groups in the group cohomology

$$\varphi_* : H^i(G, A) \to H^i(G, B)$$

for all $i \geq 0$. Here we have $\mathrm{id}_* = \mathrm{id}$ and $(\psi\varphi)_* = \psi_*\varphi_*$ for another homomorphism of G-elements $\psi : B \to C$.

Proof φ induces a homomorphism

$$\varphi^i : C^i(G, A) \to C^i(G, B)$$

on the (continuous) i-cochains by

$$(f : G^i \to A) \mapsto (\varphi \circ f : G^i \to B)\,.$$

It follows immediately from the definitions that the φ^i are compatible with the differentials ($\partial\varphi^i = \varphi^{i+1}\partial$), therefore this induces a morphism

$$\varphi : C^{\cdot}(G, A) \to C^{\cdot}(G, B)$$

of complexes. The claim follows by passing to the cohomology (Lemma 4.14).

Theorem 5.3 (Long exact cohomology sequence) Let

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

be an exact sequence of (continuous) G-modules, i.e., let α and β be G-module homomorphisms and let the sequence be exact. In case of continuous G-modules we assume

(5.3.1)
β has a continuous section as map of sets,
i.e., there is a continuous map $s : C \to B$
(not necessarily a homomorphism) with $\beta s = id_C$.

Then there is a canonical exact cohomology sequence

$$\begin{array}{ccccccccccc}
0 & \to & H^0(G,A) & \xrightarrow{\alpha_*} & H^0(G,B) & \xrightarrow{\beta_*} & H^0(G,C) & \xrightarrow{\delta} & H^1(G,A) & \to & \dots \\
\dots & \to & H^i(G,A) & \xrightarrow{\alpha_*} & H^i(G,B) & \xrightarrow{\beta_*} & H^i(G,C) & \xrightarrow{\delta} & H^{i+1}(G,A) & \to & \dots\,.
\end{array}$$

Proof We only have to show that

$$0 \to C^{\cdot}(G,A) \xrightarrow{\alpha} C^{\cdot}(G,B) \xrightarrow{\beta} C^{\cdot}(G,C) \to 0$$

is a short exact sequence (of complexes); then the claim follows by passing to cohomology (Theorem 4.16). Therefore we have to show that for every i the sequence

$$0 \to C^i(G,A) \xrightarrow{\alpha^i} C^i(G,B) \xrightarrow{\beta^i} C^i(G,C) \to 0$$

is exact. The injectivity of α^i and the exactness at $C^i(G,B)$ follows easily from the exactness of $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C$. Now, let $s : C \to B$ be a (continuous) section of β. The existence of s follows from the axiom of choice, or from the assumption (5.3.1) (in the continuous case), respectively. Then the map

$$\begin{array}{rccc} s^i : & C^i(G,C) & \to & C^i(G,B) \\ & f & \mapsto & s \circ f \end{array}$$

is a set theoretical section of β^i, i.e., we have $\beta^i s^i = \mathrm{id}$. From this follows immediately the surjectivity of β^i, therefore the exactness at $C^i(G,C)$.

Proposition 5.4 (Change of the group) (a) Let G and G' be (topological) groups, let A be a (continuous) G-module and let A' be a (continuous) G'-module. Furthermore let

$$\pi : G' \to G \quad , \quad \varphi : A \to A'$$

be (continuous) group homomorphisms with

$$\varphi(\pi(g')(a)) = g'\varphi(a)$$

for all $a \in A$ and all $g' \in G'$. ((π, φ) is then called a **compatible pair**). From this we obtain canonical homomorphisms

$$(\pi,\varphi)_* : H^n(G,A) \to H^n(G',A')$$

for all $n \geq 0$.

(b) (Functoriality) We have $(\mathrm{id}_G, \mathrm{id}_A)_* = \mathrm{id}$. If

$$\pi' : G'' \to G' \quad , \quad \varphi' : A' \to A''$$

is another compatible pair, then $(\pi\pi', \varphi'\varphi)$ is compatible and we have

$$(\pi\pi', \varphi'\varphi)_* = (\pi', \varphi')_*(\pi, \varphi)_* : H^n(G,A) \to H^n(G'',A'')\,.$$

Proof (a): We obtain the canonical homomorphisms

$$\begin{array}{rcl} C^n(G,A) & \longrightarrow & C^n(G',A') \\ (f : G^n \to A) & \mapsto & (\varphi \circ f \circ \pi^n : \begin{array}{ccc} (G')^n & \longrightarrow & A' \\ \downarrow & & \downarrow \\ G^n & \longrightarrow & A \end{array}) \end{array}$$

These are obviously compatible with the differentials and therefore induce a morphism of complexes

$$C^{\cdot}(G,A) \to C^{\cdot}(G',A')\,.$$

The claim follows from Lemma 4.14.

(b): This follows immediately from the construction and 4.14.

Examples/Definition 5.5 (a) Let $H \leq G$ be a subgroup and let A be a (continuous) G-module. Then A is a (continuous) H-module by restriction of the operation on H. The pair

$$i : H \hookrightarrow G \quad , \quad \mathrm{id} : A \to A$$

is compatible and defines a canonical homomorphism

$$\mathrm{Res} \,:\, H^n(G,A) \to H^n(H,A)\,,$$

for every $n \geq 0$, which one calls the **restriction** from G to H.

(b) Let $N \trianglelefteq G$ be a normal subgroup, and let A be a (continuous) G-module. Then the fixed module

$$A^N$$

is a (continuous) G/N-module by the definition

$$(gN)a \;:=\; ga \quad \text{for all } g \in G \text{ and } a \in A\,.$$

(this is well-defined, since $na = a$ for all $n \in N$, if $a \in A^N$). The pair

$$\pi : G \twoheadrightarrow G/N \quad , \quad i : A^N \hookrightarrow A$$

is compatible by construction and defines a canonical homomorphism

$$\mathrm{Inf} : H^n(G/N, A^N) \to H^n(G,A)\,,$$

for every $n \geq 0$, which one calls the **inflation** from G/N to G.

Now we will apply this to the so-called Galois cohomology.

Definition 5.6 Let L/K be a (possibly infinite) Galois extension of fields and let $G = \mathrm{Gal}(L/K)$ be its Galois group, equipped with the Krull topology. A **discrete G-module** is a continuous G-module A, where A carries the discrete topology.

Lemma 5.7 Let A be a G-module. Then the following properties are equivalent:

(a) A is a discrete G-module.

(b) For all $a \in A$, the stabiliser

$$\mathrm{St}_G(a) = \{g \in G \mid ga = a\}$$

(compare Algebra I, Def. 17.4) is open in G.

(c) $A = \bigcup\limits_{U \leq G} A^U$, where the union runs over all open subgroups of G.

Proof (a) $\Rightarrow$ (b): For $a \in A$ restrict

$$\begin{array}{rccc} \mu: & G \times A & \to & A \\ & (g,x) & \mapsto & gx \end{array}$$

to the open set $G \times \{a\}$. The inverse image of the open set $\{a\}$ is just $\mathrm{St}_G(a) \times \{a\}$.

(b) $\Rightarrow$ (c): For $a \in A$, we have $a \in A^{\mathrm{St}_G(a)}$.

(c) $\Rightarrow$ (a): Let $a \in A$ and let $U \leq G$ be an open subgroup with $a \in A^U$. For $(g,b) \in \mu^{-1}(\{a\})$, $Ug \times \{b\}$ is an open neighborhood of (g,b) with $\mu(Ug \times \{b\}) = \{gb\} = \{a\}$.

Examples 5.8 (a) In the situation of 5.6, $(L,+)$ and $(L^\times,\cdot)$ are discrete $\mathrm{Gal}(L/K)$-modules.

(b) Every submodule of a discrete G-module is again a discrete G-module.

Remarks 5.9 (a) A discrete $\mathrm{Gal}(L/K)$-module A is also called a **Galois module** for L/K, and

$$H^n(\mathrm{Gal}(L/K), A)$$

is called the n-th **Galois cohomology** of A. It is also denoted shortly by $H^n(L/K, A)$.

(b) In particular, let K_s be the separable closure of a field K (the set of all separable elements over K in the algebraic closure $\overline{K}$ of K). Then K_s/K is Galois, and

$$G_K := \mathrm{Gal}(K_s/K)$$

is called the **absolute Galois group** of K (compare 20.7 for the case $K = \mathbb{F}_q$). For a discrete G_K-module A one also writes

$$H^n(K,A) := H^n(K_s/K, A) = H^n(G_K, A)\,.$$

The understanding of the absolute Galois groups and its Galois cohomology is an important theme of number theory and arithmetic geometry.

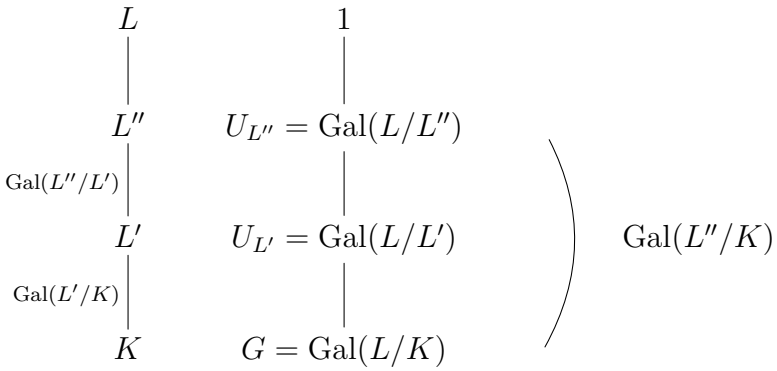
Now let L/K be a Galois extension with Galois group $G = \mathrm{Gal}(L/K)$, and let A be a discrete G-module. If L' is an intermediate field of L/K, which is Galois over K, and if $U_{L'} = \mathrm{Gal}(L/L')$ is the associated closed normal subgroup of G, then

$$A^{U_{L'}}$$

is a $\mathrm{Gal}(L'/K)$-module (via the isomorphism $\mathrm{Gal}(L'/K) \cong G/U_{L'}$), and for another intermediate field L'' with $L \supseteq L'' \supseteq L' \supseteq K$ and L''/K Galois we have

$$A^{U_{L'}} = (A^{U_{L''}})^{\mathrm{Gal}(L''/L')}$$

for the subgroup $\mathrm{Gal}(L''/L') \subseteq \mathrm{Gal}(L''/K)$.



Therefore we have an inflation map

$$\mathrm{Inf}_{L''/L'} : H^n(L'/K, A^{U_{L'}}) \to H^n(L''/K, A^{U_{L''}}) \tag{5.10.1}$$

Furthermore, by 5.4 (b) it is obvious that, for another Galois sub extension L'''/K with $L''' \supseteq L'' \supseteq L'$ we have

$$\mathrm{Inf}_{L'''/L'} = \mathrm{Inf}_{L'''/L''} \circ \mathrm{Inf}_{L''/L'}\,, \tag{5.10.2}$$

as well as $\mathrm{Inf}_{L'/L'} = \mathrm{id}$.

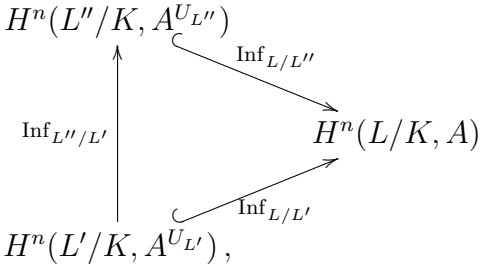
In particular, we obtain an inductive system

$$\left(H^n(L'/K, A^{U_{L'}})\right)_{L' \in \mathcal{K}(L/K)}\,, \tag{5.10.3}$$

with the inflations (5.10.1) as transition maps, where $\mathcal{K}(L/K)$ is the inductively ordered set of the *finite* partial Galois extensions of L/K (compare 2.4 (d)). For these $U_{L'}$ is open and $\mathrm{Gal}(L'/K)$ is finite.

Furthermore, for $L', L'' \in \mathcal{K}(L/K)$ and $L' \subseteq L''$ one has a commutative diagram

(5.10.4)



by (5.10.3) for $L'' = L$. By the universal property of the inductive limit (see Exercise 3), this gives a canonical homomorphism

$$\varinjlim_{L' \in \mathcal{K}(L/K)} H^n(L'/K, A^{U_{L'}}) \to H^n(L/K, A)\,. \tag{5.10.5}$$

Explicitly, an element on the left, represented by a $x \in H^n(L'/K, A^{U_{L'}})$ for an $L' \in \mathcal{K}(L/K)$, is mapped to $\mathrm{Inf}_{L/L'}(x)$.

The following theorem shows that one can calculate the Galois cohomology of L/K as an inductive limit of the cohomologies of the finite groups $\mathrm{Gal}(L'/K)$.

Theorem 5.10 The map (5.10.5) is an isomorphism.

Proof By definition, $\mathrm{Inf}_{L/L'}$ is induced by the morphism of complexes

$$\begin{array}{ccccccccc}
\ldots & \longrightarrow & C^{n-1}(G,A) & \xrightarrow{\partial} & C^n(G,A) & \xrightarrow{\partial} & C^{n+1}(G,A) & \longrightarrow & \ldots \\
 & & \uparrow{\scriptstyle \alpha^{n-1}} & & \uparrow{\scriptstyle \alpha^n} & & \uparrow{\scriptstyle \alpha^{n+1}} & & \\
\ldots & \longrightarrow & C^{n-1}(\mathrm{Gal}(L'/K), A^{U_{L'}}) & \xrightarrow{\partial} & C^n(\mathrm{Gal}(L'/K), A^{U_{L'}}) & \xrightarrow{\partial} & C^{n+1}(\mathrm{Gal}(L'/K), A^{U_{L'}}) & \longrightarrow & \ldots
\end{array}$$

Here we have $\alpha^r(f) = ifp^r$ for an r-cochain $g : \mathrm{Gal}(L'/K)^r \to A^{U_{L'}}$, where $p : G \twoheadrightarrow \mathrm{Gal}(L'/K) = G/U_{L'}$ is the projection and $i : A^{U_{L'}} \hookrightarrow A$ is the inclusion. Obviously all α^r are injective.

Surjectivity of (5.10.5): It suffices to show: If $f \in C^n(G,A)$, then there is an $L' \in \mathcal{K}(L/K)$ and a $g \in C^n(\mathrm{Gal}(L'/K), A^{U_{L'}})$ with $\alpha^n(g) = f$. In fact, if f is an n-cocycle, then g is a cocycle as well, since $\alpha^{n+1}\partial g = \partial\alpha^n g = \partial f = 0$, and since α^{n+1} is injective, and thus we have $[f] = [\alpha g] = \alpha_*[g] = \mathrm{Inf}_{L/L'}[g]$.

Therefore, let $f : G^n \to A$ be an element in $C^n(G,A)$, hence a continuous map. With G, G^n is compact as well, therefore $f(G^n)$ is compact as well, since A, as a discrete topological space, is obviously Hausdorff. Since A is discrete, this means that $f(G^n)$ is finite. Since every element $a \in A$ lies in the fixed module A^U for some open subgroup $U \leq G$, there is an open subgroup $U \leq G$ with

$$f(G^n) \subseteq A^U .$$

Moreover, by passing to an open subgroup, we can assume that $U \trianglelefteq G$ is an open normal subgroup (if $U = \mathrm{Gal}(L/K')$ for a finite partial extension K'/K, then consider $U' = \mathrm{Gal}(L/L')$ for the normal closure L'/K of K'/K).

Furthermore, by the continuity of f and the discreteness of A for every $g = (g_1, \ldots, g_n) \in G^n$, the set $f^{-1}(\{f(g_1, \ldots, g_n)\})$ is open and therefore contains an open neighborhood $g_1U_1 \times \ldots \times g_nU_n =: U(g)$ of g, with open subgroups $U_1, \ldots, U_n$ of G. As above we can assume that the U_i are open normal subgroups of G. Since G^n is compact, G^n is covered by finitely many $U(g^{(1)}), \ldots, U(g^{(r)})$. Let N be the intersection of U above and of all U_i, which occur in the finitely many $U(g^{(\nu)})$. Then f only depends on the cosets modulo N, and therefore is constant on all sets

$$g_1N \times \ldots \times g_nN$$

for *all* $(g_1, \ldots, g_n) \in G^n$. Furthermore, since $N \subseteq U$, f has its image in A^N.

If now $L' = L^N$, then, by (infinite) Galois theory, L'/K is a **finite** Galois extension and we have $N = \mathrm{Gal}(L/L') = U_{L'} = \ker(G \overset{P}{\twoheadrightarrow} \mathrm{Gal}(L'/K))$, and by construction, f lies in the image of

$$\alpha^n : C^n(\mathrm{Gal}(L'/K), A^{U_{L'}}) \to C^n(G, A)$$

(the inverse image of f is g with $g((p(g_1), \ldots, p(g_n))) = f(g_1, \ldots, g_n)$).

Injectivity of (5.10.5): Let $g \in Z^n(\mathrm{Gal}(L'/K), A^{U_{L'}})$ with $\mathrm{Inf}_{L/L'}[g] = [\alpha^n_{L/L'} g] = 0$. Therefore there is an $f_1 \in C^{n-1}(G, A)$ with $\partial f_1 = \alpha^n_{L/L'} g$. By the first step, there is a finite Galois sub extension L''/K and a $g_1 \in C^{n-1}(\mathrm{Gal}(L''/K), A^{U_{L''}})$ with $\alpha^{n-1}_{L/L''} g_1 = f_1$. Here we may assume that we have $L'' \supseteq L'$ (by possibly making the normal subgroup N above smaller). If we now form

$$a^r_{L''/L'} : C^r(\mathrm{Gal}(L'/K) A^{U_{L'}}) \to C^r(\mathrm{Gal}(L''/K), A^{U_{L''}})$$

as above, we obtain

$$\alpha^n_{L/L''} \alpha^n_{L''/L'} g = \alpha^n_{L/L'} g = \partial f_1 = \partial \alpha^{n-1}_{L/L''} g_1 = \alpha^n_{L/L''} \partial g_1 \,,$$

and therefore $\alpha^n_{L''/L'} g = \partial g_1$ by the injectivity of $\alpha^n_{L/L'''}$. This means that $\mathrm{Inf}_{L''/L'}[g] = [\alpha^n_{L''/L'} g] = 0$, i.e., that, in the inductive limit, $[g]$ is equal to 0.

Finally, we introduce a useful tool for calculating cohomology. Let G be a group with discrete topology or let $G = \mathrm{Gal}(L/K)$ for a Galois extension L/K, equipped with the Krull topology.

Lemma/Definition 5.11 Let A be an abelian group and let

$$M^G(A) = \{f : G \to A \mid f \text{ is continuous}\}$$

where A carries the discrete topology. Then $M^G(A)$ becomes a discrete G-module by the definition

$$(gf)(h) \;:=\; f(hg)$$

for $g, h \in G$ and is called the **coinduced module** associated to A.

Proof of the claims: 1) $M^G(A)$ is a G-module: It is obvious that $1 \cdot f = f$ and that $g(f_1 + f_2) = gf_1 + gf_2$ for $g \in G$. Furthermore we have

$$\begin{array}{rcccl} (g_1(g_2 f))(h) & = & (g_2 f)(hg_1) & = & f((hg_1)g_2) \\ & = & f(h(g_1 g_2)) & = & ((g_1 g_2)f)(h)\,, \end{array}$$

and hence $g_1(g_2 f) = (g_1 g_2) f$ for $g_1, g_2 \in G$.

2) $M^G(A)$ is a discrete G-module: For G with discrete topology there is nothing to show; therefore let $G = \mathrm{Gal}(L/K)$ be a Galois group. If $f : G \to A$ is continuous, where A has the discrete topology, then there is, by the proof of Theorem 5.10, an open normal subgroup $N \trianglelefteq G$, so that we have $f(g) = f(gn)$ for all $n \in N$. But this implies that we have $f = nf$ for all $n \in N$. The stabilizer of f in G therefore contains N, and hence is open.

Remarks 5.12 For G with discrete topology, $M^G(A)$ is simply the set of all maps $f : G \to A$. In particular, for a *finite* group G, one has a group isomorphism

$$\begin{array}{rcl} M^G(A) & \tilde{\to} & \bigoplus\limits_{\sigma \in A} A \\ f & \mapsto & (f(\sigma^{-1}))_{\sigma \in G}\,, \end{array}$$

and this becomes an isomorphism of G-modules, if G operates on the right hand side as follows:

$$\tau(a_\sigma)_{\sigma \in G} \;=\; (a_{\tau^{-1}\sigma})_{\sigma \in G}\,.$$

In particular, there is a isomorphism of G-modules

$$M^G(\mathbb{Z}) \tilde{\to} \mathbb{Z}[G]\,,$$

where $\mathbb{Z}[G]$ is the group ring (see Exercise 11). The usefulness of the coinduced G-modules lies in the following property:

Proposition 5.13 (a) under the assumptions of 5.11 we have

$$H^n(G, M^G(A)) = 0 \quad \text{for all} \quad n > 0\,.$$

(b) Furthermore there is a canonical isomorphism

$$H^0(G, M^G(A)) \cong A\,.$$

Proof (a) Let $n \geq 1$ and let $f \in Z^n(G, M^G(A))$. Define a map

$$h :\; G^{n-1} \to M^G(A)$$

by

$$h(g_1, \ldots, g_{n-1})(g) \;:=\; f(g, g_1, \ldots, g_{n-1})(1)\,.$$

Then h is well-defined and continuous (with respect to the discrete topology on $M^G(A)$): By the proof of Theorem 5.10, and the continuity of f, there is an open normal subgroup $N \trianglelefteq G$, such that $f : G^n \to M^G(A)$ factorizes over $(G/N)^n$. Therefore $h(g_1, \ldots, g_{n-1})$ only depends on the $g_i \mod N$, therefore is continuous, i.e., in $M^G(A)$, and furthermore h factorizes over $(G/N)^{n-1}$ and thus is continuous.

Furthermore, with Definition 3.1 we calculate for $g_1, \ldots, g_n, g \in G$

$$\begin{aligned} &((\partial_n h)(g_1, \ldots, g_n))(g) \\ &= [g_1 h(g_2, \ldots, g_n) + \sum_{i=1}^{n-1} (-1)^i h(g_1, \ldots, g_i g_{i+1}, \ldots, g_n) + (-1)^n h(g_1, \ldots, g_{n-1})](g) \\ &= [f(gg_1, g_2, \ldots, g_n) + \sum_{i=1}^{n-1} (-1)^i f(g, g_1, \ldots, g_i g_{i+1}, \ldots, g_n) + (-1)^n h(g, g_1, \ldots, g_{n-1})](1) \\ &= [-(\partial f)(g, g_1, \ldots, g_n) + g f(g_1, \ldots, g_n)](1) = (g f(g_1, \ldots, g_n))(1) = f(g_1, \ldots, g_n)(g) \end{aligned}$$

since $\partial f = 0$. Therefore we have $f = \partial h \in B^n(G, M^G(A))$ as claimed.

(b): For $f \in M^G(A)$ we have: $f \in H^0(G, M^G(A)) \Leftrightarrow f(h) = f(hg)$ for all $h, g \in G \Leftrightarrow f$ is constant. The map $a \mapsto f$ with $f(g) = a$ for all $g \in G$ therefore induces the isomorphism in (b).

Corollary 5.14 If G is a finite group, then we have $H^n(G, \mathbb{Z}[G]) = 0$ for all $n > 0$.

Lemma 5.15 Let A be a discrete G-module. Then the map

$$\begin{array}{rccl} i_A & : & A & \hookrightarrow & M^G(A) \\ & & a & \mapsto & f_a \text{ with } f_a(g) = ga \end{array}$$

is an injective homomorphism of G-modules (where, on the right hand side, A is only regarded as an abelian group).

Proof For $h \in G$ we have $f_{ha}(g) = g(ha) = (gh)a = f_a(gh) = (hf_a)(g)$, therefore $f_{ha} = hf_a$.

Remark 5.16 If we set $B := \operatorname{coker} i_A = M^G(A)/A$, then we obtain a short exact sequence of discrete G-modules

$$0 \to A \hookrightarrow M^G(A) \to B \to 0\,.$$

In the long exact cohomology sequence

$$0 \to A^G \to (M^G(A))^G \to B^G \to H^1(G, A) \to \dots\,,$$

by 5.13, we have $H^n(G, M^G(A)) = 0$ for $n \geq 1$. This gives an exact sequence

$$0 \to A^G \hookrightarrow A \to B^G \to H^1(G, A) \to 0$$

and isomorphisms

$$H^{i-1}(G, B) \xrightarrow{\sim} H^i(G, A)\,.$$

Thus one can calculate the cohomology of A in degree i (one denotes this also as dimension i) by the cohomology of B in degree $i - 1$. This is called the method of the **dimension shift**.

Another application is:

Theorem 5.17 Let G be a finite group of order N. For every G-module A and every $n > 0$ we have

$$N \cdot H^n(G, A) = 0\,.$$

Proof We have the homomorphisms of G-modules

$$\begin{array}{ccccc} A & \stackrel{i}{\to} & M^G(A) & \stackrel{\pi}{\to} & A \\ a & \mapsto & (\sigma \mapsto \sigma a) & & \\ & & f & \mapsto & \sum\limits_{\sigma \in G} \sigma^{-1} f(\sigma)\,. \end{array}$$

For $i = i_A$ (and general G!) see 5.15. The map $\pi = \pi_A$ is only defined for finite G. The additivity is obvious, and for $\tau \in G$ we have

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

Obviously, we have $\pi i = N$, i.e., $\pi(i(a)) = N \cdot a$. Then the composition

$$H^n(G, A) \stackrel{i_*}{\to} H^n(G, M^G(A)) \stackrel{\pi_*}{\to} H^n(G, A)$$

is the multiplication by N ($N_* = N$, as one can see from the definition). On the other hand, this composition is zero, since $H^n(G, M^G(A)) = 0 \quad (n > 0)$. The claim follows.

6 Hilbert 90 and Kummer theory

Theorem 6.1 (Hilbert's Theorem 90) Let L/K be a Galois extension with Galois group G. Then we have

$$H^1(L/K, L^\times) = H^1(G, L^\times) = 0\,.$$

Proof By the limit property of Theorem 5.10 it suffices to show this for finite Galois extensions (Note: For an intermediate field M of L/K, we have $L^{\times\,\mathrm{Gal}(L/M)} = M^\times$ by Galois theory). Therefore let G be finite and let

$$f : G \to L^\times$$

be a 1-cocycle. By the linear independence of field homomorphisms (Algebra I, Corollary 20.3)

$$\sum_{\sigma\in G} f(\sigma)\sigma$$

is not the zero map; therefore there is an $\alpha \in L^\times$ with

$$\beta := \sum_{\sigma\in G} f(\sigma)\sigma(\alpha) \neq 0\,,$$

i.e., $\beta \in L^\times$. Then, for $\tau \in G$, we have

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

by the cocycle property ($f(\tau\sigma) = \tau f(\sigma)\cdot f(\tau)$). Thus

$$f(\tau) = \tau(\beta)^{-1}\cdot\beta = \tau(\beta^{-1})\cdot(\beta^{-1})^{-1} \quad \text{for all} \quad \tau \in G\,,$$

is a 1-coboundary.

This theorem has many applications; one is the Kummer theory (compare Algebra I, §20):

Let K be a field and let K_s be a separable closure of K. Furthermore let n be an integer, which is invertible in K (i.e., $\mathrm{char}(K) \nmid n$) and let $\mu_n \subseteq K_s^\times$ be the group of the n-th roots of unity in K_s. Then μ_n is cyclic of the order n (see Algebra I, Lemma 15.6(e)). Every separable extension L of K we regard as subfield of K_s. For every such L let $\mu_n(L) = \mu_n \cap L$ be the set of the n-th unit roots in L.

Theorem 6.2 (Kummer isomorphism) Let L/K be a Galois extension of fields. Then there is an isomorphism

$$(L^\times)^n \cap K^\times/(K^\times)^n \xrightarrow[\sim]{\delta} H^1(L/K, \mu_n(L))\,,$$

which, for an $\alpha \in K^\times$ with $\alpha = \beta^n, \beta \in L$, maps the class of α to the class of the cocycle

$$\sigma \mapsto \frac{\sigma(\beta)}{\beta} \in \mu_n(L)\,.$$

Proof We have an exact sequence of discrete $\mathrm{Gal}(L/K)$-modules

$$1 \to \mu_n(L) \hookrightarrow L^\times \xrightarrow{n} (L^\times)^n \to 1\,,$$

where $\xrightarrow{n}$ denotes the homomorphism $x \mapsto x^n$. This gives the exact cohomology sequence

$$K^\times \xrightarrow{n} (L^\times)^n \cap K^\times \xrightarrow{\delta} H^1(L/K, \mu_n(L)) \to H^1(L/K, L^\times) = 0\,.$$

Here we used that for $G = \mathrm{Gal}(L/K)$ we have: $(L^\times)^G = K^\times, ((L^\times)^n)^G = (L^\times)^n \cap K^\times$, as well as $H^1(G, L^\times) = 0$ (Hilbert 90). Furthermore δ is the connecting homomorphism. By the exactness of the cohomology sequence, the surjectivity of δ and the claim of the theorem follows with the homomorphism theorem, since the image of the first map is $(K^\times)^n$. The explicit description of δ follows from the definition of δ and of the differential $\partial^0 : L^\times \to C^1(G, L^\times)$.

Corollary 6.3 There is an isomorphism

$$K^\times/(K^\times)^n \xrightarrow{\sim} H^1(K, \mu_n)\,.$$

Proof This follows from 6.2 for $L = K_s$, since we have $(K_s^\times)^n \cap K^\times = K^\times$: For every $\alpha \in K^\times$ there is a $\beta \in K_s^\times$ with $\beta^n = \alpha$. Initially, there is such β in the algebraic closure, as a zero of the polynomial $X^n - \alpha$, but β is in K_s, since this polynomial is separable (since $\mathrm{char}(K) \nmid n$, compare Algebra I, Proof of Theorem 20.5).

Remark 6.4 Therefore we have an exact sequence of discrete G_K-modules

$$1 \to \mu_n \to K_s^\times \xrightarrow{n} K_s^\times \to 1\,,$$

the so-called **Kummer sequence**. Corollary 6.3 follows directly from the associated cohomology sequence.

Theorem 6.2 can be strengthened to an existence claim.

Definition 6.5 Let K contain all n-th roots of unity (so that $\mu_n(K) = \mu_n$). A Galois extension L/K is called a Kummer extension of exponent n, if L/K is abelian of exponent n.

Here we define for $n \in \mathbb{N}$:

Definition 6.6 (a) An abelian group A is called of exponent n, if $nA = 0$, i.e., $na = 0$ for all $a \in A$.

(b) A Galois extension L/K is called abelian (resp. abelian of exponent n), if $\mathrm{Gal}(L/K)$ is abelian (resp. abelian of exponent n).

Theorem 6.7 (Kummer correspondence) Assume that $\mu_n \subseteq K$. Then there are inclusion-preserving bijections

$$\mathcal{K} := \left\{ \begin{array}{l} \text{finite Kummer-} \\ \text{extensions } L/K \\ \text{of exponent } n \end{array} \right\} \begin{array}{c} \xrightarrow{\phi} \\ \xleftarrow{\psi} \end{array} \left\{ \begin{array}{l} \text{subgroups } \Delta \subseteq K^\times \\ \text{with } (K^\times)^n \subseteq \Delta \text{ and} \\ \Delta/(K^\times)^n \text{ finite} \end{array} \right\} =: \mathcal{D}$$

which are inverse to each other, via the assignments

$$\begin{array}{rcl} L & \overset{\phi}{\mapsto} & \Delta_L := (L^\times)^n \cap K^\times \\ L_\Delta := L(\sqrt[n]{\Delta}) & \overset{\psi}{\mapsfrom} & \Delta\,. \end{array}$$

Here let $L(\sqrt[n]{\Delta}) = L(\sqrt[n]{\alpha} \mid \alpha \in \Delta)$.

Proof For $L \in \mathcal{K}$ we have $(K^\times)^n \subseteq \Delta_L \subseteq K^\times$, and by Theorem 6.2, we have an isomorphism

$$\Delta_L/(K^\times)^n \xrightarrow{\sim} H^1(\mathrm{Gal}(L/K), \mu_n)\,.$$

Since L/K is finite, $H^1(\mathrm{Gal}(L/K), \mu_n)$ is obviously finite, therefore Δ_L lies in $\mathcal{D}$. Conversely if we have $\Delta \in \mathcal{D}$, then, for every $\alpha \in \Delta$, the extension $K(\sqrt[n]{\alpha})/K$ is Galois, with cyclic Galois group of exponent n (since $\mu_n \subseteq K$, by the Kummer theory from Algebra I, §20). Let $\alpha_1, \ldots, \alpha_r \in \Delta$ be elements, whose cosets form a system of representatives for the finite group $\Delta/(K^\times)^n$. For every $\alpha \in \Delta$ we then have $\alpha = \alpha_{i_1} \ldots \alpha_{i_s} \gamma^n$ with $i_1, \ldots, i_s \in \{1, \ldots, r\}$ and $\gamma \in K^\times$ and thus

$$K(\sqrt[n]{\alpha}) \subseteq K(\sqrt[n]{\alpha_{i_1}}, \ldots, \sqrt[n]{\alpha_{i_s}})\,.$$

Hence $L_\Delta = K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_r})$ is the compositum of the fields $K(\sqrt[n]{\alpha_i})$ and is thus finite over K and abelian of exponent n, therefore in $\mathcal{K}$. Therefore the assignments ϕ and ψ are well-defined.

Furthermore we have

$$K(\sqrt[n]{\Delta_L}) \subseteq L \quad \text{, i.e.,} \quad \psi\,\phi\,L \;\subseteq\; L\,. \tag{6.7.1}$$

In fact, for $\alpha \in \phi L = \Delta_L = (L^\times)^n \cap K^\times$ we have $K(\sqrt[n]{\alpha}) \subseteq L$. Here $\sqrt[n]{\alpha}$ denotes an element $\gamma \in K_s$ with $\gamma^n = \alpha$. On the other hand, by definition we have $\alpha = \beta^n$ for a $\beta \in L^\times$. Thus $(\gamma/\beta)^n = \alpha/\alpha = 1$, therefore $\gamma/\beta = \zeta \in \mu_n \subseteq K$. It follows $K(\gamma) = K(\beta) \subseteq L$. Overall follows $\psi\phi L = K(\sqrt[n]{\Delta_L}) \subseteq L$, therefore (6.7.1). On the other hand we have

$$(L_\Delta^\times)^n \cap K^\times \supseteq \Delta \quad \text{, i.e.,} \quad \phi\,\psi\,\Delta \;\supseteq\; \Delta\,. \tag{6.7.2}$$

In fact, let $L_\Delta = K(\sqrt[n]{\Delta})$ and $\alpha \in \Delta$. Then there is a $\beta \in L_\Delta$ with $\beta^n = \alpha$, and it follows that $\alpha \in (L_\Delta^\times)^n \cap K^\times = \phi\psi\Delta$.

Furthermore ϕ and ψ are obviously inclusion-preserving, i.e., we have

$$\begin{array}{rcl} L \subset L' & \Rightarrow & \Delta_L \subset \Delta_{L'} \\ \Delta \subset \Delta' & \Rightarrow & L_\Delta \subset L_{\Delta'} \,. \end{array} \tag{6.7.3}$$

Now we show $\psi\phi L = L$ for $L \in \mathcal{K}$. By assumption, $\mathrm{Gal}(L/K)$ is a finite abelian group of exponent n. We use

Theorem 6.8 (Main theorem on finite abelian groups) Every finite abelian group is a direct product of cyclic groups.

Proof Follows from the theory of principal ideal domains – here $\mathbb{Z}$.

Hence we have

$$\mathrm{Gal}(L/K) = \bigoplus_{i=1}^{r} A_i \tag{6.7.4}$$

with cyclic groups A_i, which are necessarily of exponent n as well. The projections

$$\mathrm{Gal}(L/K) \twoheadrightarrow A_i$$

correspond, by Galois theory, to partial extensions $L_i \subseteq L$ with $\mathrm{Gal}(L_i/K) = A_i$ ($L_i = L^{A_i'}$ with $A_i' = \oplus_{j \neq i} A_j$), and by (6.7.4), L is the compositum of the L_i. By Kummer theory for cyclic extensions (Algebra I, Theorem 20.7) there is a $\alpha_i \in K$ with $L_i = K(\sqrt[n]{\alpha_i})$ for every i (if L_i/K is cyclic of degree m_i, we have $m_i \mid n$, therefore $\mu_{m_i} \subseteq \mu_n \subset K$, and by Algebra I 20.7 there is a $\beta_i \in K$ with $L_i = L(\sqrt[m_i]{\beta_i})$. Then we can take $\alpha_i = \beta_i^{\frac{n}{m_i}}$). By construction we have $\sqrt[n]{\alpha_i} \in L$, therefore $\alpha_i \in \Delta_L$, therefore $L_i \subseteq K(\sqrt[n]{\Delta_L})$. Thus the compositum L also lies in $K(\sqrt[n]{\Delta_L})$. From (6.7.1) follows the equality.

Now we show $\phi\psi\Delta = \Delta$. Let $\tilde{\Delta} = \phi\psi\Delta$ and let $\tilde{L} = L_\Delta = \psi\Delta$, so that $\tilde{\Delta} = \Delta_{\tilde{L}}$. By (6.7.2) we have $\Delta \subseteq \tilde{\Delta}$, and we obtain a diagram

$$\begin{array}{ccccc} \tilde{\Delta}/(K^\times)^n = & (\tilde{L}^\times)^n \cap K^\times/(K^\times)^n & \xrightarrow[\sim]{\delta} & H^1(\tilde{L}/K, \mu_n) \\ & \bigcup\vert & & \\ & \Delta/(K^\times)^n & & \end{array}$$

Assume $\Delta \subsetneqq \tilde{\Delta}$. Then $U := \delta(\Delta/(K^\times)^n)$ is a proper subgroup of

$$H^1(\tilde{L}/K, \mu_n) = \mathrm{Hom}(G, \mu_n)$$

where $G = \mathrm{Gal}(\tilde{L}/K)$. Let

$$H = \{\sigma \in G \mid \chi(\sigma) = 1 \quad \text{for all} \quad \chi \in U\}\,,$$

By the following Theorem 6.10 (see Remark 6.11) we have $H \neq 1$. On the other hand we have

$$\begin{array}{rcll} \sigma \in H & \Leftrightarrow & \delta(\alpha)(\sigma) = 1 & \text{for all} \quad \alpha \in \Delta \\ & \Leftrightarrow & \sigma(\sqrt[n]{\alpha}) = \sqrt[n]{\alpha} & \text{for all} \quad \alpha \in \Delta \\ & \Leftrightarrow & \sigma = 1\,, & \end{array}$$

since $\tilde{L} = K(\sqrt[n]{\Delta})$ – contradiction!. Thus we have $\tilde{\Delta} = \Delta$, i.e., $\phi\psi\Delta = \Delta$, and we proved Theorem 6.7.

Definition 6.9 For a finite abelian group A

$$A^\vee := \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$$

is called the **Pontrjagin-dual** of A.

Theorem 6.10 (Duality theory for finite abelian groups) Let A be a finite abelian group.

(a) $A^\vee$ is non-canonically isomorphic to A. In particular, $A^\vee$ is again finite and abelian and has the same order as A

(b) If we have A of exponent $n \in \mathbb{N}$, then we have

$$A^\vee = \mathrm{Hom}(A, \mathbb{Z}/n\mathbb{Z})\,.$$

(c) The canonical map

$$\begin{array}{rccc} \varphi_A & : & A & \to & A^{\vee\vee} \\ & & a & \mapsto & (\chi \mapsto \chi(a)) \end{array}$$

is an isomorphism.

(d) If

$$0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$$

is an exact sequence of finite abelian groups, then

$$0 \to C^\vee \xrightarrow{\beta^\vee} B^\vee \xrightarrow{\alpha^\vee} A^\vee \to 0$$

is exact (For an arbitrary homomorphism $\varphi : A \to B$ let $\varphi^\vee : B^\vee \to A^\vee$ be defined by $B^\vee \ni \chi \mapsto \chi \circ \varphi \in A^\vee$).

(e) For a subgroup $U \leq A$ let

$$U^\perp = \{\chi \in A^\vee \mid \chi_{|U} = 0\}\,.$$

Then the assignment

$$U \mapsto U^\perp$$

is an inclusions-reversing bijection between the subgroups of A and the subgroups of $A^\vee$. Thus we have $A^\vee/U^\perp \xrightarrow{\sim} U^\vee$.

Remark 6.11 From this theorem follows the relation $H \neq \{1\}$ in the proof above: If we identify both cyclic groups μ_n and $\mathbb{Z}/n\mathbb{Z}$, then we have

$$\mathrm{Hom}(G, \mu_n) \cong \mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z}) = G^\vee \,.$$

If we pass to additive notation, then, for $U \lneqq G^\vee$, we obtain the exact sequence

$$0 \to U \to G^\vee \to G^\vee/U \to 0$$

with non-trivial $G^\vee/U$ and an exact sequence

$$0 \to (G^\vee/U)^\vee \to G^{\vee\vee} \to U^\vee \to 0$$

where $(G^\vee/U)^\vee$ is non-trivial. Therefore the map $G^{\vee\vee} \to U^\vee$ (which maps $\psi \in (G^\vee)^\vee$ to $\psi_{|U}$) has a non-trivial kernel. If we use the isomorphism $\varphi_G : G \xrightarrow{\sim} G^{\vee\vee}$, then there is a non-trivial $a \in G$ with $\varphi_G(a)(\chi) = \chi(a) = 0$ for all $\chi \in U$. This gives a non-trivial element in the group H above.

Proof of Theorem 6.10: (b): If A has the exponent n, then for $\chi \in A^\vee$ we have

$$(n\chi)(a) = n \cdot \chi(a) = \chi(na) = \chi(0) = 0 \,.$$

In particular, χ has image in $\mathbb{Q}/\mathbb{Z}[n] = \mathbb{Z}/n\mathbb{Z}$ (compare 4.22), and $A^\vee$ is again of exponent n.

In the following it suffices to consider groups of a fixed exponent n.

(a) For $\mathbb{Z}/n\mathbb{Z}$ we have canonically

$$\begin{array}{rcl} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\vee \\ b & \mapsto & (\varphi_b \text{ with } \varphi_b(\overline{1}) = b) \end{array}$$

(therefore $\varphi_b(a) = ab$). For a finite cyclic group A follows a non-canonical isomorphism $A \xrightarrow{\sim} A^\vee$ by choice of an isomorphism $A \cong \mathbb{Z}/n\mathbb{Z}$. By Theorem 6.8, for an arbitrary finite abelian group A, there are cyclic subgroups $A_1, \ldots, A_r$ with

$$A = A_1 \oplus \ldots \oplus A_r \,.$$

But there is a canonical isomorphism

$$\begin{array}{rcl} A_1^\vee \oplus \ldots \oplus A_r^\vee & \xrightarrow{\sim} & (A_1 \oplus \ldots \oplus A_r)^\vee \\ (\chi_1, \ldots, \chi_r) & \mapsto & \chi \text{ with } \chi(a_1, \ldots, a_r) = \sum\limits_{i=1}^{r} \chi_i(a_i) \end{array} \tag{6.10.1}$$

This implies (a).

(c): This follows easily for cyclic groups A: if A is of the order n and a is a generator, then, for every $\overline{m} \in \mathbb{Z}/n\mathbb{Z}$ there is exactly one $\chi_{\overline{m}}$ with $\chi_{\overline{m}}(a) = \overline{m}$. Then the homomorphism

$$\varphi_A : A \to A^{\vee\vee}$$

is injective, since we have $\chi_{\overline{1}}(ka) = \overline{k} \neq 0$ for $ka \neq 0$. Since $A^{\vee\vee}$ has the same order as A, φ_A is bijective. The case of an arbitrary A follows again with (6.10.1).

(d) The exactness of

$$0 \to C^\vee \xrightarrow{\beta^\vee} B^\vee \xrightarrow{\alpha^\vee} A^\vee$$

follows easily. (Later we will prove this in the general frame of R-modules). Then $\alpha^\vee$ is surjective, since we have $|A^\vee| = |A| = |B| \cdot |C|^{-1} = |B^\vee| \cdot |C^\vee|^{-1} = |B^\vee/C^\vee|$, the injection $B^\vee/C^\vee \hookrightarrow A^\vee$ (homomorphic theorem!) is therefore an isomorphism.

(e): For subgroups $U, V \subseteq A$, the relation

$$U \subseteq V \;\Rightarrow\; V^\perp \subseteq U^\perp$$

is obvious. If we define an 'orthogonal complement' for subgroups $X \subseteq A^\vee$

$$X^\perp = \{a \in A \mid \chi(a) = 0 \quad \forall\, \chi \in X\}\,,$$

we show that

$$X \mapsto X^\perp$$

is an inverse image to $U \mapsto U^\perp$: The exact sequence

$$0 \to U \xrightarrow{i} A \to A/U \to 0$$

by (d) gives an exact sequence

$$0 \to (A/U)^\vee \to A^\vee \xrightarrow{i^\vee} U^\vee \to 0\,.$$

But obviously we just have $U^\perp = \ker i^\vee$; this gives an exact sequence

$$0 \to U^\perp \xrightarrow{j} A^\vee \xrightarrow{i^\vee} U^\vee \to 0\,,$$

where j is the inclusion. By further dualizing we obtain a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U^{\vee\vee} & \xrightarrow{i^{\vee\vee}} & A^{\vee\vee} & \xrightarrow{j^\vee} & (U^\perp)^\vee & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle \varphi_U} & \wr & & \wr & \uparrow{\scriptstyle \varphi_A} & & \\ & & U & \hookrightarrow & A & & & & \end{array}$$

with an exact top row. Obviously we have $U^{\perp\perp} = \ker(j^\vee \circ \varphi_A)$, and $U^{\perp\perp} = U$ follows. In the same way, $X^{\perp\perp} = X$ follows for $X \leq A^\vee$.

7 Properties of group cohomology

Theorem 7.1 Let $\{A_i \mid i \in I\}$ be a family of G-modules. Then one has canonical isomorphisms

(a) $H^q(G, \bigoplus_{i\in I} A_i) \cong \bigoplus_{i\in I} H^q(G, A_i)$

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

Exercise!

Theorem 7.2 If G is a (topological) group and

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

a commutative diagram of (continuous) G-modules with exact rows.

Then the diagrams

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

are commutative for all q.

Exercise!

Proposition 7.3 Let

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

be an exact sequence of (continuous) G-modules, and let $H \leq G$ be a subgroup of G. Then the diagram

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

is commutative.

Proposition 7.4 If $N \lhd G$ is a normal subgroup of G, and the sequence

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

is exact as well, then the diagram

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

is commutative

Proof Both results follow immediately from the fact that the maps on the cochains commute with the differentials.

Theorem 7.5 Let A be a (continuous) G-module, and let $N \leq G$ be a normal subgroup. If $H^i(N, A) = 0$ for $i = 1, \ldots, q-1$, and $q \geq 1$, then the sequence

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

is exact.

Proof We prove this by induction on the dimension q, using dimension shifting, and Exercise 1 from Exercise sheet 4 for the initial induction step.

If we tensor the exact sequence

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

with A, we get an exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & A \otimes \mathbb{Z}[G] & \longrightarrow & A \otimes J_G & \longrightarrow & 0 \\ & & \| & & \| & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & \ddot{B} & \longrightarrow & \ddot{C} & \longrightarrow & 0 \end{array}$$

Moreover, since $H^1(N, A) = 0$, we get an exact cohomology sequence

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

Hence we have the following commutative diagram

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

which gives the induction step from $q-1$ to q.

In fact, B is cohomologically trivial, so that the exact sequence

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

induces isomorphisms

$$H^{q-1}(G, C) \xrightarrow[\sim]{\delta} H^q(G, A)\,.$$

Moreover, B^N is a cohomologically trivial G/N-module as well, so that the sequence

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

induces an isomorphism

$$H^{q-1}(G/N, C^N) \xrightarrow[\sim]{\delta} H^q(G/N, A^N)$$

Theorem 7.6 Let G be a (topological) group, let $H \leq G$ be a subgroup, and let $f : A \to B$ be a morphism of (continuous) G-modules

(a) Then the diagram

$$\begin{array}{ccc} H^q(G, A) & \xrightarrow{f_*} & H^q(G, B) \\ \downarrow{\scriptstyle \mathrm{Res}^q} & & \downarrow{\scriptstyle \mathrm{Res}^q} \\ H^q(H, A) & \xrightarrow{f_*} & H^q(H, B) \end{array}$$

is commutative.

(b) Assume that $N \leq G$ is a normal subgroup. Then the diagram

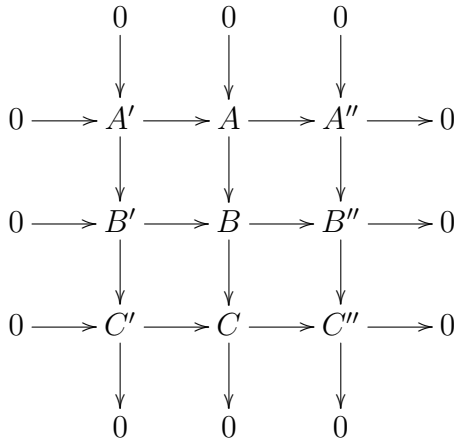
$$\begin{array}{ccc} H^q(G/N, A^N) & \xrightarrow{f_*} & H^q(G/N, B^N) \\ \downarrow{\scriptstyle \mathrm{Inf}^q} & & \downarrow{\scriptstyle \mathrm{Inf}^q} \\ H^q(G, A) & \xrightarrow{f_*} & H^q(G, B) \end{array}$$

is commutative.

Proof This follows easily from the definitions.

An amazing property of the connecting morphism is that it is "anticommutative":

Theorem 7.7 Assume that the diagram of G-modules and G-homomorphisms



is commutative with exact rows and columns. Then the diagram

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

commutes.

Proof Let D be the kernel of the composite map $B \to C''$; thus the sequence

$$0 \to D \to B \to C'' \to 0$$

is exact. We define G-homomorphisms

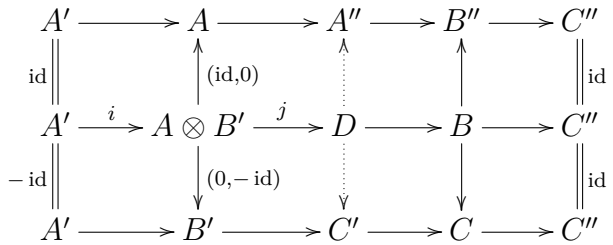
$i : A' \to A \oplus B'$ by $i(a') = (a, b')$, where a (resp. b' is the image of a' in A (resp. of b' in B'),

$j : A \oplus B' \to D$ by $j(a, b') = d_1 - d_2$, where d_1 (resp. d_2) is the image of a (resp. of b') in $D \subseteq B$.

It is easy to verify that with these definition the sequence

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

is exact, and the diagram



commutes. Because $\mathrm{im}(D \to B'') \subseteq \mathrm{im}(A'' \to B'')$ and $A'' \to B''$ is injective, there is a G-homomorphism $D \to A''$ which extends the above diagram. Similarly, since $\mathrm{im}(D \to C) \subseteq \mathrm{im}(C' \to C)$ and $C' \to C$ is injective, there is an analogous G-homomorphism $D \to C'$, Since the resulting extended diagram is commutative, it follows from 3.5 that the following diagram

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

commutes as well, which immediately implies the theorem.

8 Tate cohomology for finite groups

Let G be a finite group, and let A be a G-module. John Tate observed that one can extend the series of cohomology groups in positive degrees

$$H^0(G,A), H^1(G,A), H^2(G,A), \dots$$

by also introducing cohomology groups with negative degrees (these can also be regarded as *homology* groups). They can be obtained by a dualizing process, nd one gets, similarly as before, modified groups $\mathcal{C}^0(G,A) = A$ for $n = 0$, and $\mathcal{C}^n(G,A) = \mathrm{Hom}(G^n, A)$ for $n \geq 1$, and now also groups in negative degrees $\mathcal{C}^{-n-1}(G,A) = \mathrm{Hom}(G^n, A)$ (so that $C^{-1}(G,A) = A$), i.e., a complex

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

Here the differentials ∂^n for $n \geq 1$ are the known ones, and the differentials ∂^n for $n \leq 0$ are

$\partial^0 x = N_G X$, where $N_G x = \sum\limits_{\sigma \in G} \sigma x$,

$\partial^{-1} x = \sum\limits_{\sigma \in G} (\sigma^{-1} x(\sigma) - x(\sigma))$

$$\begin{aligned}\partial^{-n-1} x(\sigma_1, \dots, \sigma_n) = \sum_{\sigma \in G} [&\sigma^{-1} x(\sigma, \sigma_1, \dots, \sigma_n) \\ &+ \sum_{i=1}^{n} (-1)^i x(\sigma_1, \dots, \sigma_{i-1}, \sigma, \sigma^{-1}, \sigma_{i+1}, \dots, \sigma_n) \\ &+ (-1)^{n+1} x(\sigma_1 \dots, \sigma_n, \sigma)], \text{ for } n \geq 1.\end{aligned}$$

8.1 For the groups in low dimension we therefore obtain the following modified cohomology groups:

$$\begin{aligned}\hat{H}^0(G,A): \quad Z^0 &= \ker \partial^1 = A^G \qquad (= H^0(G,A)) \\ B_0 &= \mathrm{im}\, \partial^0 \ = N_G A := \{N_G a \mid a \in A\}\end{aligned}$$

Hence $\hat{H}^0(G,A) = A^G / N_G A$.

$$\begin{aligned}\hat{H}^{-1}(G,A): \quad Z^{-1} &= \ker \partial^0 = {}_{N_G}A := \{a \in A \mid N_G a = 0\} \\ B^{-1} &= \mathrm{im}\, \partial^{-1} = I_G A := \{(\sigma - 1)a \mid a \in A\}\end{aligned}$$

Here $I_G \subseteq \mathbb{Z}[G]$ is the so-called augmentation ideal, $I_G = \left\{ \sum\limits_{\sigma \in G} n_\sigma \sigma \mid \sum\limits_{\sigma \in G} n_\sigma = 0 \right\}$.

Hence $H^{-1}(G,A) = {}_{N_G}A / I_G A$.

Corollary 8.2 One has canonical isomorphisms

$$H^{-2}(G,\mathbb{Z}) \xrightarrow[\sim]{\delta} H^{-1}(G,\mathbb{Z}) \longrightarrow G^{\mathrm{ab}},$$

where $G^{\mathrm{ab}} = G/[G,G]$ is the maximal abelian quotient of G.

Proof Since $\mathbb{Z}[G]$ has trivial cohomology for $n > 0$ (see Corollary 5.14), the long exact cohomology sequence for

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

gives an isomorphism

$$H^{-2}(G, \mathbb{Z}) \xrightarrow[\sim]{\delta} H^{-1}(G, I_G)\,.$$

Since $H^{-1}(G, I_G) \cong I_G/I_G^2$ (as ${}_{N_G}I_G = I_G$), it then suffices to construct an isomorphism

$$I_G/I_G^2 \xrightarrow{\sim} G^{\mathrm{ab}}\,.$$

For this we consider the map

$$\varphi \quad G \longrightarrow I_G/I_G^2 \quad , \quad \sigma \mapsto \sigma - 1 + I_G^2$$

Since $\sigma \cdot \tau - 1 = (\sigma - 1) + (\tau - 1) + (\sigma - 1) \cdot (\tau - 1)$, this map is a homomorphism. Moreover, since I_G/I_G^2 is abelian, the kernel of φ contains the commutator group $[G, G]$, which gives a group homomorphism

$$\log : G/[G, G] \to I_G/I_G^2$$

Now we define a group homomorphism

$$\exp : I_G/I_G^2 \to G/[G, G]$$

by usiong that I_G is the free abelian group generated by the elements $\sigma - 1$, where $\sigma \in G \setminus \{1\}$. Hence setting

$$\sigma - 1 \mapsto \sigma[G, G]\,,$$

we obtain an evidently surjective homomorphism

$$I_G \to G/[G, G]\,.$$

Since

$$(\sigma - 1) \cdot (\tau - 1) = (\sigma\tau - 1) - (\sigma - 1) - (\tau - 1)$$

is mapped to

$$\sigma\tau\sigma^{-1}\tau^{-1}[G, G] = \underline{1}\,,$$

the elements in I_G^2 lie in the kernel, so that we obtain a homomorphism

$$\begin{array}{rcl} \exp : I_G/I_G^2 & \to & G/[G, G] \\ \sigma - 1 + I_G^2 & \mapsto & \sigma G'\,, \end{array}$$

with the property that $\log \circ \exp = \mathrm{id}$ and $\exp \circ \log = \mathrm{id}$. Therefore the map

$$\log : G/[G, G] \to I_G/I_G^2$$

is an isomorphism.

The method used in Corollary 8.2 is called the method of **dimension shifting**.

We have a short exact sequences of G-modules

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

and

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

If A is a G-module, we can tensor these exact sequences with A and obtain the short exact sequences (since $\mathbb{Z}, I_G, \mathbb{Z}[G]$ and J_G are free $\mathbb{Z}$-modules)

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

and

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

Then these sequences induce isomorphisms

$$H^q(G, A) \xrightarrow[\sim]{\delta} H^{q+1}(G, I_G \otimes A)$$

$$H^q(G, J_G \otimes A) \xrightarrow[\sim]{\delta} H^{q+1}(G, A)$$

Writing

$$A^m = J_G^{\otimes m} \otimes A \qquad \text{for } m \geq 0\,,$$
$$A^m = I_G^{\otimes m} \otimes A \qquad \text{for } m \leq 0\,,$$

and using iteration

$$H^{q-m}(G, A^m) \xrightarrow{\delta} H^{q-(m-1)}(G, A^{m-1}) \xrightarrow{\sim} \ldots H^q(G, A)$$

and similarly for δ^{-1} we get the isomorphism

$$\delta^m : H^{q-m}(G, A^m) \xrightarrow{\sim} H^q(G, A)$$

for $m \in \mathbb{Z}$.

9 Cohomology of cyclic groups

Let G be a cyclic group of order n with generator σ. Then, for the group ring $\mathbb{Z}[G]$ we have

$$\begin{aligned} \mathbb{Z}[G] &= \bigoplus_{i=0}^{n-1} \mathbb{Z}\sigma^i \\ N_G &= 1 + \sigma + \ldots + \sigma^{n-1} \end{aligned}$$

and, because $\sigma^{k-1} = (\sigma - 1)(\sigma^{k-1} + \ldots + \sigma + 1)(k \geq 1)$, the augmentation ideal is the principal ideal of $\mathbb{Z}[G]$ generated by $\sigma - 1$, i.e.,

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

Theorem 9.1 Let G be a cyclic group, and let A be a G-module. Then

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

Proof It suffices to specify an isomorphism

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

In fact, given this, the general case follows by dimension shifting. The group Z_1 of 1-cocycles consists of all crossed homomorphisms of G in A. Therefore, if $x \in Z_1$, then

$$\begin{aligned} x(\sigma^k) &= \sigma x(\sigma^{k-1}) + x(\sigma) \\ &= \sigma^2 x(x^{k-2}) + \sigma x(\sigma) + x(\sigma) \\ &= \sum_{i=0}^{k-1} \sigma^i x(\sigma) \quad (k \leq 1), \text{ and} \\ x(1) &= 0, \text{because } x(1) = x(1) + x(1)\,. \end{aligned}$$

It follows that

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

i.e., $x(\sigma) \in {}_{N_G}A$.

Conversely, it is easy to see that, if $a \in {}_{N_G}A = Z_{-1}$ is a (-1)-cocycle, then

$$x(\sigma) = a, \text{ and } x(\sigma^k) = \sum_{i=0}^{k-1} \sigma^i a$$

defines a 1-cocycle.

Therefore the map

$$x \mapsto x(\sigma)$$

is an isomorphism from Z_1 to $Z_{-1} = {}_{N_G}A$

Under this isomorphism, the group R_1 of 1-coboundaries is mapped to the group R_{-1} of (-1)-coboundaries:

$$\begin{array}{rcl} x \in R_{-1} & \Leftrightarrow & x(\sigma^k) = \sigma^k a - a \text{ with fixed } a \in A \\ & \Leftrightarrow & x(\sigma) = \sigma a - a \\ & \leftrightarrow & x(\sigma) \in I_G A = R_{-1}\,. \end{array}$$

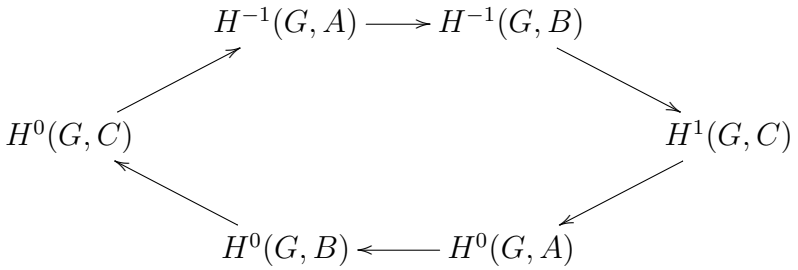
Thus for a cyclic group G we have isomorphisms

$$\begin{array}{rcl} H^{2q}(G,A) & \cong & H^0(G,A) \\ H^{2q+1}(G,A) & \cong & H^1(G,A)\,. \end{array}$$

If

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

is an exact sequence of G-modules, we can write the corresponding long exact sequence in the form



For the exactness at the term $H^{-1}(G,A)$ note that the isomorphism $H^1(G,A) \cong H^{-1}(G,A)$ from Theorem 9.1 fits into the commutative diagram

$$\begin{array}{ccc} H^{-1}(G,A) & \longrightarrow & H^{-1}(G,B) \\ \downarrow \wr & & \downarrow \wr \\ H^1(G,A) & \longrightarrow & H^1(G,B) \end{array}$$

so that the kernel of the map below corresponds to the kernel of the map above.

For many index and order considerations the notion of a **Herbrand quotient** is very useful.

We introduce it in a more general from:

Definition 9.2 Let A be an abelian group, and let f, g endomorphisms of A such that $f \circ g = g \circ f = 0$, so that we have inclusions $\operatorname{im} g \subseteq \ker f$ and $\operatorname{im} f \subseteq \ker g$. Then the **Herbrand quotient** is defined as

$$q_{f,g}(A) = \frac{(\ker f : \operatorname{im} g)}{(\ker g : \operatorname{im} f)}$$

provided both indices are finite.

We are mainly interested in the following special case:

Let A be a G-module with G cyclic of order n. Consider the endomorphisms

$$f = D = \sigma - 1 \quad \text{and} \quad g = N = 1 + \sigma + \ldots + \sigma^{n-1}\,,$$

where σ is a generator of G. Obviously we have

$$D \circ N = N \circ D = 0\,,$$

and

$$\ker D = A^G, \operatorname{im} N = N_G A; \ker N = {}_{N_G}A, \operatorname{im} D = I_G A\,.$$

Hence if both cohomology groups $H^0(G,A)$ and $H^{-1}(G,A)$ are finite, then

$$q_{D,N}(A) = \frac{|H^0(G,A)|}{|H^{-1}(G,A)|} = \frac{|H^2(G,A)|}{|H^1(G,A)|}\,.$$

If this holds, we call A a **Herbrand module**. For these special Herbrand quotients $q_{D,N}(A)$ we want to use the following notation:

Definition 9.3 Let G be a cyclic group and A a G-module. Then

$$h(A) = \frac{|H^0(G,A)|}{|H^{-1}(G,A)|} = \frac{|H^2(G,A)|}{|H^1(G,A)|}\,.$$

These special Herbrand quotients $h(-)$ are **multiplicative**:

Theorem 9.4 Let G be a cyclic group and

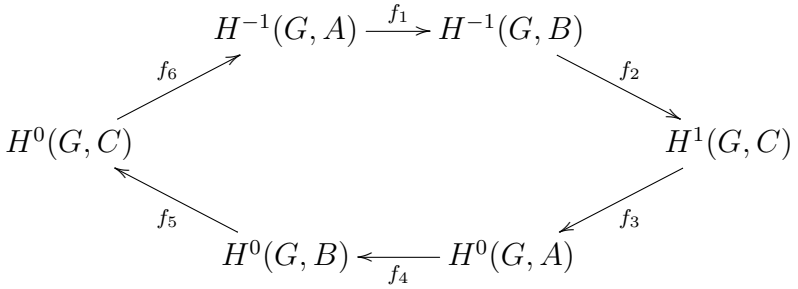
$$0 \to A \to B \to C \to 0$$

an exact sequence of G-modules. Then

$$h(B) = h(A) \cdot h(C)$$

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

Proof Consider the long exact cohomology sequence, written as the hexagon



If we write F_i for the order of the image of f_i, then

$$\begin{array}{rclrclrcl} |H^{-1}(G,A)| &=& F_6 \cdot F_1, & |H^{-1}(G,B)| &=& F_1 \cdot F_2, & |H^{-1}(G,C)| &=& F_2 \cdot F_3, \\ |H^{0}(G,A)| &=& F_3 \cdot F_4, & |H^{0}(G,B)| &=& F_4 \cdot F_5, & |H^{0}(G,C)| &=& F_5 \cdot F_6, \end{array}$$

and therefore

$$|H^{-1}(G,A)| \cdot |H^{-1}(G,C)| \cdot |H^{0}(G,B)| = |H^{-1}(G,B)| \cdot |H^{0}(G,A)| \cdot |H^{0}(G,C)|, \tag{9.4.1}$$

Hence whenever two of the three quotients $h(A), h(B), h(C)$ are defined, then so is the third, and the identity (9.4.1) implies the formula $h(B) = h(A) \cdot h(C)$.

Another special case of a Herbrand quotients occurs when A is an abelian group and f and g are the endomorphisms $f = 0$ and $g = n$ (n a positive integer), i.e., g is the map 'multiplication by n' $a \mapsto n \cdot a \in A$. Then we have

$$q_{0,n}(A) = \frac{(A : nA)}{|{}_nA|} \quad ({}_nA = \{a \in A \mid n \cdot a = 0\}) \,. \tag{9.4.2}$$

In fact, this is just a special case of what we considered above:

Proposition 9.5 If the cyclic group G of order n acts trivially on A, then

$$h(A) = q_{0,n}(A) \,.$$

In particular, the Herbrand quotients $q_{0,n}$ are multiplicative:

Proposition 9.6 If $0 \to A \to B \to C \to 0$ is an exact sequence of abelian groups, then

$$q_{0,n}(B) = q_{0,n}(A) \cdot q_{0,n}(C) \,;$$

this again in the sense that the existence of two of these quotients implies the existence of the third.

Proposition 9.7 If A is a finite group, then we always have

$$q_{f,g}(A) = 1 \,.$$

Proof Because of the isomorphisms $\operatorname{im} f \cong A/\ker f$ and $\operatorname{im} g \cong A/\ker g$,

$$|A| = |\ker f| \cdot |\operatorname{im} f| = |\ker g| \cdot |\operatorname{im} g| \,,$$

which implies the claim.

In particular, a finite G-module A has Herbrand quotient $h(A) = 1$. This remark, together with the multiplicativity shown in 9.4, implies the following:

If A is a submodule of finite index in the G-module B, then
$h(B) = h(A)$.

It is in fact this statement that is most useful in applications of the Herbrand quotient. If the direct computation of the order of the cohomology groups of a G-module B is not possible, the above fact allows us to consider without loss an appropriate submodule A, provided it has finite index. This type of consideration historically motivated the definition of the Herbrand quotient.

In the following we will show how to determine h in case of a cyclic group G of prime order p from the Herbrand quotients $q_{0,p}$. For this we need

Lemma 9.8 Let g and f be two endomorphisms of an abelian group A such that $f \circ g = g \circ f$. Then

$$q_{0,gf}(A) = q_{0,g}(A) \cdot q_{0,f}(A)\,,$$

where again all three quotients are defined whenever any two of them are.

Proof Consider the commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & g(A) \cap \ker f & \longrightarrow & g(A) & \xrightarrow{f} & fg(A) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \ker f & \longrightarrow & A & \xrightarrow{f} & f(A) & \longrightarrow & 0 \end{array}$$

We obtain the exact sequence

$$0 \to \ker f/g(A) \cap \ker f \to A/g(A) \to f(A)/fg(A) \to 0\,,$$

so that

$$\frac{(A : fg(A))}{(A : f(A))} = \frac{(A : g(A)) \cdot |g(A) \cap \ker f|}{|\ker f|}\,.$$

If we observe that

$$\ker fg/\ker g = g^{-1}(g(A) \cap \ker f)/g^{-1}(0) \cong g(A) \cap \ker f\,,$$

we in fact get

$$\frac{(A : gf(A))}{|\ker gf|} = \frac{(A : g(A))}{|\ker g|} \cdot \frac{(A : f(A))}{|\ker f|}\,.$$

It is easy to verify that all three quotients are defined, if two of them are.

Now we prove the important

Theorem 9.9 Let G be a group of prime order p and let A be a G-module. If $q_{0,p}(A)$ is defined, then $q_{0,p}(A^G)$ and $h(A)$ are also defined and we have

$$h(A)^{p-1} = q_{0,p}(A^G)^p/q_{0,p}(A)\,.$$

Proof Let σ be a generator of G and let $D = \sigma - 1$. Consider the exact sequence

$$0 \to A^G \to A \xrightarrow{D} I_G A \to 0\,.$$

From the fact that $I_G A$ is a subgroup as well as a factor group of A, we conclude immediately that if $q_{0,p}(A)$ is defined, then $q_{0,p}(I_G A)$ is also defined. Hence as a consequence of 9.6, $q_{0,p}(A^G)$ is also defined, and we have

$$q_{0,p}(A) = q_{0,p}(A^G) \cdot q_{0,p}(I_G A)\,. \tag{9.9.1}$$

Since G acts trivially on A^G, it follows from 9.5 that $q_{0,p}(A^G) = h(A^G)$.

To determine the quotient $q_{0,p}(I_G A)$ we use the following interesting trick. Since the ideal $\mathbb{Z} \cdot N_G = \mathbb{Z}(\sum_{i=0}^{p-1} \sigma^i)$ annihilates the module $I_G A$, we can consider $I_G A$ as a $\mathbb{Z}[G]/\mathbb{Z} \cdot N_G$-module. Now the ring $\mathbb{Z}[G]/\mathbb{Z} \cdot N_G$ is isomorphic to the ring $\mathbb{Z}[X]/(1 + X + \ldots + X^{p-1})$ with an indeterminate X. But the latter is isomorphic to the ring $\mathbb{Z}[\zeta]$ of integral elements of the field $\mathbb{Q}(\zeta)$ of p-th roots of unity (ζ a primitive p-th root of unity), and the map $\sigma \mapsto \zeta$ induces an isomorphism $\mathbb{Z}[G]/\mathbb{Z} \cdot N_G \cong \mathbb{Z}[\zeta]$. In $\mathbb{Z}[\zeta]$ we now have the well-known decomposition $p = (\zeta - 1)^{p-1} \cdot e$, e a unit, so that we can write

$$p = (\sigma - 1)^{p-1} \cdot \varepsilon, \quad \varepsilon \text{ unit in } \mathbb{Z}[G]/\mathbb{Z} \cdot N_G\,.$$

Since the endomorphism induced by ε is an automorphism on $I_G A$, we find $q_{0,\varepsilon}(I_G A) = 1$. If we now apply Lemma 9.8, we obtain

$$q_{0,p}(I_G A) = q_{0,D^{p-1}}(I_G A) \cdot q_{0,\varepsilon}(I_G A) = q_{0,D}(I_G A)^{p-1} = 1/q_{D,0}(I_G A)^{p-1}\,.$$

Since $N = N_G$ is the 0-endomorphism on $I_G A$, we also have

$$q_{0,p}(I_G A) = 1/q_{D,0}(I_G A)^{p-1} = 1/q_{D,N}(I_G A)^{p-1} = 1/h(I_G A)^{p-1}\,.$$

In combination with (9.9.1), this implies

$$q_{0,p}(A^G) = h(A^G), q_{0,p}(I_G A) = 1/h(I_G A)^{p-1}, q_{0,p}(A) = q_{0,p}(A^G)/h(I_G A)^{p-1}\,.$$

On the other hand, the sequence $0 \to A^G \to A \to I_G A \to 0$ gives the formula

$$h(A)^{p-1} = h(A^G)^{p-1} \cdot h(I_G A)^{p-1}\,.$$

and the claim $h(A)^{p-1} = q_{0,p}(A^G)^p / q_{0,p}(A)$ follows by substitution.

In global class field theory we will apply this theorem to certain unit groups, about which we only know that they are finitely generated of known rank. We show that this alone suffices to compute the Herbrand quotient; namely, from 9.9 we get the following theorem of C. Chevalley:

Theorem 9.10 Let A be a finitely generated G-module, where G is a cyclic group of prime order p: If α (resp. β) denotes the rank of the abelian group A (resp. A^G), then the Herbrand quotient $h(A)$ is given by the formula

$$h(A) = p^{(p \cdot \beta - \alpha)/(p-1)}\,.$$

Proof We can decompose A into its torsion group A_0 and its torsion-free part $A_1 : A = A_0 \oplus A_1$. If follows that $A^G = A_0^G \oplus A_1^G$. Since A is finitely generated, A_0 is a finite group, rank $A_1 =$ rank $A = \alpha$ and rank $A_1^G =$ rank $A^G = \beta$. Thus

$$h(A)^{p-1} = h(A_1)^{p-1} = q_{0,p}(A_1^G)^p / q_{0,p}(A_1)\,,$$

where $q_{0,p}(A_1^G) = (A_1^G : pA_1^G) = p^\beta$ and $q_{0,p}(A_1) = (A_1 : pA_1) = p^\alpha$.

10 The cup product

In the previous section we have seen that the restriction and corestriction maps are given by canonical data in dimension $q = 0$, and induce corresponding maps on cohomology in all dimensions. The same principle applies to the **cup product**, which in dimension 0 is just the **tensor product**.

Let A and B be G-modules. Then $A \otimes B$ is a G-module, and the map $(a, b) \mapsto a \otimes b$ induces a canonical bilinear mapping

$$A^G \times B^G \to (A \otimes B)^G \,,$$

which maps $N_G A \times N_G B$ to $N_G(A \otimes B)$. Hence it induces a bilinear mapping

$$H^0(G, A) \times H^0(G, B) \to H^0(G, A \otimes B) \text{ by } (\overline{a}, \overline{b}) \mapsto \overline{a \otimes b} \,.$$

We call the element $\overline{a \otimes b} \in H^0(G, A \otimes B)$ the **cup product** of $\overline{a} \in H^0(G, A)$ and $\overline{b} \in H^0(G, B)$, and denote it by

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

This cup product in dimension 0 extends to arbitrary dimensions:

Definition 10.1 There exists a uniquely determined family of bilinear mappings, the **cup product**

$$\cup : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B), p, q \in \mathbb{Z} \,,$$

with the following properties:

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

$$(\overline{a}, \overline{b}) \mapsto \overline{a} \cup \overline{b} = \overline{a \otimes b}, \quad \overline{a} \in H^0(G, A), \overline{b} \in H^0(G, B) \,.$$

(ii) If the sequences of G-modules

$$\begin{gathered} 0 \to A \to A' \to A'' \to 0 \\ 0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0 \end{gathered}$$

are both exact, then the following diagram commutes

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

so that $\delta(\overline{a}'' \cup \overline{b}) = \delta\overline{a}'' \cup \overline{b}, \overline{a}'' \in H^p(G, A''), \overline{b} \in H^q(G, B)$.

(iii) If the sequences of G-modules

$$0 \to B \to B' \to B'' \to 0$$
$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$$

are both exact, then the following diagram commutes

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

i.e., we have $\delta(\overline{a} \cup \overline{b}'') = (-1)^p(\overline{a} \cup \delta\overline{b}''), \overline{a} \in H^p(G,A), \overline{b}'' \in H^q(G,B'')$.

The factor $(-1)^p$ in the last diagram is necessary and results from the anticommutativity of the connecting homomorphism δ, see below. One cannot define a reasonable cup product omitting this factor.

As with the general restriction maps, we obtain the general cup product from the case $p = 0$, $q = 0$ by dimension shifting.

We recall that we identify the G-modules $A \otimes B$ and $B \otimes A$ as well as the G-modules $(A \otimes B) \otimes C$ and $A \otimes (B \otimes C)$. This automatically leads to a corresponding identification of the cohomology groups of these G-modules. In particular, we can write:

$A^p \otimes B = J_G \otimes \ldots \otimes J_G \otimes A \otimes B = (A \otimes B)^p$ and

$A \otimes B^q = A \otimes J_G \otimes \ldots \otimes J_G \otimes B = J_G \otimes \ldots \otimes J_G \otimes A \otimes B = (A \otimes B)^q$

for $p, q \leq 0$, and analogously for $p, q \leq 0$ with I_G in place of J_G. We will use this freely below.

Because of Proposition 3.15 we may start with the case $q = 0$, $p = 0$ and determine the cup product by the following commutative diagram:

(10.1.1)
$$\begin{array}{ccccc} H^0(G,A^p) \times H^0(G,B^q) & \xrightarrow{\cup} & H^0(G,(A \otimes B^q)^p) = H^0(G, A^p \otimes B^q) \\ \downarrow{\scriptstyle \delta^p} \qquad \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle \delta^p} \\ H^p(G,A) \times H^0(G,B^q) & \xrightarrow{\cup} & H^p(G,(A \otimes B)^q) = H^p(G, A \otimes B^q) \\ \downarrow{\scriptstyle 1} \qquad \downarrow{\scriptstyle \delta^q} & & \downarrow{\scriptstyle (-1)^{p,q}\delta^q} \\ H^p(G,A) \times H^q(G,B) & \xrightarrow{\cup} & H^{p+q}(G, A \otimes B) \end{array}$$

It follows immediately from the conditions (i), (ii) and (iii) that the cup product is unique. We use this fact to give an explicit description of the cup product in terms of cocycles in the special case $(p,q) = (0,q)$ and $(p,0)$:

Proposition 10.2 If we denote by a_p (resp. b_q) p-cocycles (resp. q-cocycles) of A (resp. B), and by $\overline{a}_p$ (resp. $\overline{b}_q$) their cohomology classes, then

$$\overline{a}_0 \cup \overline{b}_q = \overline{a_0 \otimes b_q} \quad \text{and} \quad \overline{a}_p \cup \overline{b}_0 = \overline{a_p \otimes b_0}\,.$$

For the proof note that the products $\overline{a}_0 \cup \overline{b}_q$ and $\overline{a}_p \cup \overline{b}_0$ defined here satisfy the conditions (i), (ii) and (iii) for $(0, q)$ and $(p, 0)$ respectively. This can be seen directly from the behaviour of the cocycles under the corresponding maps. Now if we consider the lower part of the diagram (10.1.1) for $p = 0$, resp. the upper part for $q = 0$, then we see that the product defined by the commutative diagram (10.1.1) must coincide with the one defined by 10.2.

Thus everything boils down to showing that the product maps defined by (10.1.1)

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

satisfy the conditions (ii) and (iii). To this end, consider the exact sequences

$$0 \to A \to A' \to A'' \to 0\,,$$
$$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$

and

$$0 \to B \to B' \to B'' \to 0\,,$$
$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0\,.$$

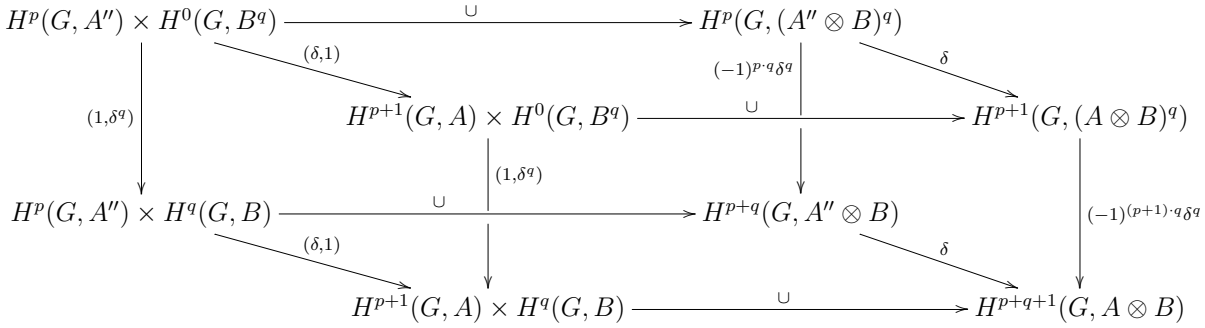
From these we get by 1.9 und 1.2 the exact sequences

$$0 \to A^q \to A'^q \to A''^q \to 0$$
$$0 \to (A \otimes B)^q \to (A' \otimes B)^q \to (A'' \otimes B)^q \to 0$$

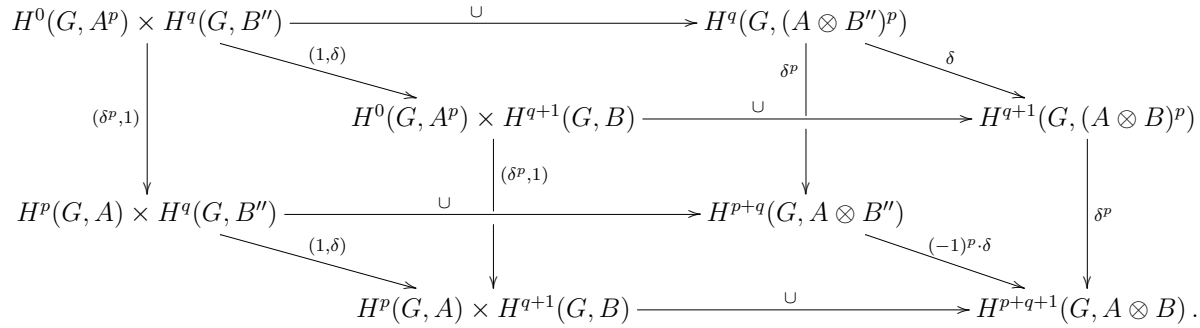
and

$$0 \to B^p \to B'^p \to B''^p \to 0$$
$$0 \to (A \otimes B)^p \to (A \otimes B')^p \to (A \otimes B'')^p \to 0\,,$$

and we have the diagrams



and



Here the left sides in both diagrams commute for trivial reasons. The right sides are composed from q (resp. p) squares as in 3.6, thus they commute as well. The front and back sides commute by definition (10.1.1) of the cup product, and the upper squares commute because 10.2 and the remarks following it. Since the vertical maps are bijective, the commutativity of the upper squares implies the commutativity of the lower squares. This completes the proof.

The axiomatic definition of the cup product in 10.1 does not give us an explicit description of it, i.e., given two cohomology classes in terms of cocycles, we are for now not in a position to decide which cocycle represents their cup product in general. Only for the cases $(p,q)=(0,q)$ and $(p,0)$ we have such a description by 10.2. The attempt to give an explicit description of the cup product for general p,q (in particular for $p<0$ and $q<0$) leads, however, to major computational problems. Thus we find ourselves in a situation which is similar to that of the restriction map, which admits a very simple description in dimensions $q\geq 0$, but not for negative dimensions. Nevertheless in both cases we will need explicit computations only in low dimensions; given these, one can manage knowing the functorial properties of these maps.

Before giving explicit formulas for small dimension, we want to convince ourselves that the cup product is compatible with the usual cohomological maps defined above.

Proposition 10.3 Let $f:A\to A'$ and $g:B\to B'$ be two G-homomorphisms, and let $f\otimes g:A\otimes B\to A'\otimes B'$ be the G-homomorphism induced by f and g. If $\overline{a}\in H^p(G,A)$ and $\overline{b}\in H^q(G,B)$, then

$$\overline{f}(\overline{a})\cup\overline{g}(\overline{b})=\overline{f\otimes g}(\overline{a}\cup\overline{b})\in H^{p+q}(G,A'\otimes B')\,.$$

This is completely trivial or $p=q=0$, and follows in general from a simple dimension shifting argument. We have demonstrated this technique already frequently enough to leave the details to the reader.

Proposition 10.4 Let A,B be G-modules, and let g be a subgroup of G. If $\overline{a}\in H^p(G,A)$ and $\overline{b}\in H^q(G,B)$, then

$$\operatorname{res}(\overline{a}\cup\overline{b})=\operatorname{res}\overline{a}\cup\operatorname{res}\overline{b}\in H^{p+q}(g,A\otimes B)\,,$$

and

$$\operatorname{cor}(\operatorname{res}\overline{a} \cup \overline{b}) = \overline{a} \cup \operatorname{cor}\overline{b} \in H^{p+q}(G, A \otimes B)\,.$$

This follows again from the case $p = q = 0$ by dimension shifting. In case $p = q = 0$ the first formula is immediate. For the second, let $a \in A^G$ and $b \in B^g$ be 0-cocycles representing $\overline{a}$ and $\overline{b}$ respectively. By definition 4.12 of the corestriction in dimension 0, we have

$$\begin{aligned}
\operatorname{cor}(\operatorname{res}\overline{a} \cup \overline{b}) &= \operatorname{cor}(a \otimes b + N_g(A \otimes B)) \\
&= \sum_{\sigma \in G/g} \sigma(a \otimes b) + N_G(A \otimes B) \\
&= \sum_{\sigma \in G/g} a \otimes \sigma b + N_G(A \otimes B) \\
&= a \otimes (\sum_{\sigma \in G/g} \sigma b) + N_G(A \otimes B) \\
&= \overline{a} \cup \operatorname{cor}\overline{b}\,.
\end{aligned}$$

We show that the cup product is anticommutative and associative:

Theorem 10.5 Let $\overline{a} \in H^p(G, A), \overline{b} \in H^q(G, B)$, and $\overline{c} \in H^r(G, C)$. Then

$$\overline{a} \cup \overline{b} = (-1)^{p \cdot q}(\overline{b} \cup \overline{a}) \in H^{p+q}(G, B \otimes A)\,,$$

and

$$(\overline{a} \cup \overline{b}) \cup \overline{c} = \overline{a} \cup (\overline{b} \cup \overline{c}) \in H^{p+q+r}(G, A \otimes (B \otimes C))$$

under the canonical isomorphisms $H^{p+q}(G, A \otimes B) \cong H^{p+q}(G, B \otimes A)$ and $H^{p+q+r}(G, (A \otimes B) \otimes C) = H^{p+q+r}(G, A \otimes (B \otimes C))$.

Again, this is trivial for $p = q = 0$, and follows in general by dimension shifting.

We now want to compute some explicit formulas for the cup product. For this we denote by a_p (resp. b_q) p-cocycles of A (resp. q-cocycles of B), and write $\overline{a}_p$ (resp. $\overline{b}_q$) for their cohomology classes in $H^p(G, A)$ (resp. $H^q(G, B)$).

Lemma 10.6 We have $\overline{a}_1 \cup \overline{b}_{-1} = \overline{x}_0 \in H^0(G, A \otimes B)$ with

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

Proof By 3.14 we have the G-induced G-module $A' = \mathbb{Z}[G] \otimes A$ and the exact sequences

$$\begin{aligned}
0 \to A \to A' \to A'' \to 0\,, \\
0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0\,.
\end{aligned}$$

We think of A embedded in A' and $A \otimes B$ embedded in $A' \otimes B$; to simplify notation we do not explicitly write out these homomorphisms. Because of the vanishing $H^1(G, A') = 0$, there is a 0-cochain $a'_0 \in A'$ with $a_1 = \partial a'_0$, so that

$$a_1(\tau) = \tau a'_0 - a'_0 \quad \text{for all} \quad \tau \in G\,. \tag{10.6.1}$$

Let $a_0'' \in A''^G$ be the image of a_0' in A''. By definition of the connecting homomorphism δ, we have $\overline{a}_1 = \delta(\overline{a_0''})$, and we obtain

$$\begin{aligned}
\overline{a} \cup \overline{b}_{-1} &= \delta(\overline{a_0''}) \cup \overline{b}_{-1} \overset{(10.1)}{=} \delta(\overline{a_0'' \cup \overline{b}_{-1}}) \overset{(10.2)}{=} \delta(\overline{a_0'' \otimes \delta b_{-1}}) = \overline{\partial(a_0'' \otimes \delta b_{-1})} \\
&= \overline{N_G(a_0' \otimes b_{-1})} = \overline{\sum_{\tau \in G} \tau a_0' \otimes \tau b_{-1}} \overset{(*)}{=} \overline{\sum_{\tau \in G} (a_1(\tau) + a_0') \otimes \tau b_{-1}} \\
&= \overline{\sum_{\tau \in G} (a_1(\tau) \otimes \tau b_{-1})} + \overline{a_0' \otimes N_G b_{-1}} = \overline{\sum_{\tau \in G} (a_1(\tau) \otimes \tau b_{-1})}
\end{aligned}$$

because $N_G b_{-1} = 0$.

In the following we restrict to the case $B = \mathbb{Z}$ and identify $A \otimes \mathbb{Z}$ with A via $a \otimes n \mapsto a \cdot n$. Recall that from 3.19 we have the canonical isomorphism

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

If $\sigma \in G$, let $\overline{\sigma}$ be the element in $H^{-2}(G, \mathbb{Z})$ corresponding to $\sigma \cdot G' \in G^{\mathrm{ab}}$.

Lemma 10.7 $\overline{a}_1 \cup \overline{\sigma} = \overline{a_1(\sigma)} \in H^{-1}(G, A)$.

Proof From the exact sequence

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

we obtain the isomorphism $H^{-1}(G, A) \overset{\delta}{\to} H^0(G, A \otimes I_G)$. Thus it suffices to show $\delta(\overline{a}_1 \cup \overline{\sigma}) = \delta(\overline{a_1(\sigma)})$. Using the definition of δ, we now compute

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

On the other hand, the proof of 3.19 shows that under the isomorphism $H^{-2}(G, \mathbb{Z}) \overset{\delta}{\to} H^{-1}(G, I_G)$ the element $\overline{\sigma}$ goes to $\delta\overline{\sigma} = \overline{\sigma - 1}$, hence we have

$$\delta(\overline{a}_1 \cup \overline{\sigma}) \overset{(10.1)}{=} -(\overline{a}_1 \cup \delta(\overline{\sigma})) = -\overline{a}_1 \cup (\overline{\sigma - 1}) = \overline{y}_0 .$$

For the cocycle y_0 we obtain from 10.6

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

The 1-cocycle $a_1(\tau)$ satisfies $a_1(\tau) = a_1(\tau\sigma) - \tau a_1(\sigma)$. Substituting this into the last sum, we find

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

Therefore $y_0 - x_0 = \sum_{\tau \in G} \tau a_1(\sigma) \otimes \tau(\sigma - 1) = N_G(a_1(\sigma) \otimes (\sigma - 1))$, which shows that $\overline{x}_0 = \overline{y}_0$.

The following formula 10.8 is of particular interest for us. Note that if we take an element $\overline{a}_2$ in the group $H^2(G,A)$, it provides us with the homomorphism

$$\overline{a}_2 \cup : H^{-2}(G,\mathbb{Z}) \to H^0(G,A)\,,$$

which maps each $\overline{\sigma} \in H^{-2}(G,\mathbb{Z})$ to the cup product $\overline{a}_2 \cup \overline{\sigma} \in H^0(G,A)$; we thus get a canonical mapping from the abelianization G^{ab} to the norm residue group $A^G/N_G A$. In class field theory we will consider a special G-module A for which the homomorphism will be shown to be bijective; in fact, the resulting canonical isomorphism $G^{\mathrm{ab}} \cong A^G/N_G A$ is the main theorem of class field theory. For this the following proposition will be important.

Proposition 10.8 We have $\overline{a}_2 \cup \overline{\sigma} = \overline{\sum_{\tau\in G} a_2(\tau,\sigma)} \in H^0(G,A)$.

Proof We consider again the G-module $A' = \mathbb{Z}[G] \otimes A$ and the exact sequence $0 \to A \to A' \to A'' \to 0$ ($A'' = J_G \otimes A$). Since $H^2(G,A') = 0$ there is a 1-cochain $a_1' \in A_1'$ with $a_2 = \partial a_1'$ i.e.,

$$a_2(\tau,\sigma) = \tau a_1'(\sigma) - a_1'(\tau\cdot\sigma) + a_1'(\tau)\,. \tag{10.8.1}$$

The image a_1'' of a_1' is a 1-cocycle of A'' such that $\overline{a}_2 = \delta(\overline{a_1''})$. Therefore

$$\begin{aligned}\overline{a}_2 \cup \overline{\sigma} \quad &= \quad \delta(\overline{a_1''}) \cup \overline{\sigma} \overset{(10.1)}{=} \delta(\overline{a_1''} \cup \overline{\sigma}) \overset{(10.7)}{=} \delta(\overline{a_1''(\sigma)}) = \overline{\partial(a_1'(\sigma))} = \overline{\sum_{\tau\in G} \tau a_1'(\sigma)} \\ &\overset{(10.8.1)}{=} \overline{\sum_{\tau\in G} a_2(\tau\sigma)} + \overline{\sum_{\tau\in G} a_1'(\tau\cdot\sigma) - \sum_{\tau\in G} a_1'(\tau)} = \overline{\sum_{\tau\in G} a_2(\tau,\sigma)}\,.\end{aligned}$$

11 The corestriction

Similar to restriction, we define corestriction using an axiomatic approach:

Definition 11.1 Let G be a finite group and let g be a subgroup of G. Then **corestriction** is the uniquely determined family of homomorphisms

$$\mathrm{cor}_q : H^q(g, A) \to H^q(G, A), \quad q \in \mathbb{Z}\,,$$

with the properties:

(i) If $q = 0$, then

$$\mathrm{cor}_0 : H^0(g, A) \to H^0(G, A),\ a + N_g A \mapsto N_{G/g} a + N_G A\ (a \in A^g)\,.$$

(ii) For every exact sequence $0 \to A \to B \to C \to 0$ of G-modules and G-homomorphisms, the following diagram is commutative

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

Exactly as for the restrictions, the homomorphisms cor_q arise from the corestriction cor_0 in dimension 0 by dimension shifting:

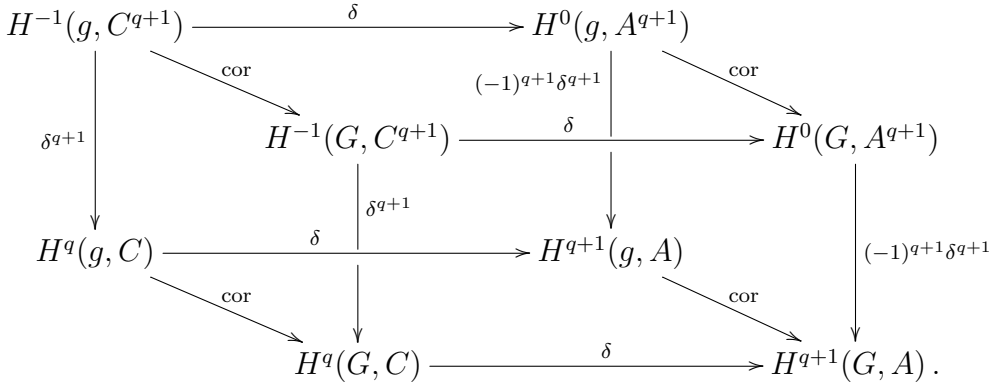
From 3.15 we have the isomorphisms

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

and by (ii) the map cor_q is uniquely determined by the commutative diagram

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

In particular, because of uniqueness and 4.11 we recover the homomorphism cor_{-1} introduced on p. 38. The fact that (ii) holds is verified in the same way as for restriction using the following diagram, together with 4.11 and 3.6,



We remark that one can define the corestriction for negative dimensions very easily by a canonical correspondence between cochains, analogously to the restrictions for positive dimension. However, we will not pursue this further. In view of 4.10 we now want to prove the following theorem

Theorem 11.2 Let $g \subseteq G$ be a subgroup. The homomorphism

$$\kappa : g^{\mathrm{ab}} \to G^{\mathrm{ab}}$$

induced by the corestriction $\mathrm{cor}_{-2} : H^{-2}(g, \mathbb{Z}) \to H^{-2}(G, \mathbb{Z})$ coincides with the canonical homomorphism induced by $\sigma g' \mapsto \sigma G'$.

This follows, using the proof of 3.19, from the commutative diagram

$$\begin{array}{ccccc} H^{-2}(g,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(g, I_g) = I_g/I_g^2 & \xleftarrow[\sim]{\log} & g^{\mathrm{ab}} \\ \downarrow{\scriptstyle \mathrm{cor}_{-2}} & & \downarrow{\scriptstyle \mathrm{cor}_{-1}} & & \downarrow{\scriptstyle \kappa} \\ H^{-2}(G,\mathbb{Z}) & \xrightarrow{\delta} & H^{-1}(G, I_G) = I_G/I_G^2 & \xleftarrow[\sim]{\log} & G^{\mathrm{ab}} . \end{array}$$

The following relation between restriction and corestriction is important.

Theorem 11.3 Let $g \subseteq G$ be a subgroup. Then the composition

$$H^q(G, A) \xrightarrow{\mathrm{res}} H^q(g, A) \xrightarrow{\mathrm{cor}} H^q(G, A)$$

is the endomorphism

$$\mathrm{cor} \circ \mathrm{res} = (G : g) \cdot \mathrm{id} \ .$$

Proof Consider the case $q = 0$. If $\overline{a} = a + N_G A \in H^0(G, A), a \in A^G$, then $\mathrm{cor}_0 \circ \mathrm{res}_0(\overline{a}) = \mathrm{cor}_0(a + N_g A) = N_{G/g} a + N_G A = (G : g) \cdot a + N_G A = (G : g) \cdot \overline{a}$. The general case follows from this by dimension shifting. In fact, the diagram

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

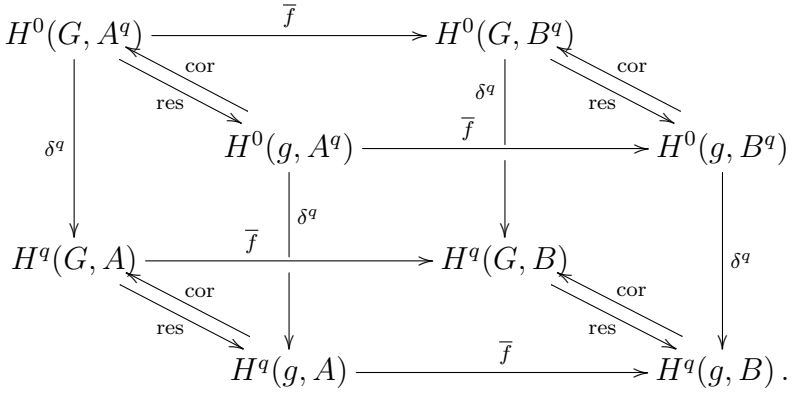
commutes and since the upper horizontal map is $(G : g) \cdot \mathrm{id}$, it follows that the same holds for the lower horizontal map, i.e., $\mathrm{cor}_q \circ \mathrm{res}_q = (G : g) \cdot \mathrm{id}$.

Because the restriction and corestriction maps res and cor commute with the connecting homomorphism δ, they also commute with maps induced by G-homomorphisms:

Proposition 11.4 If $f : A \to B$ is a G-homomorphism of the G-modules A, B, and g is a subgroup of G, then the following diagram commutes

$$\begin{array}{ccc} H^q(G,A) & \xrightarrow{\overline{f}} & H^q(G,B) \\ {\scriptstyle \text{res}}\downarrow\uparrow{\scriptstyle \text{cor}} & & {\scriptstyle \text{res}}\downarrow\uparrow{\scriptstyle \text{cor}} \\ H^q(g,A) & \xrightarrow{\overline{f}} & H^q(g,B)\,. \end{array}$$

This is clear in case of dimension $q = 0$, and the general case follows easily by dimension shifting. In fact, the homomorphism $f : A \to B$ induces a homomorphism $f : A^q \to B^q$, and in the following diagram



all vertical squares are commutative. Hence the commutativity of the lower diagram follows from that of the upper one.

Since the cohomology groups $H^q(G,A)$ are abelian torsion groups, they are direct sums of their **p-Sylow groups**, i.e., the groups $H^q(G,A)_p$ of all elements in $H^q(G,A)$ of p-power order:

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

The group $H^q(G,A)_p$ is often called the **p-primary** part of $H^q(G,A)$. For the restriction and corestriction maps on these p-primary parts we have the following:

Theorem 11.5 Let A be a G-module, and G_p a p-Sylow subgroup of G. Then the restriction

$$\text{res} : H^q(G,A)_p \to H^q(G_p,A)$$

is injective, and the corestriction

$$\text{cor} : H^q(G_p,A) \to H^q(G,A)_p$$

is surjective.

Proof Since $\mathrm{cor} \circ \mathrm{res} = (G : G_p) \cdot \mathrm{id}$, and since $(G : G_p)$ and p are relatively prime, the mapping $H^q(G,A)_p \xrightarrow{\mathrm{cor} \circ \mathrm{res}} H^q(G,A)_p$ is an automorphism. Hence if $x \in H^q(G,A)_p$ and $\mathrm{res}\, x = 0$, it follows immediately from $\mathrm{cor} \circ \mathrm{res}\, x = 0$ that $x = 0$, which shows the injectivity of res on $H^q(G,A)_p$.

On the other hand, $H^q(G_p, A)$ consists of elements whose order is a p-power (cf. 3.16), so that $\mathrm{cor}\, H^q(G_p,A) \subseteq H^q(G,A)_p$. Since $\mathrm{cor} \circ \mathrm{res}$ is a bijection on $H^q(G,A)_p$, this inclusion is an equality.

We often encounter the problem that we want to show that certain cohomology groups vanish. In many of these cases we will use the following consequence of Theorem 11.5, which reduces this problem to the case of p-groups:

Corollary 11.6 If for every prime p the group $H^q(G_p, A) = 0$ for a p-Sylow subgroup G_p of G, then we have $H^q(G,A) = 0$.

Proof Since $res : H^q(G,A)_p \to H^q(G_p, A)$ is injective, the assumption implies that all p-Sylow groups $H^q(G,A)_p$ are trivial; thus $H^q(G,A) = 0$.

We end this section with a generalization of the notion of a G-induced module: we will use this type of G-modules in global class field theory.

Definition 11.7 Let G be a finite group, and let g be a subgroup of G. A G-module A is called G/g**-induced**, if it has a representation

$$A = \bigoplus_{\sigma \in G/g} \sigma D\,,$$

where $D \subseteq A$ is a g-module and σ ranges over a system of left coset representatives of g in G.

For $g = \{1\}$ we obviously recover the G-induced modules from 3.9. As a generalization of the cohomological triviality of G-induced modules, we have the following result, which is often referred to as **Shapiro's Lemma**:

Lemma 11.8 Let $A = \oplus_{\sigma \in G/g} \sigma D$ be a G/g induced G-module. Then

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

this isomorphism is given by the composition

$$H^q(G,A) \xrightarrow{\mathrm{res}} H^q(g,A) \xrightarrow{\overline{\pi}} H^q(g,D)\,,$$

where $\overline{\pi}$ is induced by the natural projection $A \xrightarrow{\pi} D$.

We give a proof using dimension shifting. Let $A = \oplus_{i=1}^m \sigma_i D$, where σ_i ranges over a system of left coset representatives of G/g, in particular let $\sigma_1 = 1$ For $q = 0$ we define a map in the opposite direction of the homomorphism

$$A^G/N_G A \xrightarrow{\mathrm{res}} A^g/N_g A \xrightarrow{\overline{\pi}} D^g/N_g D$$

by $\nu : D^g/N_gD \to A^G/N_GA$, $\nu(d + N_gD) = \sum_{i=1}^m \sigma_i d + N_GA$. It is easy to verify that $(\overline{\pi} \circ \mathrm{res}) \circ \nu = \mathrm{id}$ and $\nu \circ (\overline{\pi} \circ \mathrm{res}) = \mathrm{id}$. Therefore $\overline{\pi} \circ \mathrm{res}$ is bijective.

In case of arbitrary dimension q we now set

$$\begin{array}{lll} A^q = J_G \otimes \cdots \otimes J_G \otimes A & & A^q = I_G \otimes \cdots \otimes I_G \otimes A \\ D^q_* = J_G \otimes \cdots \otimes J_G \otimes D & \text{resp.} & D^q_* = I_G \otimes \cdots \otimes I_G \otimes D \\ D^q = J_g \otimes \cdots \otimes J_g \otimes D & & D^q = I_g \otimes \cdots \otimes I_g \otimes D \end{array}$$

depending on wether $q \geq 0$ or $q \leq 0$. Because $A = \oplus_{i=1}^m \sigma_i D$ we have

$$J_G = J_g \oplus K_1 \quad \text{resp.} \quad I_G = I_g \oplus K_{-1}$$

with the g-induced modules

$$K_1 = \bigoplus_{\tau \in G} \tau \left(\sum_{i=2}^m \mathbb{Z} \cdot \overline{\sigma}_i^{-1} \right) \text{ and } K_{-1} = \bigoplus_{\tau \in G} \tau \left(\sum_{i=2}^m \mathbb{Z} \cdot (\sigma_i^{-1} - 1) \right) .$$

With 1.5 and 3.10 we obtain for all q the canonical g-module decomposition

$$D^q_* = D^q \oplus C^q$$

for some g-induced g module C^q. Using 3.15, we then obtain the diagram

$$\begin{array}{ccccccc} H^0(G, A^q) & \xrightarrow{\mathrm{res}} & H^0(g, A^q) & \xrightarrow{\overline{\pi}_*} & H^0(g, D^q_*) & \xrightarrow{\overline{\rho}} & H^0(g, D^q) \\ \wr \downarrow \delta^q & & \wr \downarrow \delta^q & & & & \wr \downarrow \delta^q \\ H^q(G, A) & \xrightarrow{\mathrm{res}} & H^q(g, A) & & \xrightarrow{\qquad\qquad\overline{\pi}\qquad\qquad} & & H^q(g, D) \, , \end{array}$$

in which the map $\overline{\pi}_* \circ \mathrm{res}$ in the upper row in dimension 0 is bijective, and the following map $\overline{\rho}$ is bijective because of 3.7 and 3.13. Since the composite $A^q \xrightarrow{\pi_*} D^q_* \xrightarrow{\rho} D^q$ is induced by the projection $A \xrightarrow{\pi} D$, we see that this diagram commutes. Thus the bijectivity of the upper map $\overline{\rho} \circ \overline{\pi}_* \circ \mathrm{res}$ implies the bijectivity of the lower map $\overline{\pi} \circ \mathrm{res}$.

12 Local class field theory I

Let K be a local field of characteristic zero. For any normal extension L/K we let

$$H^q(L/K) := H^q(G_{L/K}, L^\times)$$

and let

$$\mathrm{Br}(K) = \varinjlim_{\substack{L/K \\ \text{normal}}} H^2(G_{L/K}, L^\times)$$

be the so-called Brauer group of K. Note that for $L_2/L_1/K$ we have canonical injections

$$\mathrm{Br}(K) \hookrightarrow \mathrm{Br}(L_1) \hookrightarrow \mathrm{Br}(L_2)\,.$$

Theorem 12.1 (So-called second fundamental inequality) For every normal extension L/K the cardinality $|H^2(L/K, L^\times)|$ of $H^2(L/K, L^\times)$ divides $[L : K]$.

12.2 Recall the following notations: If K is a $\mathfrak{p}$-adic local field, then we have

$\mathcal{O}_K = \{x \in K \mid v(x) \leq 0\}$ the valuation ring.

$\mathfrak{p} = \{x \in K \mid v(x) > 0\}$ the maximal ideal in $\mathcal{O}_K$.

$\overline{K} = \mathcal{O}_K/\mathfrak{p}$ the residue field of K.

$U = \mathcal{O} \smallsetminus \mathfrak{p}$ the unit group.

$U^1 = 1 + \mathfrak{p}$ the group of principal units.

$U^n = 1 + \mathfrak{p}^n$ the higher unit groups.

Let q be the cardinality of $\overline{K}$ (If f is the degree of $\overline{K}$ over $\mathbb{F}_p$, then $q = p^f$)

We have a direct composition

$$K^\times = U \times \langle \pi \rangle\,,$$

where $\langle \pi \rangle$ is the infinite cyclic group generated by a prime element π.

One easily sees:

Proposition 12.3 $U/U^1 \cong \overline{K}^\times$, and $U^n/U^{n+1} \cong \overline{K}^+$ for $n \geq 1$.

Proof of Theorem 12.1 First we consider the case where L/K is cyclic of prime degree $p = [L : K]$, and we show that the Herbrand quotient

$$h(L^\times) = |H^2(L/K), L^\times| \,/\, |H^1(L/K, L^\times)|$$

is equal to $p = [L : K]$.

In fact the formula 9.9 gives

$$h(L^\times)^{p-1} = q_{0,p}(K^\times)^p / q_{0,p}(L^\times)\,,$$

where q_0, p is formed with the endomorphisms 0 and p.

Now we have

Lemma 12.4 The group $(K^\times)^m$ has finite index in $K^\times$. In fact

$$(K^\times : (K^\times)^m) = m \cdot q^{v(m)} \cdot |\mu_m(K)| = m \cdot |m|_{\mathfrak{p}}^{-1} \cdot |\mu_m(K)|\,,$$

where $|\mu_m(K)|$ is the number of m-th roots of unity in K and q is the cardinality of the residue field $\overline{K}$ of K.

For the proof we use the Herbrand quotient $q_{0,m}$ formed by the endomorphisms 0 and m. Then, by (9.4.2) we have

$$(K^\times : (K^\times)^m) = q_{0,m}(K^\times) \cdot |\mu_m(K)|\,.$$

From the multiplicativity of $q_{0,m}$ we further obtain

$$q_{0,m}(K^\times) = q_{0,m}(K^\times/U) \cdot q_{0,m}(U/U^n) \cdot q_{0,m}(U^n)\,.$$

Here we have $q_{0,m}(K^\times/U) = q_{0,m}(\mathbb{Z}) = m$ since $K^\times = U \times (\pi)$, $q_{0,m}(U/U^n) = 1$ since U/U^n is finite, and $q_{0,m}(U^n) = (U^n : U^{n+v(m)}) = q^{v(m)}$ by the following Lemma for sufficiently big n, and the fact that $(U^i : U^{i+1}) = q$.

Lemma 12.5 If m is a positive integer, then the map $x \mapsto x^m$ yields an isomorphism

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

for sufficiently large n.

Proof If π is a prime element of $\mathfrak{p}$ and $x = 1 + a\pi^n \in U^n$, then

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

and therefore $x^m \in U^{n+v(m)}$ for sufficiently large n.

To prove that the map is surjective we have to show that for every $a \in \mathcal{O}$ there exists an element $x \in \mathcal{O}$ such that

$$1 + a \cdot \pi^{n+v(m)} = (1 + x\pi^n)^m\,,$$

i.e., $1 + a\pi^{n+v(m)} = 1 + m\pi^n x + \pi^{2n} \cdot f(x)$, where $f(x)$ is an integral polynomial in X. If we set $m = u\pi^{v(m)}$, $u \in U$, we get an equation

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

If $n > v(m)$, Hensel's Lemma gives a solution $x \in \mathcal{O}$.

We now conclude as follows. By Theorem 9.9 we have

$$h(L^\times)^{p-1} = q_{0,p}(K^\times)^p / q_{0,p}(L^\times)\,.$$

Using Lemma 12.4 we get

$$\begin{aligned} q_{0,p}(K^\times) &= (K^\times : (K^\times)^p)/|\mu_p(K)| \\ &= p \cdot q_k^{U_K(p)} \\ q_{0,p}(L^\times) &= (L^\times : (L^\times)^p)/|\mu_p(L)| \\ &= p \cdot q_L^{U_L(p)} \end{aligned}$$

If $f = [\overline{L} : \overline{K}]$ is the inertia degree and e is the ramification index, then $p = e \cdot f$, $q_L = q_K^f$ and $v_L(p) = e v_K(p)$.

Substitution in the above formula yields

$$h(L^\times)^{p-1} = p^p \cdot q_K^{pU_K(p)} / p q_K^{e \cdot f \cdot U_K(p)} = p^{p-1}\,,$$

i.e. $h(L^\times) = p$.

The general case follows from this by purely cohomological methods. Since the Galois group $G_{L/K}$ is solvable (see below), there exists a cyclic intermediate field K' over K of prime degree $K \subset K' \subset L$. Since $H^1(L/K') = 1$, the sequence

$$1 \to H^2(K'/K) \xrightarrow{\text{Inf}} H^2(L/K) \xrightarrow{\text{Res}} H^2(L/K')$$

is exact (see Theorem 7.5).

This shows that

$$|H^2(L/K)|/|H^2(L/K')| \cdot |H^2(K'/K)|\,.$$

We have already shown that $|H^2(K'/K)| = [K' : K]$, and when we assume by induction on the field degree that $|H^2(L/K)|/[L : K]$, then it follows that

$$|H^2(L/K)|/[L : K'] \cdot [K' : K] = [L : K]\,.$$

The above proof makes use of the solvability of local Galois groups, which follows immediately from the fact that between K and L one has the cyclic inertia field K'/K, and above K' the tamely ramified cyclic extension K'' which is the ramification field, over which L has p-power degree.

Now we discuss a special case of local class field theory, the unramified class field theory.

An extension L/K of local fields is unramified, if a prime element π in K is also a prime element in L. This is equivalent to the statement that the degree $[L : K]$ is equal to the degree $[\overline{L} : \overline{K}]$ of the residue fields.

An unramified extension L/K is normal, and there is a canonical isomorphism

$$G_{L/K} \xrightarrow{\sim} G_{\overline{L}/\overline{K}}\,,$$

sending $\sigma \in G_{L/K}$ to the map $\overline{\sigma} : \overline{L} \to \overline{L}$ with $\overline{\sigma}(\overline{a}) = \overline{\sigma a} = \sigma a \mod \mathfrak{p}$.

Recall also that the Frobenius automorphism $\varphi_{L/K} \in G_{L/K}$ is the preimage of the morphism $\varphi : \overline{L} \to \overline{L}$, $\overline{a} \mapsto \overline{a}^q$, where q is the cardinality of $\overline{K}$.

The following result is particularly important both in local and global class field theory.

Theorem 12.6 Let L/K be an unramified extension. Then for the group of units U_L one has

$$H^q(G_{L/K}, U_L) = 1 \qquad \text{for all } q\,.$$

Proof If we identify $G_{\overline{L}/\overline{K}}$ with $G_{L/K}$, then

$$1 \to U_L^1 \to U_L \to \overline{L}^\times \to 1$$

is an exact sequence of $G_{\overline{L}/\overline{K}}$-modules. Since $H^q(G_{\overline{L}/\overline{K}}, \overline{L}^\times) = 1$ by Hilbert's Theorem 90, it follows that $H^q(G_{L/K}, U_L) \cong H^q(G_{L/K}, U_L^1)$.

A prime element $\pi \in K$ for $\mathfrak{p}_K$ is also a prime element of $\mathfrak{p}_L$, Thus the map

$$U_L^{n-1} \to \overline{L}^+, \quad 1 + a\pi^{n-1} \mapsto a \mod \mathfrak{P}_L$$

(for $a \in \mathcal{O}_L$) defines a $G_{L/K}$-homomorphism, and from the exact sequence of $G_{L/K}$-modules

$$1 \to U_L^n \to U_L^{n-1} \to \overline{L}^+ \to 0$$

we obtain, using that $H^q(G_{L/K}, L^+) = 0$ for all q (note that $G_{L/K} \cong G_{\overline{L}/\overline{K}}$, the isomorphism

$$H^q(G_{L/K}, U_L^n) \cong H^q(G_{L/K}, U_L^{n-1})\,.$$

This implies that the injection $U_L^n \to U_L$ induces an isomorphism

$$H^q(G_{L/K}, U_L^n) \to H^q(G_{L/K}, U_L)\,.$$

If m is a positive integer, the map $x \mapsto x^m$ defined an isomorphism $U_L^n \to U_L^{n+v(m)}$, provided n is sufficiently large (see 12.2).

Hence we have a homomorphism

$$H^q(G_{L/K}, U_L) \xrightarrow{m} H^q(G_{L/K}, U_L)\,,$$

and an isomorphism

$$H^q(G_{L/K}, U_L^n) \xrightarrow{m} H^q(G_{L/K}, U_L^{m+v(m)})\,.$$

Consider the diagram

$$\begin{array}{ccc} H^q(G_{L/K}, U_L^n) & \longrightarrow & H^q(G_{L/K}, U_L) \\ \Big\downarrow{\scriptstyle m} & & \Big\downarrow{\scriptstyle m} \\ H^q(G_{L/K}, U_L^{n+v(m)}) & \longrightarrow & H^q(G_{L/K}, U_L) \end{array}$$

This diagram commutes, and all maps except for the right vertical map are known to be bijections. Hence is follows that the map

$$H^q(G_{L/K}, U_L) \xrightarrow{m} H^q(G_{L/K}, U_L)$$

that sends a cohomology class c to its m-th power c^m is a bijection, too, for all m. But the elements of $H^q(G_{L/K}, U_L)$ have finite order (see 5.17), so that we must have $H^q(G_{L/K}, U_L) = 1$.

For $q = 0$ we obtain

$$U_K = N_{L/K} U_L \,.$$

13 Three Theorems of Tate

In this chapter we present three important Theorems by Tate.

Theorem 13.1 (Theorem of Cohomological Triviality) Let G be a finite group, and let A be a G-module. If there is a dimension q_0 such that

$$H^{q_0}(g, A) = H^{q_0+1}(g, A) = 0$$

for all subgroups $g \subseteq G$, then A has trivial cohomology, i.e., $H^q(g, A) = 0$ for all subgroups $g \subseteq G$ and all $q \in \mathbb{Z}$.

Proof We will reduce the general case to the case of cyclic groups, where the result is an immediate consequence of Theorem 9.1. It is clear that it suffices to show the following claim:

If $H^{q_0}(g, A) = H^{q_0+1}(g, A) = 0$ for all subgroups $g \leq G$, then $H^{q_0-1}(g, A) = 0 = H^{q_0+2}(g, A)$.

Moreover, by dimension shifting, it suffices to consider the case $q_0 = 1$. Hence assume that $H^1(g, A) = 0 = H^2(g, A)$ for all subgroups $g \subseteq G$. We have to show that

$$(*) \qquad H^0(g, A) = 0 = H^3(g, A)$$

for all subgroups $g \subset G$.

We prove this by induction on the order $|G|$ of G; the case $|G| = 1$ being trivial.

Hence we may assume that $(*)$ holds for all proper subgroups g of G, and it remains to show that $H^0(G, A) = 0 = H^3(G, A)$. This is clear if G is not a p-group, because then all Sylow groups are proper subgroups, and Corollary 11.6 shows that $H^0(G, A) = H^3(G, A) = 0$.

Therefore we may assume that G is a p-group. Then there exists a normal subgroup $H \trianglelefteq G$ such that G/H is cyclic of order p. By the induction assumption we have

$$H^0 = (H, A) = H^1(H, A) = H^2(H, A) = H^3(H, A) = 0\,,$$

and using exercise 1 on sheet 4 as well as Theorem 7.5, we obtain the isomorphisms

$$\mathrm{Inf} : H^q(G/H, A^H) \xrightarrow{\sim} H^q(G, A)$$

for $q = 1, 2, 3$.

Now $H^1(G, A) = 0$ implies $H^1(G/H, A^H) = 0$ hence $H^3(G/H, A^H) = 0$ by Theorem 9.1, and so $H^3(G, A) = 0$.

Furthermore, $H^2(G, A) = 0$ implies $H^2(G/H, A^H) = 0$, hence $H^0(G/H, A^H) = 0$ (by Theorem 9.1). This means $A^G = N_{G/H}A^H = N_{G/H}(N_H A) = N_G A$, where we have used that $H^0(H, A) = 0$, so that $A^H = N_H A$. Hence $H^0(G, A) = 0$, which proves the Theorem.

From the Theorem of cohomological triviality we obtain the following result of Tate:

Theorem 13.2 Let A be a G-module with the following properties: For every subgroup $g \subseteq G$ we have

I $H^{-1}(g, A) = 0$

II $H^0(g, A)$ is a cyclic group of order $|g|$.

If a generates the group $H^0(G, A)$, then the cup product map

$$au : H^q(G, \mathbb{Z}) \to H^q(G, A)$$

is an isomorphism for all $q \in \mathbb{Z}$.

Proof The module A itself is not suitable for the proof, since we need to use the injectivity of the map $\mathbb{Z} \to A$, $n \mapsto na_0$ (where $a = a_0 + N_G A$). Hence we replace A with

$$B = A \oplus \mathbb{Z}[G]$$

which we can do without changing the cohomology groups.

In fact, if $i : A \to B$ is the canonical injection onto the first component of B, then the induced map

$$\tilde{i} : H^q(g, A) \to H^q(g, B)$$

is an isomorphism, because $\mathbb{Z}[G]$ is cohomologically trivial.

Now choose an $a_0 \in A^G$ such that $a = a_0 + N_G A$ is a generator of $H^0(G, A)$. Then the map

$$f : \mathbb{Z} \to B, \quad n \mapsto n \cdot a_0 + n \cdot N_G$$

is injective, because of the second term $n \cdot N_G$, and induces the homomorphism

$$\overline{f} : H^q(g, \mathbb{Z}) \to H^q(g, B)\,.$$

Using Proposition 10.2, we see that the diagram

$$\begin{array}{ccc} H^q(G, \mathbb{Z}) & \xrightarrow{au} & H^q(G, A) \\ & \searrow^{\overline{f}} & \downarrow{\scriptstyle \tilde{i}} \\ & & H^q(G, B) \end{array}$$

commutes; thus it suffices to show $\overline{f}$ is bijective.

This follows easily from Theorem 13.1: Since $f : \mathbb{Z} \to B$ is injective, there is an exact sequence of G-modules

$$0 \to \mathbb{Z} \to B \to C \to 0 \tag{13.1.1}$$

Now $H^{-1}(g,B) = H^{-1}(g,A) = 0$ and $H^1(g,\mathbb{Z}) = 0$ for all $g \subseteq G$, which implies that the exact cohomology sequence for (13.1.1) has the form

$$0 \to H^{-1}(g,C) \to H^0(g,\mathbb{Z}) \xrightarrow{\overline{f}} H^0(g,B) \to H^0(g,C) \to 0\,.$$

If $q = 0$, then $\overline{f}$ is clearly an isomorphism, hence $H^{-1}(g,C) = H^0(g,C) = 0$. Then by Theorem 13.1 we get $H^q(g,C) = 0$ for all q. Hence it follows that $\overline{f} : H^q(G,\mathbb{Z}) \to H^q(G,B)$ is bijective for all q, as claimed.

From Theorem 13.2 we obtain the following, very important result, again due to Tate

Theorem 13.3 Assume A is a G-module with the following properties. For each subgroup $g \subseteq G$ we have

I $H^1(g,A) = 0$

II $H^2(g,A)$ is cyclic of order $|g|$.

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

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

is an isomorphism.

Addendum: If a generates the group $H^2(G,A)$, then $\operatorname{res} a$ generates $H^2(g,A)$.

Proof Consider the dimension shift isomorphism

$$\delta^2 : H^q(g,A^2) \to H^{q+2}(g,A)\,.$$

The assumptions I. and II. imply that $H^{-1}(g,A^2) = 0$, and that $H^0(g,A^2)$ is cyclic of order $|g|$. Furthermore, the generator $a \in H^2(G,A)$ is the image of the generator $\delta^{-2}a \in H^0(G,A^2)$.

It follows from 10.1 that the diagram

$$\begin{array}{ccc} H^q(G,\mathbb{Z}) & \xrightarrow{(\delta^{-2})au} & H^q(G,A^2) \\ \Big\downarrow{\scriptstyle \mathrm{id}} & & \Big\downarrow{\scriptstyle \delta^2} \\ H^q(G,\mathbb{Z}) & \xrightarrow{au} & H^{q+2}(G,A) \end{array}$$

commutes. Since $(\delta^{-2}a)u$ is bijective by Theorem 3.1 the map au is bijective as well.

Addendum: Since $(\operatorname{cor}\circ\operatorname{res})a = (G:g)\cdot a$, the order of the element $\operatorname{res} a \in H^2(g,A)$ is divisible by $|g|$, hence $\operatorname{res} a$ generates $H^2(g,A)$ by II.

For the class field theory, the case $q = -2$ is particularly important. In this case Tate's Theorem yields a canonical isomorphism between

$$G^{\mathrm{ab}} \cong H^{-2}(G,\mathbb{Z}) \text{ and } A^G/N_G A = H^0(G,A)$$

14 Abstract class field theory

Definition 14.1 If G is a profinite group and A is a discrete G-module, the pair (G, A) is called a **formation**.

Let $\{G_K \mid K \in X\}$ be the family of open subgroups of G, and write $A_K = A^{G_K}$ (the fixed module under G_K). Note that $A_K \subset A_L$ if $G_L \subset G_K$.

If G_L is a normal subgroup in G_K, then A_L is a $G_{L/K}$-module, and we write

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

If $N \supseteq L \supseteq K$ is a tower of normal extensions, we have inclusions $G_N \subseteq G_L \subseteq G_K$, with G_N and G_L normal in G_K, and we obtain inflations

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

where we write $G_{L/K}$ for G_K/G_L, i.e.,

$$H^q(L/K) \xrightarrow{\text{Inf}_N} H^q(N/K)$$

for $q \geq 1$. In addition, we also have restriction and corestriction maps

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

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

i.e.,

$$H^q(N/K) \xrightarrow{\text{res}} H^q(N/L) \quad \text{and} \quad H^q(N/L) \xrightarrow{\text{cor}} H^q(N/K).$$

Here we only need to assume that N/K is normal.

If both N and L are normal, then the sequence

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

is exact for $q = 1$, and exact for $q > 1$, if $H^i(N/L) = 0$ for $i = 1, \ldots, q-1$ (see Theorem 7.5).

We call a formation (G, A) a **field formation**, if for every normal extension L/K we have

$$H^1(L/K) = 0\,.$$

In a field formation, the sequence

$$0 \to H^2(L/K) \xrightarrow{\text{inf}_N} H^2(N/K) \xrightarrow{\text{res}_L} H^2(N/L)$$

is always exact for $N \supseteq L \supseteq K$.

In particular, if $N \supseteq L \supseteq K$ are normal extensions, then we can always regard $H^2(L/K)$ as embedded in $H^2(N/K)$, since the inflation

$$H^2(L/K) \xrightarrow{\mathrm{Inf}_N} H^2(N/K)$$

is injective.

If L ranges over all normal extensions of K, then the groups $H^2(L/K)$ form a direct system of groups with respect to the inflation maps, and taking the inductive limit

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

we obtain a group $H^2(\ \ /K)$ in which all groups $H^2(L/K)$ are embedded. For $N \supseteq L \supseteq K$ as above we have

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

We will regard all maps here as inclusions.

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

$$H^2(\ \ /K) \xrightarrow{\mathrm{res}_{K'}} H^2(\ \ /K')\,. \tag{14.1.1}$$

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

$$H^2(L/K) \xrightarrow{\mathrm{res}_{K'}} H^2(L/K') \tag{$*$}$$

defines an element

$$\mathrm{res}_{K'}(c) \in H^2(L/K') \subseteq H^2(\ \ /K)\,,$$

This map can easily be seen to be independent of the choice of the field $L \supseteq K'$

The restriction of $(*)$ to $H^2(L/K)$ gives back the usual restriction map

$$H^2(L/K) \to H^2(L/K')\,.$$

From this we obtain:

Proposition 14.2 Let (G, A) be a field formation. If K'/K is normal, then

$$1 \to H^2(K'/K) \xhookrightarrow{\mathrm{Inf}} H^2(\ \ /K) \xrightarrow{\mathrm{Res}} H^2(\ \ /K')$$

is exact.

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

$$G_{L/K}^{\mathrm{ab}} \cong A_K/N_{L/K}A_L \tag{14.2.1}$$

for every normal extension L/K, where $G_{L/K^{\mathrm{ab}}}$ is the abelianization of $G_{L/K}$, and $N_{L/K}A_L = N_{G_{L/K}}A_L$ is the norm group of A_L.

By Tate's Theorem 13.3 we can force the existence of such an isomorphism by postulating: If L/K is any extension, then

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

II. $H^2(L/K)$ is cyclic of order $[L : K]$.

Then the cup product with some generators a of $H^2(L/K)$ gives an isomorphism as in (14.2.1).

However the choice of a is not canonical. In order to get some canonical choice, we replace II by the condition that there is an isomorphism between $H^2(L/K)$ and the cyclic group $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, the so-called "invariant map" which uniquely determines the element $u_{L/K} \in H^2(L/K)$ with image $\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$.

The crucial point here is that this element remains "correct" when passing to extension fields and subfields, which we assume by imposing certain compatibility conditions on the invariant maps.

This leads to the following:

Definition 14.3 A formation (G, A) is called a **class formation** if it satisfies the following axioms:

I $H^1(L/K) = 0$ for every normal extension (field formation)

II For every normal extension there is an isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K) \xrightarrow{\sim} \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}\,,$$

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

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

$$\mathrm{inv}_{L/K} = \mathrm{inv}_{N/K}\,|_{H^2(L/K)}\ .$$

(b) If $N \supset L \supset K$ is a tower with N/K normal, then

$$\mathrm{inv}_{N/L} \circ \mathrm{res}_L = [L : K] \cdot \mathrm{inv}_{N/K}\ .$$

Remark 14.4 II b) becomes almost obvious, if one replaces it by the commutative diagram

$$\begin{array}{ccc} H^2(N/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \\ {\scriptstyle \mathrm{res}_L}\downarrow & & \downarrow{\scriptstyle \cdot[L:K]} \\ H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z} \end{array} \tag{14.4.1}$$

The extension property II a) of the invariant implies that for $H^2(\ \ /K) \bigcup\limits_L H^2(L/K)$ there is an injective homomorphism

$$\mathrm{inv}_K : H^2(\ \ /K) \to \mathbb{Q}/\mathbb{Z}\,.$$

By II b) we get the following for this map: If L/K is an arbitrary extension of K, then

$$\mathrm{inv}_L \circ \mathrm{res}_L = [L:K] \cdot \mathrm{inv}_K\,,$$

where $\mathrm{res}_L : H^2(\ \ /K) \to H^2(\ \ /K)$ is the canonical map (see (14.1.1)).

Conversely, from the above formula we recover II b), since $\mathrm{inv}_{N/L}$ (resp. $\mathrm{inv}_{N/K}$) is the restriction of inv_L (resp inv_K) to $H^2(N/L)$ (resp. $H^2(N/K)$).

Taken together with the formulas of Axiom II, we obtain the following formulae:

Proposition 14.5 Let $N \supseteq L \supseteq K$ be extensions with N/K normal. Then

a) $\mathrm{inv}_{N/K}\, c = \mathrm{inv}_{L/K}\, c$ if L/K is normal and $c \in H^2(L/K) \subseteq H^2(N/K)$.

b) $\mathrm{inv}_{N/L}(\mathrm{res}_L\, c) = [L:K] \cdot \mathrm{inv}_{N/K}\, c$ if $c \in H^2(N/K)$

c) $\mathrm{inv}_{N/K}(\mathrm{cor}_K\, c) = \mathrm{inv}_{N/L}\, c$ for $c \in H^2(N/L)$.

Proof a) and b) are just restatements of the formulae in Axiom II.

c): The commutative diagram (14.4.1) immediately implies that the map $H^2(N/K) \xrightarrow{\mathrm{Res}_L} H^2(N/L)$ is surjective. Hence for every $c \in H^2(N/L)$ we have $c = \mathrm{Res}_L\, \tilde{c}$ for some $\tilde{c} \in H^2(N/K)$, and hence $\mathrm{cor}_K(c) = \mathrm{cor}(K)(\mathrm{res}_L\, \tilde{c}) = \tilde{c}^{[L:K]}$ (see 11.3). Hence, by b), $\mathrm{inv}_{N/K}(\mathrm{cor}_K\, c) = [L:K] \cdot \mathrm{inv}_{N/K}(\tilde{c}) = \mathrm{inv}_{N/L}(\mathrm{res}\, \tilde{c}) = \mathrm{inv}_{N/L}(c)$.

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

Definition 14.6 Let L/K be a normal extension. The unique element $u_{L/K} \in H^2(L/K)$ such that

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

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

From the properties of the invariant maps we obtain

Proposition 14.7 Let $N \supseteq L \supseteq K$ be extensions with N/K normal. Then

a) $u_{L/K} = (u_{N/K})^{[N:L]}$, if L/K is normal.

b) $\mathrm{res}_L(u_{N/K}) = u_{N/L}$

c) $\mathrm{cor}_K(u_{N/L} = (u_{N/K})^{[L:K]}$

Proof Since two cohomology classes are equal if they have the same invariants, the claim follows from:

$$\begin{aligned}
\text{a)}\quad \mathrm{inv}_{N/K}((u_{N/L})^{[N:L]}) &= [N:L]\,\mathrm{inv}_{N/K}(u_{N/K}) \\
&= \tfrac{[N:L]}{[N:K]} + \mathbb{Z} = \tfrac{1}{[L:K]} + \mathbb{Z}
\end{aligned}$$

$$\begin{aligned}
\text{b)}\quad \mathrm{inv}_{N/L}(\mathrm{res}_L(u_{L/K} &= [L:K] \cdot \mathrm{inv}_{N/K}(u_{N/K}))) \\
&= \tfrac{[L:K]}{[N:K]} + \mathbb{Z} = \tfrac{1}{[N:L]} + \mathbb{Z}
\end{aligned}$$

$$\begin{aligned}
\text{c)}\quad \mathrm{inv}_{N/K}(\mathrm{cor}_K(u_{N/L})) &= \mathrm{inv}_{N/L}(u_{N/L}) = \tfrac{1}{[N:L]} + \mathbb{Z} \\
&= \tfrac{[L:K]}{[N:K]} + \mathbb{Z} \\
&= [L:K] \cdot \mathrm{inv}_{N/K}(u_{N/K}) \\
&= \mathrm{inv}_{N/K}((u_{N/K})^{[L:K]})\,.
\end{aligned}$$

Now we apply Tate's Theorem 3.3 and get:

Main Theorem 14.8 Let L/K be a normal extension. Then the map

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

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

For $q = 1, 2$ we immediately get:

Corollary 14.9 $H^3(L/K) = 0$ and $H^4(L/K) = \chi(G_{L/K})$.

Proof We have $H^3(L/K) \cong H^1(G_{L/K}, \mathbb{Z}) = \mathrm{Hom}(G_{L/K}, \mathbb{Z}) = 0$ and $H^4(L/K) \cong H^2(G_{L/K}, \mathbb{Z}) \cong H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z}) =: \chi(G_{L/K})$.

Corollary 14.10 For $q = -2$ we get

$$H^{-2}(G_{L/K}, \mathbb{Z}) \cong G_{L/K}^{\mathrm{ab}} \text{ and } H^0(L/K) = A^{G_{L/K}}/N_{L/K}A$$

so that we get an isomorphism

$$\Theta_{L/K} : A^{G_{L/K}}/N_{L/K}A \xrightarrow{\sim} G_{L/K}^{\mathrm{ab}}\,.$$

This isomorphism is called the Nakayama map.

Using Proposition 10.8, we can give an explicit description of this map as follows:

If u is a 2-cocycle representing the fundamental class $u_{L/K}$, then we have

$$\Theta_{L/K}(\sigma G'_{L/K}) = \left[\prod_{\tau \in G_{L/K}} u(\tau, \sigma)\right] \cdot N_{L/K}A_L$$

for all $\sigma G'_{L/K} \in G_{L/K}^{\mathrm{ab}} = G_{L/K}/G'_{L/K}$.

Despite this description, it turns out that the inverse of $\Theta_{L/K}$,

$$A_K/N_{L/K}A_L \to G_{L/K}^{\mathrm{ab}}\,, \tag{14.10.1}$$

which is also called the **reciprocity isomorphism**, is often more accessible and more important. It induces a homomorphism from A_K onto $G_{L/K}^{\mathrm{ab}}$. This homomorphism, $(\quad, L/K)$ is called the norm residue symbol. Hence we have an exact sequence

$$1 \to N_{L/K}A_L \to A_K \xrightarrow{(\quad, L/K)} G_{L/K}^{\mathrm{ab}} \to 1\,,$$

and an element $a \in A_K$ is a norm if and only if $(a, L/K) = 1$.

We note the following relation between the norm residue symbol $(\quad, L/K)$ and the invariant map $\mathrm{inv}_{L/K}$, which will be useful later:

Lemma 14.11 Let L/K be a normal extension, let $a \in A_K$, and $\overline{a} = aN_{L/K}A_L \in H^0(L/K)$. If $\chi \in \chi(G_{L/K}^{\mathrm{ab}}) = H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z})$ is a character, then

$$\chi((a, L/K)) = \mathrm{inv}_{L/K}(\overline{a} \cup \delta_\chi) \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}\,,$$

where δ_χ denotes the image of χ under the isomorphism

$$H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G_{L/K}, \mathbb{Z})$$

which is induced from the exact sequence

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

and the fact that $H^q(G_{L/K}, \mathbb{Q}) = 0$ for the finite group $G_{L/K}$.

Proof Let $\sigma_a = (a, L/K) \in G_{L/K}^{\mathrm{ab}} \cong H^{-2}(G_{L/K}, \mathbb{Z})$, and let $\overline{\sigma}_a$ be the element in $H^{-2}(G_{L/K}, \mathbb{Z})$ associated to σ_a.

By definition of the norm residue symbol, we have

$$\overline{a} = u_{L/K} \cup \overline{\sigma_a} \in H^0(G_{L/K}, A_L)\,.$$

Since the cup product is associative and commutes with the δ-map, we obtain

$$\begin{aligned} \overline{a} \cup \delta_\chi &= (u_{L/K} \cup \overline{\sigma}_a) \cup \delta_\chi = u_{L/K} \cup (\overline{\sigma}_a \cup \delta_\chi) \\ &= u_{L/K} \cup \delta(\overline{\sigma}_a \cup \chi)\,. \end{aligned}$$

By Lemma 10.7 we further have

$$\sigma_{\overline{a}} \cup \chi = \chi(\sigma_a) = \frac{r}{n} + \mathbb{Z} \in \frac{1}{n}\mathbb{Z}/\mathbb{Z} = H^{-1}(G_{L/K}, \mathbb{Q}/\mathbb{Z})\,,$$

where $n = [L : K]$. Hence, taking

$$\delta : H^{-1}(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \to H^0(G_{L/K}, \mathbb{Z})$$

gives

$$\delta(\chi(\sigma_a)) = n(\frac{r}{n} + \mathbb{Z}) = r + n\mathbb{Z} \in H^0(G_{L/K}, \mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}\,,$$

and therefore

$$\overline{a} \cup \delta_\chi = u_{L/K} \cup (r + n\mathbb{Z}) = u_{L/K}^r\,.$$

From this we get

$$\mathrm{inv}_{L/K}(\overline{a} \cup \delta_\chi) = r \cdot \mathrm{inv}_{L/K} = \frac{r}{n} + \mathbb{Z} = \chi(\sigma_a) = \chi((a, L/K))\,.$$

The behaviour of the invariant map under inflation (=inclusion) and restriction map in Axiom II already determines how the norm residue symbol behaves when passing to extensions and subfields:

Theorem 14.12 Let $N \supset L \supset K$ be a tower of extensions with N/K normal. Then the following diagrams are commutative

a)

$$\begin{array}{ccc} A_K & \xrightarrow{(\quad, N/K)} & G_{N/K}^{\mathrm{ab}} \\ {\scriptstyle \mathrm{id}}\downarrow & & \downarrow{\scriptstyle \pi} \\ A_K & \xrightarrow{(\quad, L/K)} & G_{L/K}^{\mathrm{ab}} \end{array}$$

where π is the canonical projection,

b)

$$\begin{array}{ccc} A_L & \xrightarrow{(\quad,N/L)} & G_{N/L}^{\mathrm{ab}} \\ {\scriptstyle \mathrm{incl}}\uparrow & & \uparrow{\scriptstyle \mathrm{Ver}} \\ A_K & \xrightarrow{(\quad,N/K)} & G_{N/K}^{\mathrm{ab}}\,, \end{array}$$

where the so-called Verlagerung Ver is induced by $H^{-2}(G_{N/K},\mathbb{Z}) \xrightarrow{\mathrm{Res}} H^{-2}(G_{N/L},\mathbb{Z})$,

c)

$$\begin{array}{ccc} A_L & \xrightarrow{(\quad,N/L)} & G_{N/L}^{\mathrm{ab}} \\ {\scriptstyle N_{L/K}}\downarrow & & \downarrow{\scriptstyle \kappa} \\ A_K & \xrightarrow{(\quad,N/K)} & G_{N/K}^{\mathrm{ab}} \end{array}$$

where $N_{L/K}$ is the norm and κ is the canonical homomorphism induced by $G_{N/L} \to G_{N/K}$,

d)

$$\begin{array}{ccc} A_K & \xrightarrow{(\quad,N/K)} & G_{N/K}^{\mathrm{ab}} \\ {\scriptstyle \sigma}\downarrow & & \downarrow{\scriptstyle \sigma} \\ A_{\sigma K} & \longrightarrow & G_{\sigma N/\sigma K}^{\mathrm{ab}} \end{array}$$

where, for $\sigma \in G$, the maps $A_K \xrightarrow{\sigma} A_{\sigma K}$ and $G_{N/K}^{\mathrm{ab}} \xrightarrow{\sigma} G_{\sigma N/\sigma K}^{\mathrm{ab}}$ are $a \mapsto \sigma a$ and $\tau \mapsto \sigma\tau\sigma^{-1}$, respectively.

All statements essentially follow from the formulas in Proposition 14.7.

We end this section by a discussion of the so-called norm groups.

Definition 14.13 A subgroup I of A_K is called a **norm group**, if there is an extension A_L of A_K such that $I = N_{L/K}A_L$.

Lemma 14.14 Let L/K be a normal extension, and let L^{ab} be he maximal abelian extension contained in L. Then

$$N_{N/L}A_L = N_{L^{\mathrm{ab}}/K}A_{L^{\mathrm{ab}}} \subseteq A_K\,.$$

Proof The inclusion $N_{L/K}A_L \subseteq N_{L^{\mathrm{ab}}/K}A_{L^{ab}}$ follows from the multiplicativity of the norm. The reciprocity law gives the isomorphism

$$A_K/N_{L/K}A_L \cong G_{L/K}^{\mathrm{ab}} = G_{L^{\mathrm{ab}}/K} \cong A_K/N_{L^{\mathrm{ab}}/K}A_{L^{\mathrm{ab}}}\,,$$

and $(A_K : N_{L/K}A_L) = (A_K : N_{L^{\mathrm{ab}}/K}A_{L^{\mathrm{ab}}}) < \infty$ implies that we have the equality $N_{L/K}A_L = N_{L^{\mathrm{ab}}/K}A_{L^{\mathrm{ab}}}$.

15 Local class field theory II

Now we discuss a special case of local class field theory, the unramified class field theory.

An extension L/K of local fields is unramified, if a prime element π in K is also a prime element in L. This is equivalent to the statement that the degree $[L:K]$ is equal to the degree $[\overline{L}:\overline{K}]$ of the residue fields.

An unramified extension L/K is normal, and there is a canonical isomorphism

$$G_{L/K} \xrightarrow{\sim} G_{\overline{L}/\overline{K}}\,,$$

sending $\sigma \in G_{L/K}$ to the map $\overline{\sigma}: \overline{L} \to \overline{L}$ with $\overline{\sigma}(\overline{a}) = \overline{\sigma a} = \sigma a \mod \mathfrak{p}$.

Definition 15.1 The Frobenius automorphism $\varphi_{L/K} \in G_{L/K}$ is the preimage of the morphism $\varphi: \overline{L} \to \overline{L}$, $\overline{a} \mapsto \overline{a}^q$, where q is the cardinality of $\overline{K}$.

From this we get

Proposition 15.2 Let $N \supseteq L \supseteq K$ be unramified extensions of K. Then

$$\varphi_{L/K} = \varphi_{N/K|L} = \varphi_{N/K} G_{N/L} \in G_{N/L} \quad \text{and} \quad \varphi_{N/L} = \varphi_{N/K}^{[L:K]}\,.$$

Proof This follows easily from the fact that for all $x \in \mathcal{O}_L$ we have

$$(\varphi_{L/K} x) \mod \mathfrak{P}_L = x^{q_k} \mod \mathfrak{P}_L = x^{q_K} \mod \mathfrak{P}_N = (\varphi_{N/K} x) \mod \mathfrak{P}_N\,,$$

and for all $x \in \mathcal{O}_N$ we have

$$(\varphi_{N/L} x) \mod \mathfrak{P}_N = x^{q_L} \mod \mathfrak{P}_N = x^{q_K[L:K]} \mod \mathfrak{P}_N = \varphi_{N/K}^{[L:K]} x \mod \mathfrak{P}_N\,.$$

By Theorem 12.4 we have $H^q(G_{L/K}, U_L) = 1$ for all q. In particular, if L/K is unramified, then

$$U_K = N_{L/K} U_L\,.$$

Hence every unit in K is a norm.

We show now that the unramified extensions form a class formation with respect to the multiplicative group $L^\times$. To do this, we have to specify an invariant map satisfying Axiom II in 14.3 We proceed as follows. From the long exact cohomology sequence associated with the exact sequence

$$1 \to U_L \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0$$

we obtain, using $H^q(G_{L/K}, U_L) = 1$, the isomorphism

$$H^2(G_{L/K}, L^\times) \xrightarrow{\overline{v}} H^2(G_{L/K}, \mathbb{Z})\,.$$

Moreover, the exact sequence

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

and the fact that $\mathbb{Q}$ is cohomologically trivial, implies that the connecting map

$$H^2(G_{L/K}, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G_{L/K}, \mathbb{Q}/\mathbb{Z}) = \chi(G_{L/K})$$

is an isomorphism. If $\chi \in \chi(G_{L/K})$, then $\chi(\varphi_{L/K}) \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}$, and since the Frobenius automorphism $\varphi_{L/K}$ generates the group $G_{L/K}$, the map

$$H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) = \chi(G_{L/K}) \xrightarrow{\varphi} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

is an isomorphism, too. Taking the composition of these three isomorphisms

$$H^2(G_{L/K}, L^\times) \xrightarrow{\overline{v}} H^2(G_{L/K}, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\varphi} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}\,,$$

we obtain the desired map:

Definition 15.3 If L/K is an unramified extension, define

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

to be the isomorphism $\mathrm{inv}_{L/K} = \varphi \circ \delta^{-1} \circ \overline{v}$.

For simplicity we let $H^q(L/K) := H^q(G_{L/K}, L^\times)$.

Theorem 15.4 The formation $(G_{T/K}, T^\times)$ is a class formation with respect to the invariant map of 15.1.

Proof Axiom I is always satisfied by the Theorem of Hilbert-Noether: $H^1(L/K) = 1$.

For the proof of Axiom II a) and b) we need to prove that the following two diagrams commute

$$\begin{array}{ccccccc}
H^2(L/K) & \xrightarrow{\overline{v}} & H^2(G_{L/K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{incl=inf}} & & \downarrow{\scriptstyle \mathrm{inf}} & & \downarrow{\scriptstyle \mathrm{inf}} & & \downarrow{\scriptstyle \mathrm{incl}} \\
H^2(N/K) & \xrightarrow{\overline{v}} & H^2(G_{N/K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{N/K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z}
\end{array}$$

$$\begin{array}{ccccccc}
H^2(N/K) & \xrightarrow{\overline{v}} & H^2(G_{N/K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{N/K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N:K]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \mathrm{res}} & & \downarrow{\scriptstyle \cdot[L:K]} \\
H^2(N/L) & \xrightarrow{\overline{v}} & H^2(G_{N/L}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{N/L}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z}
\end{array}$$

where $N \supseteq L \supseteq K$ are two unramified extensions of K.

But the commuting of the two left squares follows from the functoriality of inf and res, and the middle diagrams are commutative, because Inf and Res commute with the connecting morphism δ.

To prove the commutativity of the right squares, let $\chi_1 \in H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z})$ and $\chi 2 \in H^1(G_{N/K}, \mathbb{Q}/\mathbb{Z})$.

From 15.2 we have the formulas

$$\begin{aligned} \inf \chi(\varphi_{N/K}) &= \chi(\varphi_{N/K} G_{N/L}) = \chi(\varphi_{L/K}) \,, \text{and} \\ \operatorname{res} \chi(\varphi_{N/L}) &= \chi(\varphi_{N/L}) = \chi(\varphi_{N/K}^{[L:K]}) = [L:K]\chi(\varphi_{N/K}) \,. \end{aligned}$$

which completes the proof.

From the extension property II a) of the invariant map, we obtain an injective homomorphism

$$\operatorname{inv}_K : H^2(T/K) \to \mathbb{Q}/\mathbb{Z} \,.$$

This homomorphism is even bijective, since $\mathbb{Q}/\mathbb{Z} = \bigcup_{n=1}^{\infty} \frac{1}{n}\mathbb{Z}/\mathbb{Z}$, and since for every positive integer n there exists (exactly) one unramified extension L/K of degree $n = [L : K]$

Corollary 15.5

$$H^2(T/K) \cong \mathbb{Q}/\mathbb{Z} \,.$$

If L/K is an unramified extension, the Galois group is cyclic and hence coincides with its abelianization. Hence the norm residue symbol has a very simple, explicit description:

Theorem 15.6 Let L/K be unramified, and $a \in K^\times$. Then

$$(a, L/K) = \varphi_{L/K}^{v_K(a)} \,.$$

Proof If $\chi \in \chi(G_{L/K})$, $\delta_\chi \in H^2(G_{L/K}, \mathbb{Z})$ and $\overline{a} = a \cdot N_{L/K} L^\times \in H^0(L/K)$, then

$$\chi(a, L/K) = \operatorname{inv}_{L/K}(\overline{a} \cup \delta_\chi)$$

by Lemma 14.10. This formula, together with 15.3, implies that

$$\begin{aligned} & \chi(a, L/K) = \operatorname{inv}_{L/K}(\overline{a} \cup \delta_\chi) = \varphi \circ \delta^{-1} \circ \overline{v}(\overline{a} \cup \delta_\chi) \\ = \;& \varphi \circ \delta^{-1}(v_K(a) \cdot \delta_\chi) = \varphi(v_K(a) \cdot \chi) = v_K(a) \cdot \chi(\varphi_{L/K}) \\ = \;& \chi(\varphi_{L/K}^{v_k(a)}). \end{aligned}$$

Since this holds for all $\chi \in \chi(G_{L/K})$, it follows that $(a, L/K) = \varphi_{L/K}^{v_K(a)}$.

16 Local class field theory III

Finally we extend the invariant map to arbitrary extensions of local fields. This relies on the following result:

Theorem 16.1 If L/K is a normal extension of local fields, and L'/K is the unramified extension of the same degree $[L' : K] = [L : K]$, then

$$H^2(L/K) = H^2(L'/K) \subseteq H^2(\quad /K)\,.$$

Proof It suffices to show the inclusion

$$H^2(L'/K) \subseteq H^2(L/K)\,.$$

In fact, if this holds, then the inclusion must be an equality, because $|H^2(L'/K)| = [L' : K]$ by15.3, and $|H^2(L/K)|/[L : K]$ by Theorem 12.1.

But if $N = L \cdot L'$, and L'/K is unramified, then N/L is unramified, too (Note: If T is the maximal unramified extension of K, then $T \cdot L$ is the maximal extension of L). Now let $c \in H^2(L'/K) \subseteq H^2(N/K)$. Then it follows from the exact sequence

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

that c lies in $H^2(L/K)$ if and only if $\mathrm{res}_L(c) = 1$. Since $\mathrm{res}_L(c) = 1$ if and only if $\mathrm{inv}_{N/L}(\mathrm{res}_L(c)) = 0$ (see 15.1), our theorem follows once we have shown that

$$\mathrm{inv}_{N/L}(\mathrm{res}_L(c)) = [L : K]\,\mathrm{inv}_{L'/K}(c) \in \frac{1}{[N : L]}\mathbb{Z}/\mathbb{Z}\,, \tag{16.1.1}$$

since $\mathrm{inv}_{L'/K}(c) \in \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, and and hence $[L : K] \cdot \mathrm{inv}_{L'/K}(c) = 0$.

Now (16.1.1) is a special case of the following Lemma.

Lemma 16.2 Let M/K be a normal extension containing the two extensions L/K and L'/K with L'/K unramified. Then $N = L \cdot L'/K$ is also unramified. If $c \in H^2(L'/K) \subseteq H^2(M/K)$, then $\mathrm{res}_L\, c \in H^2(N/L) \subseteq H^2(M/L)$, and

$$\mathrm{inv}_{N/L}(\mathrm{res}_L c) = [L : K] \cdot \mathrm{inv}_{L'/K}\, c\,.$$

Proof The fact that the 2-cocycles of the class $\mathrm{res}_L\, c$ have their values in $N^\times$, implies that $\mathrm{res}_L\, c \in H^2(N/L)$.

Let f be the inertia degree and e the ramification index of the (not necessarily normal) extension L/K. We think of the valuations v_K and v_L as extended to M. Then we have $v_L = e \cdot v_K$. By definition, the invariant map is the composition of the three isomorphisms

$\overline{v}, \delta^{-1}$, and φ. Hence, to prove the above formula it suffices to check that the following diagram commutes:

$$\begin{array}{ccccccc}
H^2(L'/K) & \xrightarrow{\overline{v}_K} & H^2(G_{L'/K}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{L'/K}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[L':K]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \text{incl}} & & \downarrow{\scriptstyle \text{inf}} & & \downarrow{\scriptstyle \text{inf}} & & \downarrow{\scriptstyle \text{incl}} \\
H^2(M/K) & & H^2(G_{M/K}, \mathbb{Z}) & & H^1(G_{M/K}, \mathbb{Q}/\mathbb{Z}) & & \frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z} \\
\downarrow{\scriptstyle \text{res}_L} & & \downarrow{\scriptstyle e\cdot\text{res}} & & \downarrow{\scriptstyle e\cdot\text{res}} & & \downarrow{\scriptstyle \cdot[L:K]} \\
H^2(N/L) & \xrightarrow{\overline{v}_L} & H^2(G_{N/L}, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(G_{N/L}, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\varphi} & \frac{1}{[N:L]}\mathbb{Z}/\mathbb{Z}
\end{array}$$

Here it is understood that the lower vertical maps only map the images of the vertical maps to the cohomology groups in the bottom row.

That the left square commutes follows from the behaviour of the 2-cocycles under the maps in question.

The middle square commutes because he inflation and restriction maps commute with the δ-maps.

To see that the right squre commutes, we have to consider the equation

$$\varphi_{N/L|_{L'}} = \varphi^f_{L'/K}\,,$$

which is a generalization of 15.2. But it is easy to see that, if $a \in L'$, then

$$\begin{array}{rcl}
\varphi_{N/L}(a) & \equiv & a^{q_L} \mod \mathfrak{P}_N \equiv a^{q_k^f} \equiv \mod \mathfrak{P}_{L'} \\
& = & \varphi^f_{L'/K}(a)\,.
\end{array}$$

Now, if $\chi \in H^1(G_{L'/K}\,\mathbb{Q}/\mathbb{Z})$, then

$$\begin{array}{rcl}
[L:K]\cdot\chi(\varphi_{L'/K}) & = & e\cdot f\chi(\varphi_{L'/K}) = e\cdot\chi(\varphi^f_{L'/K}) \\
& = & e\cdot\chi(\varphi_{N/L|_{L'}}) = e\cdot \operatorname{Inf}\chi(N/L) \\
& = & e\cdot(\operatorname{Res}\circ\operatorname{Inf})\chi(\varphi_{N/L})\,.
\end{array}$$

Hence the right diagram commutes, which proves the lemma.

From Theorem 16.1 we have the equality

$$\operatorname{Br}(K) := H^2(\quad/K) = H^2(T/K) = \bigcup_{L/K} H^2(L/K)\,,$$

where L runs over the unramified extensions of K. Hence from 15.5 we get

Theorem 16.3 The Brauer group of a local $\mathfrak{p}$-adic field K is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$:

$$\operatorname{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$$

Definition 16.4 Let L/K be a normal extension and let L'/K be the unramified extension of the same degree $[L' : K] = [L : K]$, so that $H^2(L/K) = H^2(L'/K)$. Define the invariant map

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

to be the isomorphism with

$$\mathrm{inv}_{L/K}(c) = \mathrm{inv}_{L'/K}(c)$$

for $c \in H^2(L/K) = H^2(L'/K)$.

With the definition of this invariant map we have reached our goal:

Theorem 16.5 Let K be a $\mathfrak{p}$-adic number field, let Ω be its algebraic closure, and let $G_K = G_{\Omega/K}$ be the Galois group of Ω/K. Then the formation $(G_{\Omega/K}, \Omega^\times)$ is a class formation with respect to the invariant map defined in 16.4.

Proof Axiom I is satisfied by Hilbert 90: $H^1(L/K)(= H^1(L^\times/K^\times)) = 1$. The Axiom II is obtained by passing to the unramified extension of the same degree.

Furthermore the Main Theorem of Local Class Field Theory is

Theorem 16.6 Let L'/K be a normal extension. Then the homomorphism

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

is an isomorphism.

For $q = -2$ we get the local reciprocity law:

Theorem 16.7 For every normal extension L/K we have the isomorphism

$$G_{L/K}^{\mathrm{ab}} \cong H^{-2}(G_{L/K}, \mathbb{Z}) \overset{u_{L/K}\cup}{\underset{\sim}{\longrightarrow}} H^0(L/K) = K^\times/N_{L/K}L^\times\,.$$

Moreover, all properties of the abstract class field theory hold.

For $q = 1$ and 2 we get:

Corollary 16.8 $H^3(L/K) = 1$ and $H^4(L/K) = \chi(G_{L/K})$

17 Global class field theory I

In the following we will consider idèles. (Introduced by Chevalley, as so-called "ideal elements").

Definition 17.1 Let K be an algebraic number field. An idèle $\mathfrak{a}$ of K is a family $\mathfrak{a} = (a_\mathfrak{p})_\mathfrak{p}$ of elements $a_\mathfrak{p} \in K_\mathfrak{p}^\times$ where $a_\mathfrak{p}$ is a unit for almost all $\mathfrak{p}$.

We also obtain these idèles as follows

Definition 17.2 Let S be a finite set of primes of K. The group

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

is called the group of S-idèles of K.

The union

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

where S runs over all finite sets of primes, is then the **idèle group** (group of all idèles) of K.

The $a_\mathfrak{p}$ are called the local components of the idèle, and $a_\mathfrak{p}$ is called an **essential component**, if $a_\mathfrak{p}$ is not a unit.

If $x \in K^\times$, then we let (x) be the idèle, whose component is x at all places. Note that x is a unit for almost all $\mathfrak{p}$. In this way, $K^\times$ is embedded canonically into I_K. The idèles from $K^\times$ are called the **principal idèles** of K.

If S is a finite set of primes of K, we denote by

$$K^S = K^\times \cap I_K^S \subseteq I_K^S$$

the group of **S-principal idèles**.

The elements in K^S are also called the **S-units** in K, since they are units for all primes $\mathfrak{p} \notin S$. In particular, if $S = S_\infty$ is the set of infinite primes of K, then K^{S_∞} is the usual unit group $U_K = \mathcal{O}_K^\times$ of K.

Definition 17.3 The factor group

$$C_K = I_K / K^\times$$

is called the idèle class group.

This will be the group of our main interest.

The connection between the idèles and the ideals of K is the following.

Proposition 17.4 Let S_∞ be the set of infinite primes of K, and let $I_K^{S_\infty}$ be the group of idèles which have units as components for all finite primes. Then we have canonical isomorphisms

$$I_K/I_K^{S_\infty} \cong J_K \quad , \quad I_K/I_K^{S_\infty} \cdot K^\times \cong J_K/P_K \, ,$$

where J_K is the group of ideals and P_K is the group of principal ideals.

Exercise!

Unlike the class group $Cl_K = J_K/P_K$, the ideal class group $C_K = I_K/K^\times$ is not finite. However, the finiteness of the ideal class group is reflected in the fact that all idèle classes in C_K can be represented by S-idèles $\mathfrak{a} \in I_K^S$ for a finite set S of primes:

Proposition 17.5 Let S be a sufficiently large set of primes. Then

$$I_K = I_K^S \cdot K^\times, \text{ and therefore } C_K = I_K^S \cdot K^\times/K^\times \, .$$

Proof The ideal class group J_K/P_K is finite. Hence we can choose a finite set of ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ which represent the classes in J_K/P_K. The ideals are further composed from only finitely many prime ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$. Now, if S is any set of primes of $K^\times$ containing the primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_s$ and all the infinite primes, then one has in fact

$$I_K = I_K^S \cdot K^\times \, .$$

For this we consider the isomorphism

$$I_K/I_K^{S_\infty} \cong J_K/P_K$$

(see 17.4). If $\mathfrak{a} \in I_K$, then the corresponding ideal $\mathfrak{a} = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{p}^{v_\mathfrak{p} \mathfrak{a}_\mathfrak{p}}$ lies in a class $\mathfrak{a}_i P_K$, i.e., $\mathfrak{a} = \mathfrak{a}_i \cdot (x)$, where $(x) \in P_K$ denotes the principal ideal given by $x \in K^\times$. The idèle $\mathfrak{a}' = \mathfrak{a} \cdot x^{-1}$ is mapped onto the ideal $\mathfrak{A}' = \prod_{\mathfrak{p} \nmid \infty} \mathfrak{P}^{v_\mathfrak{p} \mathfrak{a}'_\mathfrak{p}} = \mathfrak{A}_i$. Since the prime ideal components of $\mathfrak{A}_i$ lie in the set S, we have $v_\mathfrak{p} \mathfrak{a}'_\mathfrak{p} = 0$ for all $\mathfrak{p} \notin S$; thus $\mathfrak{a}' = \mathfrak{a} \cdot x^{-1} \in I_K^S$, $\mathfrak{a} \in I_K^S \cdot K^\times$.

Now we study the behaviour in extension fields.

Let L/K be a finite extension of number fields. If $\mathfrak{p}$ is a prime of K and $\mathfrak{P}$ is a prime of L lying over $\mathfrak{p}$, we write $\mathfrak{P}/\mathfrak{p}$.

The idèle group I_K of K is embedded into the idèle group I_L of L as follows: An idèle $\mathfrak{a} \in I_K$ with components $\mathfrak{a}_\mathfrak{p}$ is mapped to the idèle $\mathfrak{a}' \in I_L$ with components $\mathfrak{a}_{\mathfrak{P}'} = \mathfrak{a}_\mathfrak{p}$ for $\mathfrak{P}'/\mathfrak{p}$. This gives an injection

$$I_K \hookrightarrow I_L \, ,$$

which we regard as an inclusion.

With this identification, an idèle $\mathfrak{a}$ in I_L is in I_K if and only if its components $a_\mathfrak{P}$ lie in $K_\mathfrak{p}$ (where $\mathfrak{P}/\mathfrak{p}$), and moreover any two primes $\mathfrak{P}$ and $\mathfrak{P}'$ lying over the same $\mathfrak{p}$ of K have equal components $a_\mathfrak{P} = a_{\mathfrak{P}'} \in K_\mathfrak{p}$.

If L/K is normal and $G = G_{L/K}$ is the associated Galois group, I_L is canonically a G-module: An element $\sigma \in G$ defines a canonical isomorphism from $L_{\sigma^{-1}\mathfrak{P}}$ to $L_{\mathfrak{P}}$, which we denote by σ again.

Hence to an idèle $\mathfrak{a} \in I_L$ with components $a_{\mathfrak{P}} \in L_{\mathfrak{P}}^{\times}$ we associate the idèle $\sigma\mathfrak{a} \in I_L$ with components

$$(\sigma\mathfrak{a})_{\mathfrak{P}} = \sigma\mathfrak{a}_{\sigma^{-1}\mathfrak{P}} \in L_{\mathfrak{P}}^{\times}\,.$$

Note that $\mathfrak{a}_{\sigma^{-1}\mathfrak{P}} \in L_{\sigma^{-1}\mathfrak{P}}$ is the $\sigma^{-1}\mathfrak{P}$-component of $\mathfrak{a}$, which is mapped by σ into $L_{\mathfrak{P}}^{\times}$. If we take into account that the $\mathfrak{P}$-component $(\sigma a)_{\mathfrak{P}}$ of $\sigma\mathfrak{a}$ is essential if and only if the $\sigma^{-1}\mathfrak{P}$-component $\mathfrak{a}_{\sigma^{-1}\mathfrak{P}}$ of $\mathfrak{a}$ is essential, we immediately see that, when passing to ideals, the map induced by $\mathfrak{a} \mapsto \sigma\mathfrak{a}$ is just the conjugation map on the ideal group J_L

Proposition 17.6 Let L/K be normal with Galois group $G = G_{L/K}$. Then

$$I_L^G = I_K\,.$$

Proof The inclusion $I_K \subseteq I_L^G$ is easy: If $\sigma \in G$, then the isomorphism

$$L_{\sigma^{-1}\mathfrak{P}} \xrightarrow{\sigma} L_{\mathfrak{P}}$$

is a $K_{\mathfrak{p}}$-isomorphism (for $\mathfrak{P}/\mathfrak{p}$), and if $\mathfrak{a} \in I_K$ is considered as an idèle of I_L, then $(\sigma\mathfrak{a})_{\mathfrak{P}} = \sigma\mathfrak{a}_{\sigma^{-1}\mathfrak{P}} = \sigma\mathfrak{a}_{\mathfrak{P}} = \mathfrak{p}_{\mathfrak{P}}$, i.e., $\sigma\mathfrak{a} = \mathfrak{a}$.

For the inclusion $I_L^G \subseteq I_K$, consider $\mathfrak{a} \in I_L$ with $\sigma\mathfrak{a} = \mathfrak{a}$ for all $\sigma \in G$. Then $(\sigma\mathfrak{a})_{\mathfrak{P}} = \sigma\mathfrak{a}_{\sigma^{-1}\mathfrak{P}} = \mathfrak{a}_{\mathfrak{p}}$ for all primes $\mathfrak{P}$ of L.

By number theory, we can regard the decomposition group $G_{\mathfrak{P}}$ of $\mathfrak{P}$ over K as the Galois group of the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. For every $\sigma \in G_{\mathfrak{P}}$ we have $\sigma^{-1}\mathfrak{P} = \mathfrak{P}$, and since $a_{\mathfrak{P}} = \sigma\mathfrak{a}_{\sigma^{-1}\mathfrak{P}} = \sigma\mathfrak{a}_{\mathfrak{P}}$, we obtain $\mathfrak{a}_{\mathfrak{P}} \in K_{\mathfrak{p}}$ $(\mathfrak{P}/\mathfrak{p})$.

Hence, if σ is an arbitrary element of G, then $(\sigma\mathfrak{a})\mathfrak{P} = \mathfrak{a}_{\mathfrak{P}} = \sigma\mathfrak{a}_{\sigma^{-1}\mathfrak{P}} = \mathfrak{a}_{\sigma^{-1}\mathfrak{P}} \in K_{\mathfrak{p}}$, i.e., two prime ideals $\mathfrak{P}$ and $\sigma^{-1}\mathfrak{P}$ lying above the same prime $\mathfrak{p}$ of K have the same components $\mathfrak{a}_{\mathfrak{P}} = \mathfrak{a}_{\sigma^{-1}\mathfrak{P}} \in K_{\mathfrak{p}}$, so that $\mathfrak{a} \in I_K$.

It is well-known that an ideal of a field K can become a principal ideal in an extension field L without being principal ideal in the base field K. The following proposition shows that the idèles behave differently

Proposition 17.7 If L/K is an arbitrary finite extension, then

$$L^{\times} \cap I_K = K^{\times}\,.$$

In particular, if $\mathfrak{a} \in I_K$ is an idèle of K that becomes a principal idèle in L, i.e., $\mathfrak{a} \in L^{\times}$, then $\mathfrak{a}$ is already principal in K.

Proof The inclusion $K^\times \subseteq L^\times \cap I_K$ is trivial. Now let $\tilde{L}$ be a finite normal extension of K containing L, and let $\tilde{G} = G_{\tilde{L}/K}$ be its Galois group. Then I_K and I_L are subgroups of $I_{\tilde{L}}$. If $\mathfrak{a} \in \tilde{L}^\times \cap I_K$, then Proposition 17.7 shows that $\mathfrak{a} \in I_{\tilde{L}}^{\tilde{G}} = K^\times$. Therefore $\tilde{L}^\times \cap I_K = K^\times$, which implies $L^\times \cap I_K \subseteq \tilde{L}^\times \cap I_K = K^\times$.

By 17.7 we can embed the idèle class group C_K of a field K into the idèle class group C_L of a finite extension L, using the canonical homomorphism

$$\iota : C_K \to C_L \quad , \quad \mathfrak{a} \cdot K^\times \mapsto \mathfrak{a} \cdot L^\times$$

($\mathfrak{a} \in I_K \subseteq I_L$). To see that ι is injective, note that, if the class $\mathfrak{a} \cdot K^\times \in C_K$ is mapped to the unit class $L^\times \in C_L$, so that $\mathfrak{a} \cdot L^\times = L^\times$, $\mathfrak{a} \in L^\times$, then we know by 17.7 that $\mathfrak{a} \in L^\times \cap I_K = K^\times$, i.e., $\mathfrak{a} \cdot K^\times = K^\times$ is the unit class of C_K.

In the following we view C_K as embedded in C_L via this canonical map, hence as a subgroup of C_L. An element $\mathfrak{a} \cdot L^\times \in C_L$ (with $\mathfrak{a} \in I_L$) lies in C_K if and only if the class $\mathfrak{a} \cdot L^\times$ contains a representative $\mathfrak{a}'$ from I_K ($\subseteq I_L$) such that $\mathfrak{a}' \cdot L^\times = \mathfrak{a} \cdot L^\times$.

Theorem 17.8 Let L/K be Galois extension with Galois group $G = G_{L/K}$. Then C_L is canonically a G-module, and

$$C_L^G = C_K \,.$$

Proof If $\mathfrak{a} \cdot L^\times \in C_L$ ($\mathfrak{a} \in I_L$), we set $\sigma(\mathfrak{a} \cdot L^\times) = \sigma\mathfrak{a} \cdot L^\times$. This definition is independent of the choice of $\mathfrak{a} \in I_L$, and makes C_L a G-module.

From the exact sequence of G-modules

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

we obtain the exact cohomology sequence

$$1 \to (L^\times)^G \to I_L^G \to C_L^G \to H^1(G, L^\times)\,,$$

where $(L^\times)^G = K^\times$, $I_L^G = I_K$, and $H^1(G, L^\times) = 1$, so that $C_L^G = C_K$.

18 Global class field theory II

We will now study the cohomology of the idèle groups.

Let L/K be a finite normal extension of number fields with Galois group $G = G_{L/K}$. We consider the cohomology groups $H^q(G, I_L)$ of the G-module I_L, and we will show that these groups can be decomposed into a direct product of cohomology groups of the local fields $K_\mathfrak{p}$.

Let S be a finite set of primes of K, and let $\tilde{S}$ be the finite set of primes in L above the primes in S. For simplicity, we denote the group of $\tilde{S}$-idèles $I_L^{\tilde{S}}$ also by I_L^S, and call them the S-idèles of the field L; we will use the same convention in later sections as well.

Thus we have

$$I_L^S = \prod_{\mathfrak{P}|\mathfrak{p}\in S} L_\mathfrak{P}^\times \times \prod_{\mathfrak{P}|\mathfrak{p}\notin S} U_\mathfrak{P} = \prod_{\mathfrak{p}\in S}\prod_{\mathfrak{P}/\mathfrak{p}} L_\mathfrak{P}^\times \times \prod_{\mathfrak{p}\notin S}\prod_{\mathfrak{P}|\mathfrak{p}} U_\mathfrak{P}\,.$$

We consider the products $I_L^\mathfrak{p} = \prod_{\mathfrak{P}/\mathfrak{p}} L_\mathfrak{P}^\times$ and $U_L^\mathfrak{p} = \prod_{\mathfrak{P}/\mathfrak{p}} U_\mathfrak{P}$ as subgroups of I_L^S, where we think of the elements in $I_L^\mathfrak{p}$ (resp. in $U_L^\mathfrak{p}$) as those idèles which have the component 1 at all the primes of L not lying over $\mathfrak{p}$ (resp. in addition have only units as components at the primes of L lying above $\mathfrak{p}$).

Since the automorphisms $\sigma \in G$ only permute the primes $\mathfrak{P}$ above $\mathfrak{p}$, the groups $I_L^\mathfrak{p}$ and $U_L^\mathfrak{p}$ are G-modules.

Thus we have decomposed I_L^S into a direct product of G-modules

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

For the G-modules $I_L^\mathfrak{p}$ and $I_L^\mathfrak{p}$ we have:

Proposition 18.1 Let $\mathfrak{P}$ be a prime of L lying over $\mathfrak{p}$. Then

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

where $G_\mathfrak{P}$ is the decomposition group of $\mathfrak{P}$ over K, considered also as the Galois group of $L_\mathfrak{P}/K_\mathfrak{p}$. If $\mathfrak{p}$ is a finite prime unramified in L, then

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

for all q.

Addendum: The first isomorphism is given by the composition

$$H^q(G, I_L^\mathfrak{p}) \xrightarrow{\text{res}} H^q(G_\mathfrak{P}, I_L^\mathfrak{p}) \xrightarrow{\overline{\pi}_\mathfrak{P}} H^q(G_\mathfrak{P}, L_\mathfrak{P}^\times)\,,$$

where $\overline{\pi}_\mathfrak{P}$ is induced by the canonical projection $I_L^\mathfrak{p} \to L_\mathfrak{P}^\times$ which takes each idèle in $I_L\mathfrak{p}$ to its $\mathfrak{P}$- component.

Proof If $\sigma \in G$ runs through a system of representations of the cosets $G/G_{\mathfrak{P}}$, for simplicity we write $\sigma \in G/G_{\mathfrak{P}}$, then $\sigma\mathfrak{P}$ runs through all distinct primes of L above $\mathfrak{p}$. Hence

$$I_L^{\mathfrak{p}} = \prod_{\sigma \in G/G_{\mathfrak{P}}} L_{\sigma\mathfrak{P}}^{\times} = \prod_{\sigma \in G/G_{\mathfrak{P}}} \sigma L_{\mathfrak{P}}^{\times}, \text{ and}$$

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

which shows that $I_L^{\mathfrak{p}}$ and $U_L^{\mathfrak{p}}$ are $G/G_{\mathfrak{P}}$-induced modules.

Applying Shapiro's Lemma (Lemma 11.8), we get

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

and

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

where the first isomorphism is the one given in the addendum.

If $\mathfrak{p}$ is unramified in L, then the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is unramified, and by Theorem 12.4 we get $H^q(G, U_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{P}}, U_{\mathfrak{P}}) = 1$.

By Proposition 18.1 and the decomposition

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

the cohomology groups of the idèle groups I_L^S and I_L are easy to compute. By the compatibility of cohomology groups with products (see exercise sheet 5) we get

$$H^q(G, I_L^S) = \prod_{\mathfrak{p} \in S} H^q(G, I_L^{\mathfrak{p}}) \times \prod_{\mathfrak{p} \notin S} H^q(G, U_L^{\mathfrak{p}})$$

If the finite set S contains all (finite) primes of K which are ramified in L, then by Proposition 18.1 we have $H^q(G, I_L^{\mathfrak{p}}) \cong H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^{\times})$ ($\mathfrak{P}$ any primes above $\mathfrak{p}$), and $H^q(G, U_L^{\mathfrak{p}}) = 1$ for each $\mathfrak{p} \notin S$. Therefore

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

($\mathfrak{P}$ any primes above $\mathfrak{p}$).

Since $I_L = \bigcup_S I_L^S$, we also have

$$\begin{aligned} H^q(G, I_L) &= \varinjlim_S H^q(G, I_L^S) \\ &= \varinjlim_S \prod_{\mathfrak{p} \in S} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^{\times}) \\ &\cong \bigoplus_{\mathfrak{p}} H^q(G_{\mathfrak{P}}, L_{\mathfrak{p}}^{\times}) \end{aligned}$$

(where $\oplus$ denotes the direct sums of the groups in question, so that almost all components are zero). So we get

Theorem 18.2 Let S be a finite set of primes of K which contains all primes ramified in L. Then

$$\text{(a)} \quad H^q(G, I_L^S) = \prod_{\mathfrak{p}\in S} H^q(G_\mathfrak{P}, L_\mathfrak{P}^\times)$$

$$\text{(b)} \quad H^q(G, I_L) \cong \bigoplus_{\mathfrak{p}} H^q(G_\mathfrak{P}, L_\mathfrak{P}^\times) \ .$$

From the proof and the addendum in 18.1 we further get:

Addendum: The isomorphism (b) is given by the projections $H^q(G, I_L) \xrightarrow{\text{res}} H^q(G_\mathfrak{P}, L_\mathfrak{P}^\times)$, i.e., the composition

$$H^q(G, I_L) \xrightarrow{\text{res}} H^q(G_\mathfrak{P}, I_L) \xrightarrow{\overline{\pi}} H^q(G_\mathfrak{P}, L_\mathfrak{P}^\times)$$

where $\overline{\pi}$ is induced by the canonical projection $I_L \xrightarrow{\pi} L_\mathfrak{P}^\times$ which takes each idèle to its $\mathfrak{P}$-component $a_\mathfrak{P}$.

The following proposition shows how changing the fields affects local components.

Proposition 18.3 Let $N \supseteq L \supseteq K$ be normal extensions of K, and let $\mathfrak{P}'/\mathfrak{P}/\mathfrak{p}$ be primes of N, L, and K, respectively. Then

$$\begin{array}{lcll} (\inf_N c)_\mathfrak{p} & = & \inf_{N_\mathfrak{P}}(c_\mathfrak{p}), & c \in H^q(G_{L/K}, I_L), q \geq 1 \, . \\ (\text{res}_L\, c)_\mathfrak{P} & = & \text{res}_{L_\mathfrak{P}}(c_\mathfrak{p}), & c \in H^q(G_{N/K}, I_N) \, , \\ (\text{cor}_K\, c)_\mathfrak{p} & = & \sum_{\mathfrak{P}/\mathfrak{p}} \text{cor}_{K_\mathfrak{p}}(c_\mathfrak{P}), & c \in H^q(G_{N/L}, I_N) \, . \end{array}$$

For the last two formulas it suffices to assume that only N/K is normal.

For the third formula note that for each prime $\mathfrak{P}/\mathfrak{p}$ we choose a prime $\mathfrak{P}'$ of N above $\mathfrak{P}$; thus the corestrictions $\text{cor}_{K_\mathfrak{p}}(c_\mathfrak{P})$ a priori lie in distinct cohomology groups $H^q(G_{N_{\mathfrak{P}'}/K\mathfrak{p}}, N_{\mathfrak{P}'}^\times)$. But we can identify these as follows: Given two primes $\mathfrak{P}'$ and $\mathfrak{P}''$ of N lying over $\mathfrak{p}$, there is a canonical automorphism $\sigma \in G_{N/K}$ interchanging these primes; given this, the isomorphism $N_{\mathfrak{P}'}^\times \xrightarrow{\sigma} N_{\sigma\mathfrak{P}'}^\times$ induces a canonical isomorphism

$$H^q(G_{N_{\mathfrak{P}'}/K_\mathfrak{p}}, N_{\mathfrak{P}'}^\times) \cong H^q(G_{N_{\sigma\mathfrak{P}'}/K'_\mathfrak{p}} N_{\sigma\mathfrak{P}'}^\times) \, .$$

Hence we may regard $\text{cor}_{K_\mathfrak{p}}(c_\mathfrak{P})$ for each $\mathfrak{P}/\mathfrak{p}$ as an element of the group $H^q(G_{N_{\mathfrak{P}'}/K_\mathfrak{p}}, N_\mathfrak{P}^\times)$ for a fixed choice of $\mathfrak{P}'/\mathfrak{p}$, and form the sum in the corestriction in this group.

The proof of Proposition 18.3 uses the general and purely cohomological fact that the restriction map which occurs when passing to the local components, commutes with the maps Inf, Res, and Cor.

This is easy to see at the cocycle level for inf and res for $q \geq 1$, and for cor if $q = -1, 0$. The general case follows by dimension shifting.

Theorem 18.2 gives the following result, which is also called the Norm Theorem for idèles.

Corollary 18.4 An idèle $\mathfrak{a} \in I_K$ is the norm of an idèle b of I_L if and only if each component $a_\mathfrak{p} \in K_\mathfrak{p}^\times$ is the norm of an element $b_\mathfrak{P} \in L_\mathfrak{P}^\times$ $(\mathfrak{P}/\mathfrak{p})$, i.e., if and only if it is a local norm everywhere.

Corollary 18.5 $H^1(G, I_L) = H^3(G, I_L) = 1$.

This follows from Corollary 16.8.

The fact that $H^1(G, I_L) = 1$ implies that, with respect to the idèle groups, the extensions L/K form a field formation.

This allows us to regard the cohomology groups $H^2(G_{L/K}, I_L)$ as the elements of the inductive limit of all these groups, via the inflations, regarded as inclusions:

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

where Ω is the field of all algebraic numbers (the algebraic closure of $\mathbb{Q}$).

In local class field theory we have seen that the Brauer group is generated by all unramified extensions.

In the global case we have:

Theorem 18.6 Let K be a number field of finite degree over $\mathbb{Q}$. Then we have

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

and

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

where L/K ranges over all cyclic cyclotomic extensions.

We only prove this for I_L; the case of the Brauer group is similar.

For the proof we use the following:

Lemma 18.7 Let K be a finite extension of $\mathbb{Q}$, let S be a finite set of primes of K, and let m be a natural number. Then there exists a cyclic cyclotomic field L/K with the property that

a) $m \mid [L_\mathfrak{P} : K_\mathfrak{p}]$ for all finite $\mathfrak{p} \in S$,

b) $[L_\mathfrak{P} : K_\mathfrak{p}] = 2$ for all real infinite $\mathfrak{p} \in S$.

Proof It suffices to prove the lemma for $K = \mathbb{Q}$; the general case follows by taking composita. More precisely, if $N/\mathbb{Q}$ is a totally imaginary cyclic cyclotomic field, such that for every prime number p above which there is a prime of K in S the degree $[N_{\mathfrak{P}} : \mathbb{Q}_p]$ is divisible by $m \cdot [K : \mathbb{Q}]$, then $L \cdot N$ has the desired property.

Let ℓ^n be a prime power, and let ζ be a primitive ℓ^n-th root of unity. If $\ell \neq 2$, then the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is cyclic of degree $\ell^{n-1} \cdot (\ell - 1)$, and we denote the cyclic subfield of degree ℓ^{n-1} by $L(\ell^n)$.

If $\ell = 2$, then the Galois group of $\mathbb{Q}(\zeta)/\mathbb{Q}$ is the direct product of a cyclic group of order 2 and a cyclic group of order 2^{n-2}. In this case we consider the field $L(2^n) = \mathbb{Q}(\xi)$ with $\xi = \zeta - \zeta^{-1}$. The automorphisms of $\mathbb{Q}(\zeta)$ are defined by σ_ν with $\sigma_\nu(\zeta) = \zeta^\nu$ with ν odd, and we have $\sigma_\nu(\xi) = \zeta^\nu - \zeta^{-\nu}$.

Since $\zeta^{2^{n-1}} = -1$, we have $\sigma_\nu(\xi) = \sigma_{\nu+2}^{n+1}(\xi)$ and since either ν or $-\nu + 2^{n-1} \equiv 1 \bmod 4$, the automorphisms of $L(2^n) = \mathbb{Q}(\xi)$ are induced by those with $\nu \equiv 1 \bmod 4$.

Now an elementary calculation shows that the Galois group of $L(2^n)/\mathbb{Q}$ is cyclic of order 2^{n-2}. Moreover, because $\sigma_{-1}\xi = -\xi$, the field $L(\ell^n)$ is totally imaginary for large n.

If p is a prime number, then the local degree $[L(\ell^n)_{\mathfrak{P}} : \mathbb{Q}_p]$ becomes an arbitrarily high ℓ-power, because in any case $[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p]$ becomes arbitrarily big, and we have $[\mathbb{Q}_p(\zeta) : L(\ell^n)_{\mathfrak{P}}] \leq \ell - 1$ for odd ℓ and ≤ 2 for $\ell = 2$.

If we now consider $m = \ell_1^{r_1} \dots \ell_s^{r_s}$, then the field

$$L = L(\ell_1^{n_1}) \cdot L(\ell_2^{n_2}) \cdot \ldots \cdot (L(\ell_s^{n_s}) L(2^t))$$

gives the wished property, if the n_i and t are sufficiently big.

In fact, then for the finitely many primes $p \in S$ the local degrees $[L_{\mathfrak{P}} : \mathbb{Q}_p]$ are divisible by each power $\ell_i^{r_i}$, hence divisible by m; L is totally imaginary by the factor $L(2^t)$, and cyclic over $\mathbb{Q}$, since the $L(\ell^n)$ are cyclic with pairwise coprime degrees.

Now we prove Theorem 18.6. We only give the proof for the group $H^2(G_{\Omega/K}, I_\Omega)$, since the case $\mathrm{Br}(K)$ is verbatim the same, if one replaces the idèle groups I_L by the multiplicative groups $L^\times$.

Hence let $c \in H^2(G_{\Omega/K}, I_\Omega)$, e.g., $c \in H^2(G_{L'/K}, I_{L'})$, let m be the order of c, and S the (finite) set of primes $\mathfrak{p}$ of K, for which the local components $c_{\mathfrak{p}}$ of c are different from 1.

By the above Lemma we find a cyclic cyclotomic L/K with $m \mid [L_{\mathfrak{p}} : K_{\mathfrak{p}}]$ for the finite $\mathfrak{p} \in S$ and $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = 2$ for real infinite $\mathfrak{p} \in S$.

If we form the compositum $N = L \cdot L'$, then

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

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

By the exactness of the sequence

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

it suffices to show that $\operatorname{res}_L c = 1$.

But by local class field theory and by 18.2 and 18.3 we have

$\operatorname{res}_L c = 1$

$\Leftrightarrow (\operatorname{res}_L c)_{\mathfrak{P}} = \operatorname{res}_{L_{\mathfrak{P}}} c_{\mathfrak{p}} = 1$ for all primes $\mathfrak{P}$ of L

$\Leftrightarrow \operatorname{inv}_{N_{\mathfrak{P}'}/L_{\mathfrak{p}}}(\operatorname{Res}_{L_{\mathfrak{P}}} c_{\mathfrak{p}}) = [L_{\mathfrak{P}} : K_{\mathfrak{p}}] \cdot \operatorname{inv}_{N_{\mathfrak{P}'}/K_{\mathfrak{p}}} = \operatorname{inv}_{N_{\mathfrak{P}'}/K_{\mathfrak{p}}} c_{\mathfrak{p}} = \operatorname{inv}_{N_{\mathfrak{P}'}/K_{\mathfrak{p}}} c_{\mathfrak{p}}^{[L_{\mathfrak{P}}:K_{\mathfrak{p}}]} = 0$ for all primes $\mathfrak{p}$ of K

$\Leftrightarrow c_{\mathfrak{p}}^{[L_{\mathfrak{P}}:K_{\mathfrak{p}}]} = 1$ for all $\mathfrak{p} \in S$.

But the last property holds, since $c_{\mathfrak{p}}^m = 1$ and $m \mid [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$ for the finite places and $[L_{\mathfrak{P}} : K_{\mathfrak{p}}] = 2$ for the real infinite $\mathfrak{p} \in S$.

19 Global class field theory III

We will now consider the cohomology of the idèle class groups. In particular, for showing that we get the class field theory axioms, we have to show that, for a Galois extension L/K of number fields with Galois group $G = G_{L/K}$, that $H^1(G, C_L) = 1$ and that $H^2(G, C_L)$ is cyclic of order $[L : K]$.

Consider a normal extension L/K with cyclic Galois group $G = G_{L/K}$ of prime order p.

Theorem 19.1 The idèle class group C_L is a Herbrand module with Herbrand quotient

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

Corollary 19.2 (First fundamental inequality)

$$|H^0(G, C_L)| = (C_K : N_{L/K} C_L) = p \cdot |H^1(G, C_L)| \geq p\,.$$

Proof of Theorem 19.1 Let S be a finite set of primes of K such that

1. S contains all infinite primes and all primes ramified in L/K.
2. $I_L = I_L^S \cdot L^\times$.
3. $I_K = I_K^S \cdot K^\times$.

Note that, by Proposition 17.5, such a set S certainly exists.

Then we have

$$C_L = I_L^S \cdot L^\times / L^\times \cong I_L^S / L^S\,,$$

where $L^S = L^\times \cap I_L^S$ is the group of S-units, i.e., the groups of all those elements of $L^\times$ which are units for all primes $\mathfrak{P}$ of L which do **not** lie above the primes in S.

From Theorem 9.4 we get

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

in the sense that when two of these Herbrand quotients are defined, then the third Herbrand quotient is defined as well, and we get the above equality.

By Theorem 18.2, the computation of $h(I_L^S)$ is a local question. Let

n be the number of primes in S

N be the number of primes of L which lie over S.

n_1 the number of primes in S which are inert.

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

To compute the quotient

$$h(I_L^S) = |H^0(G, I_L^S)|/|H^1(G, I_L^S)|\,,$$

we have to determine $|H^0(G, I_L^S)|$ and $|H^1(G, I_L^S)|$.

We do this by making use of the isomorphism $H^qG, I_L^S) \cong \prod_{\mathfrak{p}\in S} H^q(G_{\mathfrak{P}}, L_{\mathfrak{P}}^\times)$ from Theorem 18.2.

If $q = 1$, the above isomorphism gives $H^1(G, I_L^S) = 1$, since $H^1(G_{\mathfrak{P}}, L_{\mathfrak{P}}^\times) = 1$. If $q = 0$, then $H^0(G, I_L^S) = \prod\limits_{\mathfrak{p}\in S} H^0(G_{\mathfrak{P}}, L_{\mathfrak{P}}^\times)$, and it remains to determine the order of $H^0(G_{\mathfrak{P}}, L_{\mathfrak{P}}^\times)$, which is done using local class field theory. In fact, we have $H^0(G_{\mathfrak{P}}, L_{\mathfrak{P}}^\times) \cong G_{\mathfrak{P}}$ by local class field theory.

Hence we have

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

With this we get $|H^0(G, I_L^S)| = p^{n_1}$, and since $H^1(G, I_L^S) = 1$, we have $h(I_L^S) = p^{n_1}$.

For the computation of $h(L^S)$ we use the formula for the Herbrand quotient from Theorem 9.10: By Number Theory, the group L^S of S-units in L is a finitely generated group, and its rank is equal to $|S| - 1$, where $|S|$ denotes the number of primes in S, and the group $L^S)^G = K^S = K^\times \cap L^S$ is the group of S-units of K and finitely generated of rank $n - 1$.

Hence Theorem 9.10 gives

$$\begin{aligned} h(L^S) &= p^{(p(n-1)-N+1)/(p-1)} \\ &= p^{(p(n-1)-n_1-p(n-n_1)+1)/(p-1)} \\ &= p^{(n_1-1)}\,. \end{aligned}$$

Since both Herbrand quotients $h(I_L^S)$ and $h(L^S)$ are defined, $h(C_L)$ is defined as well, and the above formulas imply

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

This implies 19.1 and 19.2.

We now show the second fundamental inequality

$$(C_K : N_G C_L) \leq p$$

for cyclic extensions of prime degree, under the additional assumption that K contains the p-th roots of unity. In this case L is a Kummer extension: $L = K(\sqrt[p]{x_0})$ for some $x_0 \in K^\times$. We start with the following lemma:

Lemma 19.3 Let $N = K(\sqrt[p]{x}), x \in K^\times$ be any Kummer extension over K, and let $\mathfrak{p}$ be a finite prime of K not lying over the prime number p. Then $\mathfrak{p}$ is unramified in N if and only if $x \in U_\mathfrak{p} \cdot (K_\mathfrak{p}^\times)^p$, and $\mathfrak{p}$ splits completely in N if and only if $x \in (K_\mathfrak{p}^\times)^p$.

Proof Let $\mathfrak{P}$ be a prime of N over $\mathfrak{p}$. Then $N_\mathfrak{P} = K_\mathfrak{p}(\sqrt[p]{x})$. If $x = u \cdot y^p, u \in U_\mathfrak{p}$ and $y \in K_\mathfrak{p}^\times$, then $N_\mathfrak{P} = K_\mathfrak{p}(\sqrt[p]{x}) = K_\mathfrak{p}(\sqrt[p]{x})$. If the equation $X^p - u = 0$ is irreducible over the residue field of $K_\mathfrak{p}$, then it is also irreducible over $K_\mathfrak{p}$, and $N_\mathfrak{P}/K_\mathfrak{p}$ is an unramified extension of degree p. If $X^p - u = 0$ is reducible over the residue field of $K_\mathfrak{p}$, then it splits into p distinct linear factors there, since p is distinct from the characteristic of the residue field, and by Hensel's Lemma, $X^p - u = 0$ also splits into linear factors over $K_\mathfrak{p}$, so that $N_\mathfrak{P} = K_\mathfrak{p}$.

In both cases $N_\mathfrak{P}/\mathfrak{p}$ is unramified, i.e., $\mathfrak{p}$ is unramified in N.

Conversely, if $\mathfrak{p}$ is unramified in N, then $N_\mathfrak{P} = K(\sqrt[p]{x})$ is unramified over $K_\mathfrak{p}$, and we have $\sqrt[p]{x} = u \cdot \pi^k$, where $u \in U_\mathfrak{P}$ and $\pi \in K_\mathfrak{p}$ is a prime element (of smallest value 1). Thus we have $x = u^p \cdot x^{k \cdot p}$, and therefore $u^p \in U_\mathfrak{p}$, $x^{k \cdot p} \in (K_\mathfrak{p}^\times)^p$, i.e., $u \in U_\mathfrak{p} \cdot (K_\mathfrak{p}^\times)^p$.

The prime $\mathfrak{p}$ decomposes in N if and only if $N_\mathfrak{P} = K_\mathfrak{p}(\sqrt[p]{x}) = K_\mathfrak{p}$, hence if and only if $x \in (K_\mathfrak{p}^\times)^p$.

Theorem 19.4 (Second fundamental equality) Let L/K be a cyclic extension of prime degree p. Assume the field K contains the p-th roots of unity, then

$$|H^0(G, C_L)| = (C_K : N_G C_L) \leq p\,.$$

The difficulty here is that we cannot a priori decide which idèle classes in C_K lie in $N_G C_L$. This is completely different from the case of I_K, which by the Norm-Theorem for idèle groups we want to construct $\overline{F} \subseteq N_G C_L$ such that

$$(C_K : N_G C_L) \leq (C_K : \overline{F}) = p\,.$$

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

1) S contains all the primes above p and S_∞.

2) $I_K = I_K^S K^\times$

3) $x_0 \in K^S = I_K^S \cap K^\times$ (i.e. x_0 is an S-unit).

Here, 2) can be satisfied by Proposition 17.5, and 3) because x_0 is a unit for almost all primes.

Together with S we choose m additional primes $\mathfrak{a}_1 \ldots \mathfrak{a}_m \notin S$ that splits completely in L; set $S^* = S \cup \{\mathfrak{a}_1, \ldots, \mathfrak{a}_m\}$. To construct $\overline{F}$, we have to specify an idèle group $F \subseteq I_K$ whose elements represent the idèle classes of $\overline{F}$, it must be sufficiently large to ensure

that the index $(C_K : \overline{F})$ is finite and it must be simple enough so that it is possible to compute the index. These properties are satisfied by the idèle group

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

To see that $F \subseteq N_G I_L$, it suffices by Norm Theorem for idèles to convince ourselves that the components $\mathfrak{a}_p$ of each idèle $\mathfrak{a} \in F$ are norms from the extension $L_\mathfrak{P}/K_\mathfrak{p}(\mathfrak{P}/\mathfrak{p})$. This is true for $\mathfrak{p} \in S$, because $\mathfrak{a}_\mathfrak{p} \in (K_\mathfrak{p}^\times)^p \subseteq N_{L_\mathfrak{P}/K_\mathfrak{p}} L_\mathfrak{P}^\times$; this is trivially true for $\mathfrak{p} = \mathfrak{a}_i$, because $\mathfrak{a}_i$ splits completely so that $L_\mathfrak{P} = K_\mathfrak{p}$, and it is true for $\mathfrak{p} \notin S^*$, because $x_0 \in U_\mathfrak{p}$ by 3) and therefore by Lemma 19.3 each $\mathfrak{p} \notin S^*$ is unramified in $L = K(\sqrt[p]{x_0})$, so that $\mathfrak{a}_\mathfrak{p} \in U_\mathfrak{p} \subseteq N_{L_\mathfrak{p}/K_\mathfrak{p}} L_\mathfrak{P}^\times$ by local class field theory. If we now set $\overline{F} = F \cdot K^\times/K^\times$, then $\overline{F} \subseteq N_G C_L$, since each idèle class $\overline{\mathfrak{a}}$ is represented by a norm idèle $\mathfrak{a} \in F$.

To compute the index $(C_F : \overline{F})$, we consider the following decomposition:

$$(C_K : \overline{F}) = (I_K^{S^*} \cdot K^*/K^\times : F \cdot K^\times/K^\times) = (I_K^{S^*} \cdot K^\times : F \cdot K^\times) = (I_K^{S^*}) : F/((I_K^{S^*} \cap K^\times) : (F \cap K^\times))$$

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

(I) Claim: $(I_K^{S^*} : F) = \prod_{\mathfrak{p}\in S}(K_\mathfrak{p}^\times : (K_\mathfrak{p}^\times)^p = p^{2n}$, where $n = \sharp S$.

Since $S \subset S^*$, the map

$$\begin{array}{rccc} \varphi: & I_K^{S^*} & \to & \prod_{\mathfrak{p}\in S} K_\mathfrak{p}^\times/(K_\mathfrak{p}^\times)^p \\ & \mathfrak{a} & \mapsto & (\mathfrak{a}_\mathfrak{p} \cdot (K_\mathfrak{p}^\times)^p)_\mathfrak{p} \end{array}$$

is surjective, and $\ker(\ell) = \{\mathfrak{a} \in I_K^{S^*} \mid \mathfrak{a}_\mathfrak{p} \in (K_\mathfrak{p}^\times)p \text{ for all } \mathfrak{p} \in S\} = F$.

By the local structure of $K_\mathfrak{p}^\times$, we have

$$(K_\mathfrak{p}^\times : (K_\mathfrak{p}^\times)^p) = p^2 |p|_\mathfrak{p}^{-1}$$

(Here we use $\sum_p \in K$), so that $(I_K^{S^*}) : F) = p^{2n} \prod_{\mathfrak{p}\in S} |p|_\mathfrak{p}^{-1}$, where $n = \sharp S$.

Since the primes $\mathfrak{p} \notin S$ do not lie above the prime number p, $|p|_\mathfrak{p}\mathfrak{p} = 1$ for $\mathfrak{p} \notin S$, and by the product formula

$$\prod_{\mathfrak{p}\in S} |p|_\mathfrak{p} = \prod_\mathfrak{p} |p|_\mathfrak{p} = 1\,.$$

Hence $(I_K^{S^*} : F) = p^{2n}$

Calculation of $((I_K^{S^*} \cap K^\times) : (F \cap K^\times))$

We have

$$((I_K^{S^*} \cap K^\times) : (F \cap K^\times)) = (K^{S^*} : (F \cap K^\times)) = \frac{(K^{S^*} : (K^{S^*})^p)}{(F \cap K^\times : (K^{S^*})^p)}$$

where K^{S^*} is the group of S^*-units, it is finitely generated of rank $\sharp S^* - 1 = n + m - 1$. Moreover K^{S^*} contains the p-th roots of unity. Hence $(K^{S^*} : (K^{S^*})^p) = p^{n+m}$ on the other hand,

$$\begin{aligned} K^\times \cap F &= K^\times \cap (\prod_{\mathfrak{p}\in S})^p (K_\mathfrak{p}^\times)^p \times \prod_{i=1}^{m} K_{\mathfrak{a}_i}^\times \times \prod_{\mathfrak{p}\notin S^*} U_\mathfrak{p}) \\ &= K^\times \cap \bigcap_{\mathfrak{p}\in S} (K_\mathfrak{p}^\times)^p \cap \bigcap_{i=1}^{m} K_{\mathfrak{a}_i}^\times \cap \bigcap_{\mathfrak{p}\notin S^*} U_\mathfrak{p} \\ &= K^\times \cap \bigcap_{\mathfrak{p}\in S} (K_\mathfrak{p}^\times)^p \cap \bigcap_{\mathfrak{p}\notin S^*} U_\mathfrak{p} \end{aligned}$$

If we choose the primes $\mathfrak{a}_1, \ldots, \mathfrak{a}_m$ splitting in L such that

(i) $m = n - 1$

(ii) $(K^\times \cdot \cap F : (K^{S^*})^p) = 1$

Then we are done.

Lemma 19.5 There exist $n-1$ primes of K, $\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1} \notin S$ that splits completely in L and satisfies the following condition: (If $N = K(\sqrt[p]{x})$ is a Kummer extension over K in which all $\mathfrak{p} \in S$ split completely and all $\mathfrak{p} \neq \mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}$ are unramified, then $N = K(\sqrt[p]{x}) = K$.

Using this subscheme, we finish our proof of second fundamental inequality:

Claim

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

for $S^* = S \cup \{\mathfrak{a}_1, \ldots \mathfrak{a}_{n-1}\}$.

"$\supseteq$" it is trivial

"$\subseteq$" let $x \in K^\times \cap \bigcap_{\mathfrak{p}\in S} (K_\mathfrak{p}^\times)^p \cap \bigcap_{\mathfrak{p}\notin S^*} U_\mathfrak{p}$, and $N = K(\sqrt[p]{x})$.

By Lemma 18.3, every $\mathfrak{p} \in S$ splits completely in N, since $x \in (K_\mathfrak{p}^\times)^p$. For $\mathfrak{p} \notin S^*$ we have $x \in U_\mathfrak{p} \subseteq U_\mathfrak{p} \cdot (K_\mathfrak{p}^\times)^p$, so every $\mathfrak{p} \notin S^*$ is ramified in N. Hence by the above sublemma 19.5 yields $= K(\sqrt[p]{x}) = K$, i.e., $x \in (K^\times)^\mathfrak{p}$ and since $x \in U_\mathfrak{p}$ for $\mathfrak{p} \notin S^*$, $x \in (K^\times)^p \cap K^{S^*} = (K^{S^*})^p$.

We omit the proof of Lemma 19.5.

By technical abstract nonsense we can show

Theorem 19.6 If L/K is a normal extension with Galois group $G = G_{L/K}$, then

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

(ii) $|H^2(G, C_L)|$ divides $[L : K]$.

20 Global class field theory IV

In order to prove that $H^2(G, C_L) \cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, we need to study idèle invariants. Let L/K be a normal extension with Galois group $G = G_{L/K}$. The exact sequence $1 \to L^\times \to I_L \to C_L \to 1$ induces $0 \to H^2(G_{L/K}, L^\times) \to H^2(G_{L/K}, I_L)$, since $H^1(G_{L/K}, L^\times) = 1$. But we know

$$H^2(G_{L/K}, I_L) = \bigoplus_{\mathfrak{p}} H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^\times) \xrightarrow[L\subset FT]{\sim} \bigoplus_{\mathfrak{p}} \frac{1}{[L_{\mathfrak{P}}:K\mathfrak{p}]}\mathbb{Z}/\mathbb{Z}$$

$$\bigoplus_{\mathfrak{p}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

$$\text{inv}_{L/K} \qquad \Big\downarrow \sum$$

$$\frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

i.e., $\text{inv}_{L/K}\, c = \sum\limits_{\mathfrak{p}} \text{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}\, c_{\mathfrak{p}}$ for $c \in H^2(G_{L/K}, I_L)$.

Theorem 20.1 $H^2(G_{L/K}, L^\times) \subset \ker(\text{inv}_{L/K})$.

Proof One can reduce to the case $K = \mathbb{Q}$, $L/\mathbb{Q}$ cyclic cyclotomic extension. Then in this case this inclusion can be checked explicitly.

Theorem 20.2 (Hasse principle of a number field) For every number field K, we have a canonical exact sequence

$$1 \to \text{Br}(K) \to \bigoplus_{\mathfrak{p}} \text{Br}(K_{\mathfrak{p}}) \xrightarrow{\text{inv}_K} \mathbb{Q}/\mathbb{Z} \to 0$$

Proof It's enough to prove that

$$(*) \qquad 1 \to H^2(G_{L/K}, L^\times) \to H^2(G_{L/K}, I_L) \xrightarrow{\text{inv}_{L/K}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \to 0$$

is exact, for L/K cyclic.

By Theorem 20.1, it is a complex. Since $H^1(G_{L/K}, C_L) = 1$, the exactness on the left is clear.

For the surjectivity of $\text{inv}_{L/K}$, we use the surjectivity of local invariant maps, and this can be checked explicitly.

It is enough to show

$$\left|\frac{H^2(G_{L/K} I_L)}{H^2(G_{L/K}, L^\times)}\right| \leq [L:K]\,.$$

Again , the exact sequence $1 \to L^\times \to I_L \to C_L \to 1$ induces an exact sequence

$$1 \to H^2(G_{L/K}, L^\times) \to H^2(G_{L/K}, I_L) \to H^2(G_{L/K}, C_L)$$

Therefore $\left|\frac{H^2(G_{L/K} I_L)}{H^2(G_{L/K}, L^\times)}\right| \leq |H^2(G_{L/K}, C_L)| \leq [L:K]$.

There the last inequality follows from Theorem 19.6.

The crucial point to show $H^2(G_{L/K}, C_L) \cong \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$, for any normal extension L/K, is the following theorem.

Theorem 20.3 If L/K is a normal extension, and L^1/K is a cyclic extension of equal degree $[L:K] = [L^1:K]$, then

$$H^2(G_{L^1/K^1}, C_{L^1}) = H^2(G_{L/K}, C_L) \subseteq H^2(G_{\Omega/K}, C_\Omega)$$

where Ω is an algebraic closure of K.

Proof We first show $H^2(G_{L^1/K}, C_{L^1}) \subseteq H^2(G_{L/K}, C_L)$. If $N = L \cdot L^1$ is the compositum of L and L^1, then N/L is also cyclic. Now let $\overline{c} \in H^2(G_{L^1/K}, C_{L^1}) \subseteq H^2(G_{N/K}, C_N)$.

By the exact sequence

$$1 \to H^2(G_{L/K}, C_L) \xrightarrow{\text{inv}} H^2(G_{N/K}, C_N) \xrightarrow{\text{res}_L} H^2(G_{N/L}, C_N)$$

We see that $\overline{c} \in H^2(G_{N/K}, C_N)$ is an element of $H^2(G_{L/K}, C_L)$ if and only if $\text{res}_L\, \overline{c} = 1$. To show this, we use the idèle invariants.

We have the following exact sequence

$$(**) \quad 1 \to H^2(G_{L^1/K}, L^{1\times}) \to H^2(G_{L^1/K}, I_{L^1}) \xrightarrow{j} H^2(G_{L^1/K}, C_{L^1}) \to H^3(G_{L^1/K}, L^{1\times})$$

Since $H^3(G_{L^1/K}, L^{1\times}) = H^1(G_{L^1/K}, L^{1\times}) = 1$, the map j is surjective. Hence there exists $c \in H^2(G_{L^1/K}, I_{L^1}) \subseteq H^2(G_{N/K}, I_N)$ s.t. $E = jc$.

Note that j commutes with inflation and with restriction, we have

$$\text{res}_L \overline{c} = \text{res}_L(jc) = j\text{res}_L c$$

Thus $\text{res}_L\, \overline{c} = 1 \Leftrightarrow \text{res}_L\, c \in \ker j = H^2(G_{N/L}, N^\times)$.

Since N/L is cyclic, by the proof of Hasse principle (i.e. $(*)$)

$$\text{res}_L c \in \ker j \Leftrightarrow \text{inv}_{N/L}(\text{res}_L c) = 0$$

This last statement now follows from

$$\text{inv}_{N/L}(\text{res}_L c) = [L:K]\, \text{inv}_{N/K}\, c = [L^1:K]\, \text{inv}_{L^1/K}\, c = 0$$

Therefore $H^2(G_{L/K}, C_{L^1}) \subseteq H^2(G_{L/K}, C_L)$. To obtain the equality, we just compare the orders of these groups. The exact sequence $(**)$ is

$$1 \to H^2(G_{L^1/K}, L^{1\times}) \to H^2(G_{L^1/K}, I_{L^1}) \to H^2(G_{L^1/K}, C_{L^1}) \to 1$$

We already have seen

$$|H^2(G_{L^1/K}, C_{L^1})| = \left| \frac{H^2(G_{L^1/K}, I_{L^1})}{H^2(G_{L^1/K}, L^{1\times})} \right| = [L^1 : K] = [L : K] .$$

On the other hand, $|H^2(G_{L/K}, C_L)| \mid [L : K]$ by Theorem 19.6.

Hence $H^2(G_{L/K}, C_L) = H^2(G_{L^1/K}, C_{L^1})$.

Note that in the above proof, for a cyclic extension L^1/K,

$$\begin{array}{ccccccccc} 1 & \longrightarrow & H^2(G_{L^1/K}, L^{1\times}) & \longrightarrow & H^2(G_{L^1/K}, I_{L^1}) & \longrightarrow & H^2(G_{L^1/K}, C_{L^1}) & \longrightarrow & 1 \\ & & & \searrow^{0} & \downarrow{\scriptstyle \mathrm{inv}_{L^1/K}} & \swarrow_{\mathrm{inv}_{L^1/K}}^{\exists} & & & \\ & & & & \frac{1}{[L^1:K]}\mathbb{Z}/\mathbb{Z} & & & & \end{array}$$

by Theorem 20.1

Theorem 20.4 The invariant maps

$$\mathrm{inv}_K : H^2(G_{\Omega/K}, C_\Omega) \to \mathbb{Q}/\mathbb{Z}$$

and

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

are isomorphisms.

We denote $U_{L/K} \in H^2(G_{L/K}, C_L)$ the fundamental class of L/K, which is (uniquely determined by $\mathrm{inv}_{L/K}(U_{L/K}) = \frac{1}{[L:K]} + \mathbb{Z}$.

Now Tate-Nakayama Theorem implies

Theorem 20.5 The homomorphism cup product with $U_{L/K}$ induces

$$H^1(G_{L/K}, \mathbb{Z}) \underset{\cong}{\overset{\bigcup U_{L/K}}{\longrightarrow}} H^{q+2}(G_{L/K}, C_L) .$$

In particular, for $q = -2$, we have

Theorem 20.6 (Artin reciprocity law)

$$\begin{array}{ccc} H^{-2}(G_{L/K}, \mathbb{Z}) & \xrightarrow{\bigcup U_{L/K}} & H^0(G_{L/K}, C_L) \\ \| & & \| \\ G_{L/K}^{ab} & \xleftarrow{\psi_{L/K} = \pi\psi_{L_\mathfrak{P}/K_\mathfrak{p}}} & C_K/N_G C_L \end{array}$$

Theorem 20.7 (Existence theorem) The norm groups of C_K are precisely the open subgroups of finite index, i.e., there is a bijection:

$$\begin{array}{ccc} (H \subset C_K \text{open of finite index}) & \overset{1\text{–}1}{\leftrightarrow} & (\text{finite abelian extension of } K) \\ N_{L/K}C_L & \leftarrow\!\shortmid & L \end{array}$$