

# Class Field Theory

Ido Karshon

November 27, 2025

Part I

# Group Cohomology

## Chapter 1

# Finite Group Cohomology

## 1.1 Definitions

Given two  $G$ -modules  $M, N$ , we consider  $\text{Hom}(M, N)$  as a  $G$ -module with action  $(g.f)(m) = g.f(g^{-1}m)$  and we consider  $M \otimes N$  as a  $G$ -module with action  $g.(m \otimes n) = (gm) \otimes (gn)$  (this will only become relevant later).

We denote by  $\text{Mod}_G$  the category of left  $G$ -modules. Let  $G$  be a finite group and let  $H \leq G$  be a subgroup. Let  $\text{Res}_H^G : \text{Mod}_G \rightarrow \text{Mod}_H$  be the restriction functor and let  $\text{Ind}_H^G, \text{Coind}_H^G : \text{Mod}_H \rightarrow \text{Mod}_G$  be the two induction functors, defined by

$$\text{Ind}_H^G(M) = \text{Hom}_H(\mathbb{Z}[G], M), \quad \text{Coind}_H^G(M) = \mathbb{Z}[G] \otimes_H M$$

where the left  $G$ -module action on  $\text{Hom}_H(\mathbb{Z}[G], M)$  is given by  $(g.f)(x) = f(xg)$ . There are adjunctions  $\text{Coind}_H^G \vdash \text{Res}_H^G \vdash \text{Ind}_H^G$ . In fact, there is a natural isomorphism  $\text{Ind}_H^G \rightarrow \text{Coind}_H^G$  defined by  $f \mapsto \sum_{g \in G/H} g \otimes_H f(g^{-1})$ , but we treat them as separate functors since this clarifies things (and since they differ in the infinite case). Note that all three functors are exact. Thus,  $\text{Ind}_H^G$  preserves injectives and  $\text{Coind}_H^G$  preserves projectives. Since  $\text{Ab} = \text{Mod}_{\{e\}}$  has enough injectives and projectives, so does  $\text{Mod}_G$ . As the functor of invariants  $(-)^G : \text{Mod}_G \rightarrow \text{Ab}$  is left exact, it has right derived functors that we denote by  $H^i(G, M)$  and call the cohomology of  $G$  with coefficients in  $M$ . Likewise, the functor of coinvariants  $(-)_G : \text{Mod}_G \rightarrow \text{Ab}$  is right exact, and has left derived functors that we denote by  $H_i(G, M)$  and call the homology of  $G$  with coefficients in  $M$ .

**Lemma 1.1.1** (Shapiro). *There are natural isomorphisms*

$$H^*(G, \text{Ind}_H^G M) \simeq H^*(H, M), \quad H_*(G, \text{Coind}_H^G M) \simeq H_*(H, M)$$

*Proof.* Consider an injective resolution  $M \rightarrow I_H^\circ$  in  $\text{Mod}_H$ . Then  $\text{Ind}_H^G I_H^\circ$  is an injective resolution of  $\text{Ind}_H^G M$  in  $\text{Mod}_G$ . Since  $(\text{Ind}_H^G I_H^\circ)^G \cong (I_H^\circ)^H$ , the first isomorphism follows. The second isomorphism is similar.  $\square$

Note that for a  $G$ -module  $M$  we have a  $G$ -module isomorphism  $\text{Hom}(\mathbb{Z}[G], M) \rightarrow \mathbb{Z}[G] \otimes M$  given by  $f \mapsto \sum_{g \in G} g \otimes f(g)$ .

**Lemma 1.1.2.** *Let  $M$  be a  $G$ -module. Then the  $G$ -modules  $\text{Hom}(\mathbb{Z}[G], M)$  and  $\mathbb{Z}[G] \otimes M$  are acyclic for both  $H^i$  and  $H_i$ .*

*Proof.* There is an adjunction  $\mathbb{Z}[G] \otimes (-) \vdash \text{Hom}(\mathbb{Z}[G], -)$ . Thus,  $\text{Hom}(\mathbb{Z}[G], -)$  is an exact functor that is adjoint to itself. It follows that it preserves injectives and projectives, and from the isomorphisms

$$\text{Hom}(\mathbb{Z}[G], M)^G \cong \text{Res } M, \quad (\mathbb{Z}[G] \otimes M)_G \cong \text{Res } M$$

the result follows.  $\square$

The bar resolution is the following projective resolution of  $\mathbb{Z}$  as a trivial  $G$ -module:

$$\cdots \rightarrow \mathbb{Z}[G]^{n+1} \rightarrow \mathbb{Z}[G]^n \rightarrow \cdots \rightarrow \mathbb{Z}[G]^2 \rightarrow \mathbb{Z}[G] \rightarrow \mathbb{Z} \rightarrow 0$$

where the map  $\mathbb{Z}[G] \rightarrow \mathbb{Z}$  is the augmentation map sending  $\sum_{g \in G} a_g g$  to  $\sum_{g \in G} a_g$ , and the differential  $\partial_n : \mathbb{Z}[G]^{n+1} \rightarrow \mathbb{Z}[G]^n$  is defined by

$$\partial_n(g_0, g_1, \dots, g_n) = \sum_{i=0}^n (-1)^i (g_0, \dots, g_{i-1}, g_{i+1}, \dots, g_n).$$

For any  $G$ -module  $M$ , there is a resolution

$$0 \rightarrow M \rightarrow C^0(G, M) \rightarrow C^1(G, M) \rightarrow C^2(G, M) \rightarrow \dots$$

where  $C^i(G, M) = \text{Hom}(\mathbb{Z}[G]^{i+1}, M)$  with the augmentation map  $M \rightarrow C^0(G, M)$  defined by  $m \mapsto (g \mapsto gm)$  and the differential  $\partial^i : C^i(G, M) \rightarrow C^{i+1}(G, M)$  defined by

$$(\partial^i f)(g_0, \dots, g_{i+1}) = \sum_{j=0}^{i+1} (-1)^j f(g_0, \dots, g_{j-1}, g_{j+1}, \dots, g_{i+1}).$$

Since  $C^i(G, M) = C^0(G, C^{i-1}(G, M))$  and  $C^0(G, M)$  was shown to be acyclic, we find that  $C^i(G, M)$  is an acyclic resolution. Thus, the cohomologies  $H^*(G, M)$  are isomorphic to the cohomologies of the complex

$$0 \rightarrow C^0(G, M)^G \rightarrow C^1(G, M)^G \rightarrow C^2(G, M)^G \rightarrow \dots$$

We identify the abelian group  $C^i(G, M)^G$  with the space of functions  $G^i \rightarrow M$  via the isomorphism

$$f \mapsto (g_1, \dots, g_i) \mapsto f(e, g_1, g_1 g_2, \dots, g_1 \cdots g_i).$$

This provides a concrete description of  $H^*(G, M)$  in terms of crossed homomorphisms. For instance,  $H^1(G, M)$  is the (additive) group of functions  $\phi : G \rightarrow M$  satisfying  $\phi(\sigma\tau) = \phi(\sigma) + \sigma.\phi(\tau)$  modulo the principal crossed homomorphisms, i.e. those of the form  $\phi(\sigma) = \sigma.m - m$  for some  $m \in M$ .

**Lemma 1.1.3.** *Let  $\phi : H^i \rightarrow M$  be a crossed homomorphism corresponding to an element of  $H^i(H, M)$ . Then a corresponding crossed homomorphism in  $\Phi : G^i \rightarrow \text{Ind}_H^G M$  under the Shapiro isomorphism is given by*

$$\Phi(g_0, \dots, g_i)(g) = \phi(\psi(gg_0), \dots, \psi(gg_i))$$

where  $\psi : G \rightarrow H$  is any function satisfying  $\psi(hg) = h\psi(g)$  for all  $h \in H, g \in G$ .

*Proof.* This follows from the construction of the Shapiro isomorphism, together with the isomorphism  $\text{Ind}_H^G(C^i(H, M)) \cong C^i(G, \text{Ind}_H^G M)$ , which is given by  $f \mapsto ((g_0, \dots, g_i) \mapsto g \mapsto f(g)(\psi(gg_0), \dots, \psi(gg_i)))$ .  $\square$

**Lemma 1.1.4.** *Let  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  be a short exact sequence of  $G$ -modules. The differentials in the long exact cohomology sequence  $\partial : H^i(G, C) \rightarrow H^{i+1}(G, A)$  correspond to the following construction in terms of crossed homomorphisms: Given a crossed homomorphism  $\phi : G^i \rightarrow C$ , lift it to a function  $\tilde{\phi} : G^i \rightarrow B$ , and define  $\partial\phi : G^{i+1} \rightarrow A$  by*

$$(\partial\phi)(g_0, \dots, g_{i+1}) = \sum_{j=0}^{i+1} (-1)^j \tilde{\phi}(g_0, \dots, g_{j-1}, g_{j+1}, \dots, g_{i+1}).$$

*Proof.* This follows from the construction of the long exact cohomology sequence.  $\square$

### 1.1.1 Examples

**Lemma 1.1.5.**  $H_1(G, \mathbb{Z}) = G^{ab}$

*Proof.* By the bar resolution,  $H_1(G, \mathbb{Z})$  is the cohomology of the complex  $\mathbb{Z}[G]_G^3 \rightarrow \mathbb{Z}[G]_G^2 \rightarrow \mathbb{Z}[G]_G$ . Its elements can be represented as sums  $\sum a_g(e, g)$  modulo the relations  $(e, g) + (g, h) - (e, gh) = 0$ .  $\square$

**Lemma 1.1.6.** *If  $M$  is a trivial  $G$ -module, then  $H^1(G, M) \cong \text{Hom}(G, M)$*

*Proof.* This follows from the crossed homomorphism description of  $H^1(G, M)$ .  $\square$

## 1.2 Restriction and Corestriction

We define the cohomology restriction map,  $\text{Res}_H^G : H^i(G, M) \rightarrow H^i(H, M)$ , as follows. Given an injective resolution  $M \rightarrow I_G^\circ$  in  $\text{Mod}_G$ , and an injective resolution  $\text{Res } M \rightarrow I_H^\circ$  in  $\text{Mod}_H$ , there is a unique-up-to-homotopy map  $I_G^\circ \rightarrow \text{Ind } I_H^\circ$  extending  $M \rightarrow \text{Ind } M$ . It induces a unique-up-to-homotopy map  $(I_G^\circ)^G \rightarrow (I_H^\circ)^H$ , and thus a well-defined  $H^*(G, M) \rightarrow H^*(H, M)$ . Following the proof of Shapiro's lemma, one sees that this map coincides with the composition

$$H^*(G, M) \rightarrow H^*(G, \text{Ind Res } M) \cong H^*(H, \text{Res } M).$$

In the same fashion, but with the projective resolutions  $P_G^\circ \rightarrow M$ ,  $P_H^\circ \rightarrow M$ , and the unique-up-to-homotopy map  $\text{Coind } P_H^\circ \rightarrow P_G^\circ$ , we define the cohomology corestriction map  $\text{Cor}_H^G : H^*(H, M) \rightarrow H^*(G, M)$ , which coincides with the composition

$$H^*(H, \text{Res } M) \cong H^*(G, \text{Ind Res } M) \cong H^*(G, \text{Coind Res } M) \rightarrow H^*(G, M).$$

In the same fashion we define the homology restriction map  $\text{Res}_H^G : H_i(G, M) \rightarrow H_i(H, \text{Res } M)$  and homology corestriction map  $\text{Cor}_H^G : H_i(H, \text{Res } M) \rightarrow H_i(G, M)$ .

In the construction of the cohomology restriction map, one sees that it suffices to use acyclic resolutions. Using the acyclic resolution  $C^i(G, M)$ , we find that under the restriction map, a crossed homomorphism  $\phi : G^i \rightarrow M$  is simply mapped to  $\phi|_{H^i}$ .

**Claim 1.2.1.** *Given a short exact sequence  $0 \rightarrow M \rightarrow M' \rightarrow M'' \rightarrow 0$ , the restriction and corestriction maps commute with the differentials of the long exact cohomology sequence. The same works for restriction and corestriction in the long exact sequence of homologies.*

*Proof.* Take  $M \rightarrow I_G^\circ, I_H^\circ, M' \rightarrow I_G'^\circ, I_H'^\circ, M'' \rightarrow I_G''^\circ, I_H''^\circ$ , such that there is a short exact sequence of the  $I_H^\circ$  and the  $I_G^\circ$ . Apply  $\text{Ind}$  to the  $I_H^\circ$  and construct a natural map between the short exact sequence of complexes. This shows the case of cohomology restriction. The other cases should be similar.  $\square$

**Claim 1.2.2.**  $\text{Cor} \circ \text{Res} = [G : H]$ .

*Proof.* This follows from  $M \rightarrow \text{Ind Res } M \cong \text{Coind Res } M \rightarrow M$  being multiplication by  $[G : H]$ .  $\square$

**Corollary 1.2.3.** *For  $i \geq 1$  the groups  $H^i(G, M)$  and  $H_i(G, M)$  are  $|G|$ -torsion.*

### 1.2.1 Examples

**Lemma 1.2.4.**  $H^2(G, \mathbb{Z}) \cong \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$

*Proof.* This follows from the cohomology long exact sequence induced by the short exact sequence  $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$ , together with  $H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \text{Hom}(G, \mathbb{Q}/\mathbb{Z})$  and the fact that  $H^i(G, \mathbb{Q}) = 0$ , as a divisible  $G$ -torsion group.  $\square$

The homology corestriction map  $H_1(H, \mathbb{Z}) \rightarrow H_1(G, \mathbb{Z})$  corresponds to the obvious map  $H^{\text{ab}} \rightarrow G^{\text{ab}}$ . However, the restriction map  $H_1(G, \mathbb{Z}) \rightarrow H_1(H, \mathbb{Z})$  corresponds to the Verlagerung map  $G^{\text{ab}} \rightarrow H^{\text{ab}}$  defined by  $x \mapsto \sum_i \psi(g_i x)$ , where  $g_i$  are coset representatives such that  $G = \bigcup H g_i$ , and  $\psi$  is defined by  $\psi(h g_i) = h$ . This map turns out to be well-defined.

### 1.3 Inflation and Co-Inflation

Suppose  $H \triangleleft G$ . We define the Cohomology inflation  $\text{Inf} : H^i(G/H, M^H) \rightarrow H^i(G, M)$  like so. Let  $M \rightarrow I_G^\circ$  be an injective resolution in  $\text{Mod}_G$  and let  $M^H \rightarrow I_{G/H}^\circ$  be an injective resolution in  $\text{Mod}_{G/H}$ . There is a unique-up-to-homotopy map  $I_{G/H}^\circ \rightarrow I_G^\circ$  in  $\text{Mod}_G$ , which induces a unique-up-to-homotopy map  $(I_{G/H}^\circ)^{G/H} \rightarrow (I_G^\circ)^G$ , and thus a well-defined map  $H^i(G/H, M^H) \rightarrow H^i(G, M)$ . We define the Homology coinflation  $\text{Coinf} : H_i(G, M) \rightarrow H_i(G/H, M_H)$  similarly.

As in the case of restrictions, we can compute the inflation of a crossed homomorphism  $\phi : (G/H)^i \rightarrow M^H$  explicitly, and it turns out to be the composition  $G^i \rightarrow (G/H)^i \xrightarrow{\phi} M^H \rightarrow M$ . The coinflation  $H_1(G, \mathbb{Z}) \rightarrow H_1(G/H, \mathbb{Z})$  corresponds to the obvious map  $G^{\text{ab}} \rightarrow (G/H)^{\text{ab}}$ .

**Theorem 1.3.1.** *Let  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  be a short exact sequence of  $G$ -modules. Denote  $C'^H = \text{im}(B^H \rightarrow C^H)$  and  $A'_H = \text{im}(A_H \rightarrow B_H)$ . Then inflation and coinflation commute with the differentials of the long exact homology and cohomology sequences, in the sense that the following squares commute:*

$$\begin{array}{ccc}
 H^i(G/H, C'^H) & \xrightarrow{\partial} & H^{i+1}(G/H, A^H) \\
 \downarrow & & \downarrow \text{Inf} \\
 H^i(G/H, C^H) & & \\
 \downarrow \text{Inf} & & \\
 H^i(G, C) & \xrightarrow{\partial} & H^{i+1}(G, A)
 \end{array}
 \qquad
 \begin{array}{ccc}
 H_i(G, C) & \xrightarrow{\partial} & H_{i-1}(G, A) \\
 \downarrow \text{Coinf} & & \downarrow \text{Coinf} \\
 H_i(G/H, C_H) & \xrightarrow{\partial} & H_{i-1}(G/H, A'_H)
 \end{array}$$

*Proof.* For cohomology we have an easy way to see this from the crossed homomorphism perspective. For homology, we have to pick projective resolutions  $P^A, P^B, P^C, P^{A_H}, P^{B_H}, P^{C_H}, P^{A'_H}$  with a map  $P^{A_H} \rightarrow P^{A'_H}$ . Begin with a cycle  $\alpha \in P^C$ . One path lifts it to  $P^B$ , takes boundary, lifts to  $P^A$ , and then reduces it via  $P^A \rightarrow P_H^A \rightarrow P^{A_H} \rightarrow P^{A'_H}$ . The other path reduces it via  $P^C \rightarrow P_H^C \rightarrow P^{C_H}$ , then lifts to  $P^{B_H}$ , takes boundary and lifts to  $P^{A'_H}$ . We need them to coincide in  $P^{B_H}$ . This follows from the commutative diagram

$$\begin{array}{ccccc}
 P^B & \longrightarrow & P_H^B & \longrightarrow & P^{B_H} \\
 \downarrow & & \downarrow & & \downarrow \\
 P^C & \longrightarrow & P_H^C & \longrightarrow & P^{C_H}
 \end{array}$$

One just needs to verify that it is possible to construct the resolution maps in this fashion.  $\square$

**Theorem 1.3.2.** *Inflation and Coinflation commute with restriction and corestriction.*

*Proof.* Starting with inflation-restriction and coinflation-corestriction: Looking at the original definitions, we get a square of injective/projective resolutions that we should prove is commutative (up to homotopy). But the diagonal map, to an injective/from a projective resolution, has to be unique up to homotopy.

For the other pairs, we note that their definitions were also basically coming from maps between the resolutions, only noting that the resolutions for  $\text{Ind } M$ ,  $\text{Coind } M$  are identical.  $\square$

#### 1.3.1 Deflation

We define the Deflation map  $\text{Def}_H^G : H_i(G, M) \rightarrow H_i(G/H, M^H)$  as the composition

$$H_i(G, M) \xrightarrow{\text{Coinf}} H_i(G/H, M_H) \xrightarrow{\text{Nm}_H^H} H_i(G/H, M^H).$$

## 1.4 The Quotient Action on Cohomology

Suppose  $H \leq G$  and  $\sigma \in G$ . We have the conjugation functor  $\sigma(-) : \text{Mod}_H \rightarrow \text{Mod}_{H^\sigma}$  sending  $M \in \text{Mod}_H$  to  ${}^\sigma M$ , with the action  $(\sigma h \sigma^{-1})(\sigma m) = {}^\sigma(hm)$ , and composition of such functors corresponds to multiplication in  $G$ . We get a natural isomorphism  $H^*(H, M) \cong H^*(H^\sigma, {}^\sigma M)$ . In the crossed-homomorphism perspective, this isomorphism corresponds to conjugating the input.

**Claim 1.4.1.** *If  $H \leq G$  and  $M$  is a  $G$ -module, then each  $\sigma \in G$  defines an isomorphism  $f_\sigma : H^*(H, M) \rightarrow H^*(H^\sigma, M)$ , and  $f_\sigma f_\tau = f_{\sigma\tau}$ .*

*Proof.* There is an isomorphism  ${}^\sigma M \cong M$  in  $\text{Mod}_{H^\sigma}$ , sending  ${}^\sigma m \mapsto \sigma m$ . This provides the map  $H^*(H, M) \cong H^*(H^\sigma, {}^\sigma M) \cong H^*(H^\sigma, M)$  that we denote  $f_\sigma$ . For the composition claim we write a diagram

$$\begin{array}{ccccc}
 H^*(H, M) & \longrightarrow & H^*(H^\tau, {}^\tau M) & \longrightarrow & H^*(H^\tau, M) \\
 & \searrow & \downarrow & & \downarrow \\
 & & H^*(H^{\sigma\tau}, {}^{\sigma\tau} M) & \longrightarrow & H^*(H^{\sigma\tau}, {}^\sigma M) \\
 & & & \searrow & \downarrow \\
 & & & & H^*(H^{\sigma\tau}, M)
 \end{array}$$

□

We can describe  $f_\sigma$  by taking an acyclic  $H$ -resolution and applying  $\sigma(-)$  to it. In the crossed homomorphism perspective, this corresponds to conjugating the inputs and applying  $\sigma$  to the output.

**Claim 1.4.2.** *The diagram*

$$\begin{array}{ccc}
 H^i(G, M) & & \\
 \downarrow \text{Res} & \searrow \text{Res} & \\
 H^i(H, M) & \xrightarrow{f_\sigma} & H^i(H^\sigma, M)
 \end{array}$$

*commutes.*

*Proof.* By the commutative diagram

$$\begin{array}{ccccc}
 H^*(G, M) & \longrightarrow & H^*(G^\sigma, {}^\sigma M) & \longrightarrow & H^*(G^\sigma, M) \\
 \downarrow \text{Res} & & \downarrow \text{Res} & & \downarrow \text{Res} \\
 H^*(H, M) & \longrightarrow & H^*(H^\sigma, {}^\sigma M) & \longrightarrow & H^*(H^\sigma, M)
 \end{array}$$

it suffices to prove that the map  $H^i(G, M) \xrightarrow{f_\sigma} H^i(G, M)$  is the identity, which is not difficult. □

**Corollary 1.4.3.** *In the case  $H \triangleleft G$ , these  $f_\sigma$  define an action of  $G/H$  on  $H^*(H, M)$ , and the image of restriction lies in the invariants of this action.*

**Claim 1.4.4.** *The cohomology  $H^i(H, M)$ , as a  $G/H$ -module, is the derived functor of  $(-)^H : \text{Mod}_G \rightarrow \text{Mod}_{G/H}$ .*

*Proof.* Take an explicit resolution  $M \rightarrow I_G^\bullet$ . The definition of the action was literally this: take the  $H$ -invariants, and then take cohomologies when remembering the  $G/H$ -action. □

**Corollary 1.4.5.** *Suppose  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  is an exact sequence of  $G$ -modules. Then the long exact sequence of  $H$ -cohomologies is  $G/H$ -equivariant.*

### 1.4.1 Grothendieck Spectral Sequence

Consider the functors  $(-)^H : \text{Mod}_G \rightarrow \text{Mod}_{G/H}$  and  $(-)^{G/H} : \text{Mod}_{G/H} \rightarrow \text{Ab}$ . Since the first,  $(-)^H$ , sends injectives to injectives (thus acyclics) we get the spectral sequences  $H^i(G/H, H^j(H, M)) \Rightarrow H^{i+j}(G, M)$  and  $H_i(G/H, H_j(H, M)) \rightarrow H_{i+j}(G, M)$ .

Since we know the maps from the boundary row and column of the Grothendieck spectral sequence,  $H^*(G/H, M^H) \rightarrow H^*(G, M)$  and  $H^*(G, M) \rightarrow H^*(H, M)$ , we see those are the inflation and the restriction! Note also that the internal  $G/H$ -module structure on  $H^j(H, M)$  is the one encountered before. This gives an exact sequence

$$0 \rightarrow H^1(G/H, M^H) \rightarrow H^1(G, M) \rightarrow H^1(H, M)^{G/H} \rightarrow H^2(G/H, M^H) \rightarrow H^2(G, M)$$

## 1.5 Tate Cohomology

Consider the norm map  $H_0(G, M) \xrightarrow{\text{Nm}} H^0(G, M)$ . We define the Tate cohomology  $\hat{H}_T^i(G, M)$  in the following way:

$$\hat{H}_T^i(G, M) = \begin{cases} H^i(G, M) & i > 0 \\ \text{coker} \left( H_0(G, M) \xrightarrow{\text{Nm}} H^0(G, M) \right) & i = 0 \\ \ker \left( H_0(G, M) \xrightarrow{\text{Nm}} H^0(G, M) \right) & i = -1 \\ H_{-i-1}(G, M) & i < -1 \end{cases}$$

**Lemma 1.5.1.** *Let  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  be a short exact sequence of  $G$ -modules. Then there is a long exact sequence of Tate cohomologies*

$$\begin{aligned} \cdots \rightarrow \hat{H}_T^{-2}(G, C) \rightarrow \hat{H}_T^{-1}(G, A) \rightarrow \hat{H}_T^{-1}(G, B) \rightarrow \hat{H}_T^{-1}(G, C) \rightarrow \\ \rightarrow \hat{H}_T^0(G, A) \rightarrow \hat{H}_T^0(G, B) \rightarrow \hat{H}_T^0(G, C) \rightarrow \hat{H}_T^1(G, A) \rightarrow \cdots \end{aligned}$$

*Proof.* This follows from a diagram chase (which is basically the Snake lemma) in the commutative diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & H_1(G, C) & \longrightarrow & H_0(G, A) & \longrightarrow & H_0(G, B) \longrightarrow H_0(G, C) \\ & & \downarrow \text{Nm} & & \downarrow \text{Nm} & & \downarrow \text{Nm} \\ & & H^0(G, A) & \longrightarrow & H^0(G, B) & \longrightarrow & H^0(G, C) \longrightarrow H^1(G, A) \longrightarrow \cdots \end{array}$$

□

**Lemma 1.5.2** (Shapiro lemma for Tate cohomology). *Let  $H \leq G$  and let  $M$  be an  $H$ -module. Then there are isomorphisms*

$$\hat{H}_T^i(G, \text{Ind}_H^G M) \cong \hat{H}_T^i(H, M)$$

for all  $i \in \mathbb{Z}$ .

*Proof.* For  $i > 0$  and  $i < -1$ , this is just the usual Shapiro lemma. For  $i = 0, -1$ , this follows from the commutative diagram

$$\begin{array}{ccccc} M_H & \xrightarrow{\text{Nm}_H} & M^H \\ \downarrow \sim & & \downarrow \sim \\ (\text{Coind } M)_G & \xrightarrow{\sim} & (\text{Ind } M)_G \xrightarrow{\text{Nm}_G} (\text{Ind } M)^G. \end{array}$$

□

**Lemma 1.5.3.** *Let  $M$  be a  $G$ -module. The (isomorphic)  $G$ -modules  $\text{Hom}(\mathbb{Z}[G], M)$  and  $\mathbb{Z}[G] \otimes M$  are acyclic for the Tate cohomology. That is,  $\hat{H}_T^i(G, \text{Hom}(\mathbb{Z}[G], M)) = 0$  and  $\hat{H}_T^i(G, \mathbb{Z}[G] \otimes M) = 0$  for all  $i \in \mathbb{Z}$ .*

*Proof.* This is known for  $i > 0$  and  $i < -1$ . For those values, it is required to show that the map

$$\text{Nm} : \text{Hom}(\mathbb{Z}[G], M)_G \rightarrow \text{Hom}(\mathbb{Z}[G], M)^G$$

is an isomorphism, which is straightforward to check. □

Consider the following two diagrams:

$$\begin{array}{ccc} H_0(G, M) & \xrightarrow{\text{Nm}_G} & H^0(G, M) \\ \downarrow \text{Res}_H^G & & \downarrow \text{Res}_H^G \\ H_0(H, M) & \xrightarrow{\text{Nm}_H} & H^0(H, M) \end{array} \quad \begin{array}{ccc} H_0(H, M) & \xrightarrow{\text{Nm}_H} & H^0(H, M) \\ \downarrow \text{Cor}_H^G & & \downarrow \text{Cor}_H^G \\ H_0(G, M) & \xrightarrow{\text{Nm}_G} & H^0(G, M) \end{array}$$

Their commutativity is straightforward to check explicitly, and they imply that restriction and corestriction maps extend naturally for Tate cohomology,

$$\text{Res}_H^G : \hat{H}_T^i(G, M) \rightarrow \hat{H}_T^i(H, M), \quad \text{Cor}_H^G : \hat{H}_T^i(H, M) \rightarrow \hat{H}_T^i(G, M).$$

**Lemma 1.5.4.** *The restriction and corestriction maps for Tate cohomology commute with the differentials of the long exact Tate cohomology sequence.*

*Proof.* This follows from a diagram chase in the three-dimensional version of the diagram from the proof of 1.5.1, where the front and back faces correspond to  $G$  and  $H$ . Note that the commutative diagrams from above appear as the squares connecting the two faces. The most involved part is following the map  $\hat{H}_T^{-1}(G, C) \rightarrow \hat{H}_T^0(G, A)$ . □

**Lemma 1.5.5.** *The composition  $\text{Cor}_H^G \circ \text{Res}_H^G$  on  $\hat{H}_T^i(G, M)$  is multiplication by  $[G : H]$ .*

*Proof.* This follows from the analogous fact for homology and cohomology. □

**Corollary 1.5.6.** *The group  $\hat{H}_T^i(G, M)$  is  $|G|$ -torsion for all  $i \in \mathbb{Z}$ .*

### 1.5.1 Tate Resolution

Suppose  $(P_i)_{i \geq 0}$  is a free  $G$ -resolution of  $\mathbb{Z}$  (for instance, the bar resolution), with differentials  $\partial : P_i \rightarrow P_{i-1}$  and an augmentation map  $\epsilon : P_0 \rightarrow \mathbb{Z}$ . Let  $P_{-i-1} = \text{Hom}(P_i, \mathbb{Z})$ , with the  $G$ -action defined by  $(g.f)(p) = f(pg)$ . There is a norm map  $\text{Nm} : P_0 \rightarrow P_0^* = P_{-1}$ , defined by sending  $a \in P_0$  to  $\epsilon(a) \cdot \epsilon$ . It is easy to check that this establishes an exact sequence

$$\cdots \xrightarrow{\partial} P_2 \xrightarrow{\partial} P_1 \xrightarrow{\partial} P_0 \xrightarrow{\text{Nm}} P_{-1} \xrightarrow{\partial^*} P_{-2} \xrightarrow{\partial^*} P_{-3} \xrightarrow{\partial} \cdots$$

**Lemma 1.5.7.** *Let  $M$  be a  $G$ -module. The  $i$ th cohomology of the complex*

$$\cdots \rightarrow \text{Hom}_G(P_{-2}, M) \rightarrow \text{Hom}_G(P_{-1}, M) \rightarrow \text{Hom}_G(P_0, M) \rightarrow \text{Hom}_G(P_1, M) \rightarrow \text{Hom}_G(P_2, M) \rightarrow \cdots$$

*is isomorphic to  $\hat{H}_T^i(G, M)$ .*

*Proof.* For  $i \geq 0$ , there is a  $G$ -module isomorphism  $P_i \otimes M \rightarrow \text{Hom}(P_i^*, M)$  defined by  $p \otimes m \mapsto \phi \mapsto \phi(p)m$ . Also, the norm map  $\text{Nm} : (P_i \otimes M)_G \rightarrow (P_i \otimes M)^G$  is an isomorphism. It follows that we have a commutative diagram

$$\begin{array}{ccccccccc}
\text{Hom}_G(P_i^*, A) & \xrightarrow{\sim} & \text{Hom}(P_i^*, A)^G & \xrightarrow{\sim} & (P_i \otimes A)^G & \xrightarrow{\sim} & (P_i \otimes A)_G & \xrightarrow{\sim} & P_i \otimes_G A \\
\downarrow f \mapsto (\phi \mapsto f(\phi\partial)) & & \downarrow f \mapsto (\phi \mapsto f(\phi\partial)) & & \downarrow \partial \otimes 1 & & \downarrow \partial \otimes 1 & & \downarrow \partial \otimes 1 \\
\text{Hom}_G(P_{i-1}^*, A) & \xrightarrow{\sim} & \text{Hom}(P_{i-1}^*, A)^G & \xrightarrow{\sim} & (P_{i-1} \otimes A)^G & \xrightarrow{\sim} & (P_{i-1} \otimes A)_G & \xrightarrow{\sim} & P_{i-1} \otimes_G A
\end{array}$$

which shows that the left-hand side of the complex computes  $\hat{H}_T^i(G, A)$  for  $i \leq -2$ . Since the boundary map  $P_0 \otimes_G M \cong \text{Hom}_G(P_0^*, M) \rightarrow \text{Hom}_G(P_0, M)$  corresponds to  $p \otimes m \mapsto p' \mapsto \varepsilon(p)\varepsilon(p')m$ , we see that  $\ker(P_0 \otimes_G M \rightarrow \text{Hom}_G(P_0, M)) = \ker(P_0 \otimes_G M \rightarrow M)$ , and thus the complex computes  $\hat{H}_T^{-1}(G, M)$  as well.

For the right-hand side, we just note that  $C^i(G, M) \cong \text{Hom}(P_i, M)$ . This shows that the complex computes  $\hat{H}_T^i(G, M)$  for  $i > 0$ , but the image of  $\text{Hom}(P_{-1}, M) \rightarrow C^0(G, M)$  is equal to the image of  $M \rightarrow C^0(G, M)$ , and thus the complex computes  $\hat{H}_T^0(G, M)$  as well.  $\square$

## 1.6 Cyclic group cohomology

If  $G = \mathbb{Z}/n$ , there is a special 2-periodic resolution of  $\mathbb{Z}$  by free  $G$ -modules:

$$\dots \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\text{Nm}} \mathbb{Z}[G] \xrightarrow{g-1} \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z}.$$

It follows that the Tate cohomologies  $\hat{H}_T(G, M)$  are 2-periodic. We let  $h(M) = \frac{\#\hat{H}_T^{\text{even}}(G, M)}{\#\hat{H}_T^{\text{odd}}(G, M)}$  when those cohomologies are finite.

**Lemma 1.6.1.** *If  $G$  is cyclic and  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  is a short exact sequence of  $G$ -modules, two of which have finite Tate cohomologies, then the third also has finite Tate cohomologies, and  $h(B) = h(A) \cdot h(C)$ .*

*Proof.* This follows from the long exact Tate cohomology sequence together with the 2-periodicity.  $\square$

**Lemma 1.6.2.** *If  $G$  is cyclic and  $M$  is a finite  $G$ -module, then  $h(M) = 1$ .*

*Proof.* Let  $\sigma$  be a generator of  $G$ . Consider the exact sequence  $0 \rightarrow M^G \rightarrow M \xrightarrow{\sigma-1} M \rightarrow M_G \rightarrow 0$ . Since all the modules in it are finite, it follows that  $|M^G| = |M_G|$ . However, there is also an exact sequence  $0 \rightarrow \hat{H}_T^{-1}(M) \rightarrow M_G \xrightarrow{\text{Nm}} M^G \rightarrow \hat{H}_T^0(M) \rightarrow 0$ . This time, we can deduce that  $|\hat{H}_T^{-1}(M)| = |\hat{H}_T^0(M)|$ . Thus  $h(M) = 1$ .  $\square$

**Corollary 1.6.3.** *If  $G$  is cyclic,  $M$  is a  $G$ -module with  $N \subseteq M$  a submodule of finite index, and if one of  $M$  or  $N$  has finite Tate cohomologies, then both do and  $h(M) = h(N)$ .*

## 1.7 Hilbert 90 and the Normal Basis Theorem

The Normal Basis Theorem states that for every finite Galois extension  $L/K$  with Galois group  $G$ , there is  $\alpha \in L$  such that  $\{\sigma\alpha \mid \sigma \in G\}$  is a basis for  $L/K$ . It means that  $L$  is a trivial  $G$ -module. (and for infinite fields it follows from a determinant argument, and generalizes the Primitive Element Theorem).

For the first cohomology, it is possible to define the cohomology with coefficients in a non-abelian group. Namely, if  $G$  is a group acting (from the left) on a group  $A$  by automorphisms, we define a crossed homomorphism  $\phi : G \rightarrow A$  to be a function satisfying  $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)^\sigma$ . Two crossed homomorphisms  $\phi, \psi$  are called equivalent if there is  $a \in A$  such that  $\psi(\sigma) = a^{-1}\phi(\sigma)a^\sigma$  for all  $\sigma \in G$ . This is an equivalence relation, and we define  $H^1(G, A)$  to be the (pointed) set of equivalence classes of crossed homomorphisms from  $G$  to  $A$ .

**Theorem 1.7.1** (Hilbert 90). *If  $L/K$  is Galois with group  $G$ , then  $H^1(G, \text{GL}_n(L)) = \{1\}$ .*

*Proof.* Let  $\phi : G \rightarrow \text{GL}_n(L)$  be a crossed homomorphism. Denote  $V = L^n$  and define a map  $\rho : G \rightarrow \text{Aut}_K(V)$  by  $\rho(\sigma)(v) = \phi(\sigma)(v^\sigma)$  for all  $v \in V$ . This map satisfies

1.  $\rho(\sigma)(\rho(\tau)(v)) = \rho(\sigma)(\phi(\tau)(v^\tau)) = \phi(\sigma)(\phi(\tau)^\sigma(v^{\sigma\tau})) = \phi(\sigma\tau)(v^{\sigma\tau}) = \rho(\sigma\tau)(v)$
2.  $\rho(\sigma)(\lambda v) = \phi(\sigma)(\sigma(\lambda)v^\sigma) = \sigma(\lambda) \cdot \rho(\sigma)(v)$ .

The first property says  $\rho$  is a group homomorphism, so  $V$  is a  $G$ -representation over  $K$ . Consider the function  $f : V \rightarrow V^G$  defined by  $f(v) = \sum_{\sigma \in G} \rho(\sigma)(v)$ . Using an independence-of-characters type argument, we can show that the image of  $f$  generates  $V$  as an  $L$ -vector space. This implies there are  $v_1, \dots, v_n \in V$  such that  $f(v_i)$  are  $L$ -independent. Let  $M$  be the matrix whose columns are  $f(v_1), \dots, f(v_n)$ . Then  $M \in \text{GL}_n(L)$ , and we have  $\rho(\sigma)(Mv) = Mv^\sigma$ . Thus,  $\phi(\sigma)(M^\sigma v^\sigma) = Mv^\sigma$ , implying that  $\phi(\sigma) = M \cdot (M^{-1})^\sigma$ . This shows that the crossed homomorphism  $\phi$  is equivalent to the trivial one.  $\square$

We write  $H^i(L/K)$  for  $H^i(\text{Gal}(L/K), L^\times)$ . Then Hilbert 90, for the case  $n = 1$ , says that  $H^1(L/K)$  vanishes.

**Theorem 1.7.2** (Normal Basis Theorem). *If  $L/K$  is a finite Galois extension with Galois group  $G$ , then there is an element  $\alpha \in L$  such that the set  $\{\sigma(\alpha) \mid \sigma \in G\}$  is a basis of  $L$  over  $K$ .*

**Corollary 1.7.3.** *If  $L/K$  is a finite Galois extension with Galois group  $G$ , then  $\hat{H}_T^i(G, L) = 0$ .*

## 1.8 Tate Cup Product

Let  $G$  be a finite group. Let  $P_i$  be the bar resolution, and let  $P_{-i-1} = \text{Hom}_{\mathbb{Z}}(P_i, \mathbb{Z})$  for  $i \geq 0$ , such that  $(P_i)_{i \in \mathbb{Z}}$  forms the Tate resolution of  $\mathbb{Z}$ .

**Theorem 1.8.1.** *There exists a  $\text{Mod}_G$ -map  $\phi_{a,b} : P_{a+b} \rightarrow P_a \otimes_{\mathbb{Z}} P_b$  such that*

1.  $\phi_{a,b} \circ \partial = (\partial \otimes 1) \circ \phi_{a+1,b} + (-1)^a (1 \otimes \partial) \circ \phi_{a,b+1}$ .
2.  $\varepsilon \circ \phi_{0,0} = \varepsilon \otimes \varepsilon$ .
3.  $(\phi_{a,b} \otimes \text{id}) \circ \phi_{a+b,c} = (\text{id} \otimes \phi_{b,c}) \circ \phi_{a,b+c}$

*Proof.* We define  $\phi$  as follows:

1.  $\phi_{p,q}(g_0, \dots, g_{p+q}) = (g_0, \dots, g_p) \otimes (g_p, \dots, g_{p+q})$
2.  $\phi_{-p,-q}(g_1^*, \dots, g_{p+q}^*) = (g_1^*, \dots, g_p^*) \otimes (g_{p+1}^*, \dots, g_{p+q}^*)$
3.  $\phi_{p,-p-q}(g_1^*, \dots, g_q^*) = \sum_{s_1, \dots, s_p} (g_1, s_1, \dots, s_p) \otimes (s_p^*, \dots, s_1^*, g_1^*, \dots, g_q^*)$
4.  $\phi_{-p-q,p}(g_1^*, \dots, g_q^*) = \sum_{s_1, \dots, s_q} (g_1^*, \dots, g_q^*, s_1^*, \dots, s_q^*) \otimes (s_q, \dots, s_1, g_q)$
5.  $\phi_{p+q,-q}(g_0, \dots, g_p) = \sum_{s_1, \dots, s_q} (g_0, \dots, g_p, s_1, \dots, s_q) \otimes (s_q^*, \dots, s_1^*)$
6.  $\phi_{-q,p+q}(g_0, \dots, g_p) = \sum_{s_1, \dots, s_q} (s_1^*, \dots, s_q^*) \otimes (s_q, \dots, s_1, g_0, \dots, g_p)$

and verify the properties by direct computation. □

This gives us a map  $\widehat{H}_T^i(G, M) \otimes \widehat{H}_T^j(G, N) \rightarrow \widehat{H}_T^{i+j}(G, M \otimes N)$ , called the Tate cup product. It is skew-commutative and associative. For  $i = j = 0$ , it corresponds to the obvious map  $(M^G / \text{Nm } M) \otimes (N^G / \text{Nm } N) \rightarrow (M \otimes_{\mathbb{Z}} N)^G / \text{Nm}(M \otimes_{\mathbb{Z}} N)$ .

From the compatibility of  $\phi$  with restrictions and corestrictions, we see that  $\text{Res}(\alpha\beta) = \text{Res}(\alpha) \text{Res}(\beta)$  and  $\text{Cor}(\alpha \cdot \text{Res}(\beta)) = \text{Cor}(\alpha) \cdot \beta$ ,

### 1.8.1 Inflation-deflation cup products

By compatibility of  $\phi$  with inflation and deflation maps, we have the following formulas relating cup products with inflation and deflation.

**Theorem 1.8.2.** *The following formulas hold:*

1. If  $|\alpha|, |\beta| > 0$ , then  $\text{Inf}(\alpha \cdot \beta) = \text{Inf}(\alpha) \cdot \text{Inf}(\beta)$
2. If  $|\alpha|, |\beta| \leq 0$ , then  $\text{Def}(\alpha \cdot \beta) = \text{Def}(\alpha) \cdot \text{Def}(\beta)$
3. If  $|\alpha| \leq 0, |\beta| > 0, |\alpha \cdot \beta| > 0$ , then  $\alpha \cdot \text{Inf}(\beta) = \text{Inf}(\text{Def}(\alpha) \cdot \beta)$ .
4. If  $|\alpha| \leq 0, |\beta| > 0, |\alpha \cdot \beta| \leq 0$ , then  $\text{Def}(\alpha) \cdot \beta = \text{Def}(\alpha \cdot \text{Inf}(\beta))$ .

### 1.8.2 Explicit cup product computations

Recall that  $H_1(G, \mathbb{Z}) = G^{\text{ab}}$ , with the identification  $(a, 1) \otimes 1 \leftrightarrow a$ . Using the canonical isomorphism  $\text{Hom}_G(\mathbb{Z}[G^2]^*, \mathbb{Z}) \cong \mathbb{Z}[G^2] \otimes_G \mathbb{Z}$ , we see that the element  $(a, 1) \otimes 1$  on the right-hand side corresponds to  $((g^*, h^*) \mapsto 1_{g=ha}) \in \text{Hom}_G(P_{-2}, \mathbb{Z})$ .

**Theorem 1.8.3.** *Under the canonical isomorphisms  $\hat{H}_T^1(G, \mathbb{Z}/n) \cong \text{Hom}(G, \mathbb{Z}/n)$  and  $\hat{H}_T^{-2}(G, \mathbb{Z}) \cong G^{\text{ab}}$ , and the canonical projection  $\mathbb{Z}/n \rightarrow \hat{H}_T^{-1}(G, \mathbb{Z}/n)$ , the product  $\hat{H}_T^1(G, \mathbb{Z}/n) \otimes \hat{H}_T^{-2}(G, \mathbb{Z}) \rightarrow \hat{H}_T^{-1}(G, \mathbb{Z}/n)$  corresponds to  $\chi \otimes a \mapsto \chi(a)$ .*

*Proof.* Recall  $P_{-1} \mapsto P_1 \otimes P_{-2}$  is defined by  $(g^*) \mapsto \sum_x (g, x) \otimes (x^*, g^*)$ . Then  $\chi \in \text{Hom}(G, \mathbb{Z}/n)$  and  $a \in G^{\text{ab}}$  are represented by  $(g, h \mapsto \chi(g^{-1}h)) \in \text{Hom}_G(P_1, \mathbb{Z}/n)$  and  $(g^*, h^*) \mapsto 1_{g=ha} \in \text{Hom}_G(P_{-2}, \mathbb{Z})$ . Their product is  $(g^*) \mapsto \chi(a)$ , which is  $\chi(a)$  under  $\hat{H}_T^{-1}(G, \mathbb{Z}/n) \cong \mathbb{Z}/n$   $\square$

**Theorem 1.8.4.** *Let  $M$  be a  $G$ -module. Then the cup product  $\hat{H}_T^2(G, M) \otimes \hat{H}_T^{-2}(G, \mathbb{Z}) \rightarrow \hat{H}_T^0(G, M)$  is explicitly given by  $\gamma \otimes \bar{\tau} \mapsto \sum_{\sigma \in G} \phi(\sigma, \sigma\tau)$ , where  $\tau \in G$  has the projection  $\bar{\tau} \in G^{\text{ab}}$ , and  $\phi : G \times G \rightarrow M$  is a representative for  $\gamma$ .*

*Proof.* The map  $P_0 \rightarrow P_2 \otimes P_{-2}$  is given by  $1 \mapsto \sum_{g, h \in G} (g, h) \otimes (h^*, g^*)$ . Then  $\gamma$  is represented by  $((g, h) \mapsto \phi(g, h)) \in \text{Hom}_G(P_2, A)$  and  $\bar{\tau}$  by  $((h^*, g^*) \mapsto 1_{h=g\tau}) \in \text{Hom}_G(P_{-2}, \mathbb{Z})$ . It follows that the cup product is  $\sum_{g, h \in G} 1_{h=g\tau} \phi(g, h) = \sum_{\sigma \in G} \phi(\sigma, \sigma\tau)$   $\square$

Any specific class in  $\hat{H}_T^2(G, M)$  induces a Nakayama map  $G^{\text{ab}} \rightarrow \hat{H}_T^0(G, A)$ .

## 1.9 Tate's Theorem

**Lemma 1.9.1.** *Let  $G$  be a finite group. Let  $M$  be a  $G$ -module. Suppose there is an integer  $i$  such that  $\hat{H}_T^i(H, M) = \hat{H}_T^{i+1}(H, M) = 0$  for all  $H \leq G$ . Then it vanishes for all  $i$ .*

*Proof.* This is trivial for  $G$  cyclic by 2-periodicity. By dimension shifting, it suffices to assume that the cohomology vanishes for  $i = 1, 2$ , and prove it for all  $i \geq 0$ .

Suppose first that  $G$  solvable. We will prove this by induction on the size of  $G$ . Let  $H \triangleleft G$  be a normal subgroup such that  $G/H$  is cyclic. Since the lemma holds for  $H$  by induction, We have  $\hat{H}_T^i(H, M) = 0$  for all  $i$ . Thus, by the spectral sequence  $H^i(G/H, H^j(H, M)) \implies H^{i+j}(G, M)$ , we get  $H^i(G, M) \cong H^i(G/H, M^H)$  for  $i > 0$ . Thus, the result follows for  $i > 0$  from the cyclic case. For  $i = 0$ , let  $x \in M^H$ . Since  $\hat{H}_T^0(G/H, M^H) = 0$ , we have  $x = N_{G/H}(y)$  for some  $y \in M^H$ . Since  $\hat{H}_T^0(H, M) = 0$ , we also have  $y = N_H(z)$  for some  $z \in M$ . It follows that  $x = N_G(z)$ , and thus  $\hat{H}_T^0(G, M) = 0$ .

For the case of a general  $G$ , we utilize the fact that for  $G_p$  a  $p$ -Sylow subgroup of  $G$ , the restriction map  $\text{Res} : \hat{H}_T^i(G, M) \rightarrow \hat{H}_T^i(G_p, M)$  is injective on the  $p$ -part and on the torsion-free part. Since  $G_p$  is solvable, this completes the proof.  $\square$

For a finite group  $G$ , we say that the  $G$ -module  $C$  is a class module for  $G$  if  $H^1(G, C) = 0$  and  $H^2(G, C)$  is a cyclic group of order  $\#G$ . A generator  $\gamma \in H^2(G, C)$  is then called a fundamental class.

**Definition 1.9.2.** *Consider the abelian group  $\mathbb{Z}^{G \setminus \{e\}}$ , with free generators  $x_\sigma$  for  $\sigma \in G \setminus \{e\}$ . For a  $G$ -module  $M$  and a 2-cocycle  $\phi : G \times G \rightarrow M$ , we define a  $G$ -module  $M(\phi)$ , called the splitting module of  $\phi$ , by the presentation*

$$M(\phi) = (\mathbb{Z}^{G \setminus \{e\}} \oplus M) / \langle \sigma(x_\tau) = x_{\sigma\tau} - x_\sigma + \phi(\sigma, \sigma\tau) \rangle$$

where  $\sigma, \tau$  run over all the elements of  $G \setminus \{e\}$ .

There is a  $G$ -module homomorphism  $M \rightarrow M(\phi)$  annihilating the cocycle  $\phi$ , whose cokernel is isomorphic to  $I_G$ . It is not too hard to check that the homomorphism  $M \rightarrow M(\phi)$  is also injective.

**Theorem 1.9.3** (Tate). *Let  $G$  be a finite group, and let  $C$  be a class module for  $G$  with fundamental class  $\gamma$ . Then a cup product with  $\gamma$  induces an isomorphism  $\hat{H}_T^*(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}_T^{*+2}(G, C)$  that we call the Tate isomorphism.*

*Proof.* We construct a natural homomorphism  $\hat{H}_T^*(G, M) \rightarrow \hat{H}_T^{*+2}(G, M \otimes_{\mathbb{Z}} C)$  for any  $G$ -module  $M$ . We will then show that it is an isomorphism when  $M = \mathbb{Z}$ , and that it is given by cup product with  $\gamma$ .

Let  $\phi : G \times G \rightarrow C$  be a representative for  $\gamma$ . Consider the exact sequence  $0 \rightarrow C \rightarrow C(\phi) \rightarrow \mathbb{Z}[G] \rightarrow \mathbb{Z} \rightarrow 0$ . This sequence is split over  $\mathbb{Z}$ , so we also have an exact sequence

$$0 \rightarrow M \otimes C \rightarrow M \otimes C(\phi) \rightarrow M \otimes \mathbb{Z}[G] \rightarrow M \rightarrow 0.$$

This sequence induces a spectral sequence, natural in  $M$ , that converges to 0 and has the first page

$$\begin{array}{ccccccc}
& \dots & & \dots & & \dots & & \dots \\
\widehat{H}_T^2(G, M \otimes C) & \longrightarrow & \widehat{H}_T^2(G, M \otimes C(\phi)) & \longrightarrow & \widehat{H}_T^2(G, M \otimes \mathbb{Z}[G]) & \longrightarrow & \widehat{H}_T^2(G, M) \\
\widehat{H}_T^1(G, M \otimes C) & \longrightarrow & \widehat{H}_T^1(G, M \otimes C(\phi)) & \longrightarrow & \widehat{H}_T^1(G, M \otimes \mathbb{Z}[G]) & \longrightarrow & \widehat{H}_T^1(G, M) \\
\widehat{H}_T^0(G, M \otimes C) & \longrightarrow & \widehat{H}_T^0(G, M \otimes C(\phi)) & \longrightarrow & \widehat{H}_T^0(G, M \otimes \mathbb{Z}[G]) & \longrightarrow & \widehat{H}_T^0(G, M) \\
& \dots & & \dots & & \dots & & \dots
\end{array}$$

Since  $M \otimes \mathbb{Z}[G]$  is acyclic, this spectral sequence collapses to a long exact sequence

$$\dots \rightarrow \widehat{H}_T^{i+1}(G, M \otimes C) \rightarrow \widehat{H}_T^{i+1}(G, M \otimes C(\phi)) \rightarrow \widehat{H}_T^i(G, M) \rightarrow \widehat{H}_T^{i+2}(G, M \otimes C) \rightarrow \dots$$

from which we get the desired homomorphism  $\widehat{H}_T^i(G, M) \rightarrow \widehat{H}_T^{i+2}(G, M \otimes C)$ .

In the case where  $M = \mathbb{Z}$  and  $i = 0$ , the map  $\widehat{H}_T^2(G, C) \rightarrow \widehat{H}_T^2(G, C(\phi))$  annihilates the class  $\gamma$  by the definition of  $C(\phi)$ , and thus is the zero map. It follows that the homomorphism  $\widehat{H}_T^0(G, \mathbb{Z}) \rightarrow \widehat{H}_T^2(G, C)$  is surjective, and hence an isomorphism since both groups have the same size.

Since  $\widehat{H}_T^1(G, C) = 0$  and  $\widehat{H}_T^1(G, \mathbb{Z}) = 0$ , it follows that the groups  $\widehat{H}_T^i(G, C(\phi))$  vanish for  $i = 1, 2$ . By the previous lemma we find that  $\widehat{H}_T^i(G, C(\phi))$  vanishes for all  $i$ , so the Tate homomorphism we constructed is an isomorphism for all  $i$  when  $M = \mathbb{Z}$ .

It remains to show that the Tate homomorphism coincides with cup product with  $\gamma$  for all  $M$ . By a coherence property connecting the long exact sequence above with the long exact sequence of Tate cohomologies arising from some  $0 \rightarrow M \rightarrow M' \rightarrow M'' \rightarrow 0$ , we can reduce the problem to the case  $i = 0$ . That is, we should show the Tate homomorphism  $\widehat{H}_T^0(G, M) \rightarrow \widehat{H}_T^2(G, M \otimes C)$  coincides with cup product with  $\gamma$ .

By the naturality of the construction in  $M$ , and since elemry element of  $\widehat{H}_T^0(G, M)$  lies in the image of  $\widehat{H}_T^0(G, \mathbb{Z}) \rightarrow \widehat{H}_T^0(G, M)$  for some homomorphism  $\mathbb{Z} \rightarrow M$ , it suffices to show the claim for  $M = \mathbb{Z}$  and  $i = 0$ . This can be checked directly from the definition.  $\square$

**Corollary 1.9.4.** *If  $C$  is a class module with fundamental class  $\gamma$ , then cup product with  $\gamma$  induces an isomorphism  $G^{ab} \rightarrow \widehat{H}_T^0(G, C)$  which is explicitly given by  $\bar{\tau} \mapsto \sum_{\sigma} \phi(\sigma, \sigma\tau)$  where  $\phi$  is a crossed homomorphism representing  $\gamma$ .*

## Chapter 2

# Profinite Group Cohomology

## 2.1 Profinite Cohomology

Let  $G$  be a profinite group. We denote the category of discrete  $G$ -modules by  $\text{Mod}_G$ . A  $G$ -module  $A$  is discrete if for every  $a \in A$ , the stabilizer of  $a$  is open in  $G$ . Equivalently,  $A = \bigcup_U A^U$ , where the union is over all open normal  $U \triangleleft G$ .

We define the functor  $C^i(G, -) : \text{Mod}_G \rightarrow \text{Mod}_G$  by  $C^i(G, M) = \varinjlim_U \text{Hom}(\mathbb{Z}[G/U]^{i+1}, M^U)$ . Note that  $C^i(G, -)$  is an exact functor.

**Lemma 2.1.1.** *Let  $\text{triv} : \text{Ab} \rightarrow \text{Mod}_G$  be the functor that considers an abelian group as a trivial  $G$ -module. Then  $C^0(G, -) \circ \text{triv} : \text{Ab} \rightarrow \text{Mod}_G$  is right-adjoint to the forgetful functor  $\text{Mod}_G \rightarrow \text{Ab}$ .*

*Proof.*

$$\begin{aligned} \text{Hom}_G(M, C^0(G, N)) &\cong \text{Hom}_G(\varinjlim_U M^U, \varinjlim_U \text{Hom}(\mathbb{Z}[G/U], N)) \cong \\ \varprojlim_U \text{Hom}_{G/U}(M^U, \text{Hom}(\mathbb{Z}[G/U], N)) &\cong \varprojlim_U \text{Hom}_{G/U}(M^U \otimes \mathbb{Z}[G/U], N) \cong \\ \varprojlim_U \text{Hom}((M^U \otimes \mathbb{Z}[G/U])^{G/U}, N) &\cong \varprojlim_U \text{Hom}((M^U \otimes \mathbb{Z}[G/U])_{G/U}, N) \cong \\ \varprojlim_U \text{Hom}(M^U, N) &\cong \text{Hom}(M, N). \end{aligned}$$

□

**Corollary 2.1.2.**  *$\text{Mod}_G$  has enough injectives.*

We can now define  $H^i(G, -)$  as the right derived functors of  $(-)^G : \text{Mod}_G \rightarrow \text{Ab}$ .

**Theorem 2.1.3.** *Let  $M$  be a discrete  $G$ -module. Then  $C^i(G, M)$  is acyclic.*

*Proof.* We have  $C^i(G, M) \cong C^0(G, C^{i-1}(G, M))$ , so it suffices to prove this for  $i = 0$ . Let  $I^\circ$  be an injective resolution of  $M$  in  $\text{Mod}_G$ . Since  $C^0(G, -)$  is exact, we find that  $C^0(G, I^\circ)$  is a resolution for  $C^0(G, M)$ . As  $C^0(G, I^\circ)^G \cong I^\circ$ , it suffices to show that the resolution  $C^0(G, I^\circ)$  is injective. That is, we need to show that  $C^0(G, -)$  preserves injectives.

Suppose  $N \subseteq M$  is an injection of  $G$ -modules, and we have a  $G$ -module map  $f : N \rightarrow C^0(G, I)$ , for  $I$  an injective  $G$ -module. We wish to extend  $f$  to  $M$ . It suffices to extend  $f$  to a single arbitrary element  $m \in M$ . We may replace  $N, M$  by  $\text{Span}(m) \cap N, \text{Span}(m)$ , to assume without loss of generality that  $M$  is finite. In this case we have  $M = M^U$  for some open normal  $U \triangleleft G$ . We may assume  $U$  is sufficiently small that the image of  $f$  consists of functions  $G/U \rightarrow I^U$ .

Thus, we have an inclusion of finite  $G/U$ -modules  $N \subseteq M$ , and we have a  $G/U$ -module map  $f : N \rightarrow \text{Hom}(\mathbb{Z}[G/U], I^U)$  that we wish to extend to  $M$ . We now have

$$\text{Hom}_{G/U}(N, \text{Hom}(\mathbb{Z}[G/U], I^U)) \cong \text{Hom}_{G/U}(N \otimes \mathbb{Z}[G/U], I^U)$$

and the functor  $(-) \otimes \mathbb{Z}[G/U] : \text{Mod}_{G/U} \rightarrow \text{Mod}_{G/U}$  is exact. Thus, it suffices to show that  $I^U$  is an injective  $G/U$ -module, which is clear.

□

**Remark 2.1.4.** *There is probably a way to do these arguments like in the finite case. I could not figure out what it is.*

Like in the finite case, cohomologies of a profinite group can be computed with crossed homomorphisms, that are now required to be continuous. It follows that  $H^n(G, A) = \varinjlim_U H^n(G/U, A^U)$ , as every crossed homomorphism factors through some  $U$ .

**Part II**

**Class Field Theory**

## Chapter 1

# Local Class Field Theory

## 1.1 Statement

Let  $K$  be a non-Archimedean local field. Note that every open subgroup of  $K^\times$  has finite index, however  $K^\times$  is not profinite. We let  $\widehat{K}^\times = \varprojlim_U K^\times/U$  where  $U$  runs over the open subgroups in  $K^\times$ . Then  $\widehat{K}^\times$  is the profinite completion of  $K^\times$ , and there is a bijection between open subgroups of  $\widehat{K}^\times$  and open subgroups of  $K^\times$ .

Local class field theory is the following statement.

**Theorem 1.1.1.** *There exists a profinite group isomorphism  $\phi_K : \widehat{K}^\times \rightarrow \text{Gal}(K^{ab}/K)$  such that  $\phi_K(\pi)|_{K^{un}} = \text{id}$  for every uniformizer  $\pi$  of  $K$ , and such that  $\phi_K(\text{Nm}_K^L L^\times) = \text{Gal}(K^{ab}/L)$  for every finite abelian Galois extension  $L/K$ .*

**Corollary 1.1.2.** *There is an isomorphism  $K^\times / \text{Nm}_K^L L^\times \cong \text{Gal}(L/K)$  for every finite abelian Galois extension  $L/K$ .*

**Corollary 1.1.3.** *The open subgroups in  $K^\times$  correspond bijectively to the finite abelian extensions of  $K$  via the norm map.*

## 1.2 The Invariant Map

### 1.2.1 Unramified Case

**Claim 1.2.1.** *For a finite unramified Galois extension  $L/K$  with Galois group  $G$ ,*

*Proof.* Since  $L^\times \cong U_L \times \mathbb{Z}$ , we find that  $\widehat{H}_T^i(G, U_L)$  is a direct summand of  $\widehat{H}_T^i(G, L^\times)$ , and in particular vanishes for  $i = 1$  by Hilbert 90. By the lemma preceding Tate's theorem, it suffices to show  $\widehat{H}_T^0(G, U_L) = 0$ , i.e. that  $\text{Nm} : U_L \rightarrow U_K$  is surjective, which can be shown using the filtrations of the unit groups.  $\square$

The short exact sequence  $0 \rightarrow U_L \rightarrow L^\times \rightarrow \mathbb{Z} \rightarrow 0$  provides isomorphisms  $\widehat{H}_T^i(L/K) \cong \widehat{H}_T^i(G, \mathbb{Z})$ . We define the invariant map  $\text{inv}_{L/K} : H^2(L/K) \rightarrow \mathbb{Q}/\mathbb{Z}$  by the composition

$$H^2(L/K) \cong H^2(G, \mathbb{Z}) \cong H^1(G, \mathbb{Q}/\mathbb{Z}) \cong \text{Hom}_{\text{cts}}(G, \mathbb{Q}/\mathbb{Z}) \rightarrow \mathbb{Q}/\mathbb{Z}$$

where the last map is the evaluation at the Frobenius element of  $G$ . Since this element generates  $G$ ,  $\text{inv}_{L/K}$  is injective. We can check that  $\text{inv}_{L/K}$  is invariant to inflations, and thus it induces a map  $\text{inv}_K : H^2(K^{un}/K) \rightarrow \mathbb{Q}/\mathbb{Z}$ .

**Claim 1.2.2.** *Let  $L/K$  be a finite extension. Then the following squares commute:*

$$\begin{array}{ccccc} H^2(K^{un}/K) & \xrightarrow{\text{Res}} & H^2(L^{un}/L) & H^2(L^{un}/L) & \xrightarrow{\text{Cor}} & H^2(K^{un}/K) \\ \downarrow \text{inv}_K & & \downarrow \text{inv}_L & \downarrow \text{inv}_L & & \downarrow \text{inv}_K \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{[L:K]} & \mathbb{Q}/\mathbb{Z} & \mathbb{Q}/\mathbb{Z} & \xlongequal{\quad} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

*Proof.* We have  $L^{un} = LK^{un}$ , so  $G_{L^{un}/L} \rightarrow G_{K^{un}/K}$  is injective. The first square, follows from the following diagram, where the rows are isomorphisms, and  $f, e$  are the residue degree and ramification

index of  $L/K$  respectively:

$$\begin{array}{ccccccc}
H^2(K^{\text{un}}/K) & \longrightarrow & H^2(\text{Gal}(\overline{K}/K), \mathbb{Z}) & \longleftarrow & H^1(\text{Gal}(\overline{K}/K), \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\
\downarrow \text{Res} & & \downarrow e \text{ Res} & & \downarrow e \text{ Res} & & \downarrow ef \\
H^2(L^{\text{un}}/L) & \longrightarrow & H^2(\text{Gal}(\overline{L}/L), \mathbb{Z}) & \longleftarrow & H^1(\text{Gal}(\overline{L}/L), \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

The case of corestrictions follows similarly.  $\square$

### 1.2.2 From the Unramified Case to General Case

**Lemma 1.2.3.** *Let  $K$  be a non-Archimedean local field. Let  $L/K$  be a finite Galois extension with Galois group  $G$ . Then  $|H^2(L/K)| \leq [L : K]$ .*

*Proof.* We begin with the case  $G$  is cyclic. By the normal basis theorem, there is  $\alpha \in L$  such that  $\{\sigma(\alpha) : \sigma \in G\}$  is a  $K$ -basis of  $L$ . The two  $G$ -submodules  $\mathcal{O}_L$  and  $\langle \alpha \rangle$  inside  $L$  are commensurable, so  $h(\mathcal{O}_L) = h(\langle \alpha \rangle) = h(\mathbb{Z}[G]) = 1$ . There exists a  $G$ -module isomorphism  $\log : U \rightarrow V$ , where  $U \subseteq \mathcal{O}_L^\times$  and  $V \subseteq \mathcal{O}_L$  are open sub- $G$ -modules, and it follows that  $h(\mathcal{O}_L^\times) = h(U) = h(V) = h(\mathcal{O}_L) = 1$ . Thus,  $h(L^\times) = h(\mathcal{O}_L^\times) \cdot h(\mathbb{Z}) = h(\mathbb{Z})$ . Since  $H^1(L/K)$  and  $H^1(G, \mathbb{Z})$  vanish, this implies  $|H^2(L/K)| = |H^0(L/K)| = |H^0(G, \mathbb{Z})| = [L : K]$ .

For the general case, we note that  $G$  has to be solvable as a Galois group over a local field. Thus, assuming  $G$  is not cyclic, there is a nontrivial Galois subextension  $K'/K$  of  $L/K$ . The spectral sequence for the corresponding group extension gives an exact sequence

$$0 \rightarrow H^2(K'/K) \xrightarrow{\text{Inf}} H^2(L/K) \xrightarrow{\text{Res}} H^2(L/K')^{\text{Gal}(K'/K)}$$

which finishes the proof by induction on  $[L : K]$ .  $\square$

**Theorem 1.2.4.** *The inflation map  $H^2(K^{\text{un}}/K) \rightarrow H^2(\overline{K}/K)$  is an isomorphism.*

*Proof.* The inflation map is injective by the spectral sequence together with Hilbert 90. Thus, it suffices to show surjectivity. Every  $\alpha \in H^2(\overline{K}/K)$  lies in the image of some inflation map  $H^2(L/K) \rightarrow H^2(\overline{K}/K)$  for a finite extension  $L/K$ . Denote  $n = [L : K]$ . Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & H^2(K^{\text{un}}/K) & \xrightarrow{\text{Res}} & H^2(L^{\text{un}}/L) \\
& & \downarrow & & \downarrow \text{Inf} & & \downarrow \text{Inf} \\
0 & \longrightarrow & H^2(L/K) & \longrightarrow & H^2(\overline{K}/K) & \xrightarrow{\text{Res}} & H^2(\overline{L}/L).
\end{array}$$

Since the middle vertical map is injective, the left vertical map is also injective. From the previous lemma we have  $|H^2(L/K)| \leq n$ . Thus, it follows that the left vertical map is an isomorphism, and  $\alpha$  lies in the image of  $\text{Inf} : H^2(K^{\text{un}}/K) \rightarrow H^2(\overline{K}/K)$ . This finishes the proof.  $\square$

**Remark 1.2.5.** *This proof also shows that  $H^2(L/K)$  is a cyclic group of order  $[L : K]$ .*

**Corollary 1.2.6.** *There is a natural isomorphism  $\text{inv}_K : H^2(\overline{K}/K) \rightarrow \mathbb{Q}/\mathbb{Z}$  such that the restrictions  $H^2(\overline{K}/K) \rightarrow H^2(\overline{L}/L)$  correspond to multiplication by  $[L : K]$  and the corestrictions  $H^2(\overline{L}/L) \rightarrow H^2(\overline{K}/K)$  correspond to the identity.*

### 1.3 The Artin Map

Let  $K$  be a non-Archimedean local field, and let  $L/K$  be a finite Galois extension with Galois group  $G$ . The previous discussion, together with Hilbert 90, shows that  $L^\times$  is a class module for  $G$ . Let  $u_{L/K} \in H^2(L/K)$  be the element with  $\text{inv}(u_{L/K}) = \frac{1}{[L:K]}$ . By Tate's theorem, cup product with  $u_{L/K}$  induces isomorphisms  $\hat{H}_T^i(G, \mathbb{Z}) \xrightarrow{\sim} \hat{H}_T^{i+2}(L/K)$ . In the particular case of  $i = -2$ , we get an isomorphism  $\phi_{L/K} : K^\times / \text{Nm}_L^K L^\times \xrightarrow{\sim} G^{\text{ab}}$ , which we call the Artin map of  $L/K$ . This map satisfies the following functoriality properties for a tower of extensions  $L/E/K$ :

$$\begin{array}{ccc} E^\times / \text{Nm}_L L^\times & \xrightarrow{\phi_{L/E}} & \text{Gal}(L/E)^{\text{ab}} \\ \downarrow \text{Nm} & & \downarrow \\ K^\times / \text{Nm}_L L^\times & \xrightarrow{\phi_{L/K}} & \text{Gal}(L/K)^{\text{ab}} \end{array} \quad \begin{array}{ccc} E^\times / \text{Nm}_L L^\times & \xrightarrow{\phi_{L/E}} & \text{Gal}(L/E)^{\text{ab}} \\ \uparrow & & \uparrow \text{Ver} \\ K^\times / \text{Nm}_L L^\times & \xrightarrow{\phi_{L/K}} & \text{Gal}(L/K)^{\text{ab}}. \end{array}$$

The short exact sequence  $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$  induces isomorphisms  $\hat{H}_T^i(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\partial} \hat{H}_T^{i+1}(G, \mathbb{Z})$ . Elements of  $H^1(G, \mathbb{Q}/\mathbb{Z})$  correspond to characters  $\chi : G \rightarrow \mathbb{Q}/\mathbb{Z}$ , and the corresponding 2-cocycle in  $H^2(G, \mathbb{Z})$  corresponding to  $\chi$  via this isomorphism is  $\delta_\chi(\sigma, \sigma\tau) = 1_{\tilde{\chi}(\sigma) + \tilde{\chi}(\tau) - \tilde{\chi}(\sigma\tau) = 1}$  where  $\tilde{\chi}(x)$  is the representative in  $[0, 1)$  for  $x \in \mathbb{Q}/\mathbb{Z}$ . The following is a useful lemma.

**Lemma 1.3.1.** *Let  $L/K$  be a finite Galois extension with degree  $n$  and Galois group  $G$ . Let  $\chi \in \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$  be a character, Then  $\chi(\phi_{L/K}(a)) = \text{inv}_{L/K}(a \cup \delta_\chi)$  for every  $a \in \hat{H}_T^0(L/K) \cong K^\times / \text{Nm}_L^K L^\times$ .*

*Proof.* Denote  $\alpha = \phi_{L/K}(a)$ , so  $a = \alpha \cup u_{L/K}$ . The left hand side, under the isomorphism  $(\mathbb{Q}/\mathbb{Z})[n] \cong \hat{H}_T^{-1}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\partial} \hat{H}_T^0(G, \mathbb{Z})$ , corresponds to the element  $\delta(\chi \cup \alpha)$ . Meanwhile, the right hand side is  $\text{inv}_{L/K}(a \cup \delta_\chi) = \text{inv}_{L/K}(\delta_\chi \cup \alpha \cup u_{L/K}) = \text{inv}_{L/K}(\delta(\chi \cup \alpha) \cup u_{L/K})$ . The result follows since  $\text{inv}_{L/K}(u_{L/K}) = \frac{1}{n}$ .  $\square$

**Corollary 1.3.2.** *Given a Galois tower  $L/E/K$ , we have  $\phi_{L/K}(a)|_{E/K} = \phi_{E/K}(a)$ .*

*Proof.* Let  $\chi : \text{Gal}(\bar{K}/K) \rightarrow \mathbb{Q}/\mathbb{Z}$  be a character factoring through  $\text{Gal}(E/K)$ , and let  $a \in K^\times$ . Then

$$\chi(\phi_{E/K}(a)) = \text{inv}_{E/K}(a \cup \delta_\chi) = \text{inv}_{L/K}(a \cup \delta_\chi) = \chi(\phi_{L/K}(a)).$$

where the equality in the middle uses the facts that  $\text{inv}$  and the cup product are compatible with inflations.  $\square$

**Claim 1.3.3.** *Let  $L/K$  be a finite unramified extension and let  $\pi_K$  be a uniformizer of  $K$ . Then  $\phi_{L/K}(\pi_K) = \text{Frob}_{L/K}$ .*

*Proof.* Let  $G = \text{Gal}(L/K)$ . We need to show that the Nakayama map  $G^{\text{ab}} \cong \hat{H}_T^{-2}(G, \mathbb{Z}) \rightarrow \hat{H}_T^0(L/K)$  defined by  $\bar{\tau} \mapsto \sum_{\sigma \in G} u_{L/K}(\sigma, \sigma\tau)$  sends the Frobenius element to the class of a uniformizer.

In the unramified case,  $\text{inv}_{L/K}$  is explicitly given by the isomorphism

$$\hat{H}_T^2(L/K) \cong \hat{H}_T^2(G, \mathbb{Z}) \cong \hat{H}_T^1(\mathbb{Q}/\mathbb{Z}) \rightarrow \mathbb{Q}/\mathbb{Z}$$

so the 2-cocycle  $u_{L/K}$  is given by  $(\sigma, \tau) \mapsto \pi_K^{\delta_\chi(\sigma, \tau)}$  for the character  $\chi : G \rightarrow \mathbb{Q}/\mathbb{Z}$  sending the Frobenius element to  $\frac{1}{n}$ . It follows that the image of  $\text{Frob}_{L/K}$  under the Nakayama map is

$$\prod_{i=0}^{n-1} \delta_\chi(\text{Frob}_{L/K}^i, \text{Frob}_{L/K}^{i+1})$$

in which only the last term is nonzero, and equals  $\pi_K$ .

where the last map is evaluation at the Frobenius element. Thus, the 2-cocycle  $u_{L/K}$  is defined by  $(\text{Frob}_{L/K}^i, \text{Frob}_{L/K}^j)$  corresponding to  $\frac{1}{n} \in \mathbb{Q}/\mathbb{Z}$

In our case, the cycle  $\phi \in H^2(L/K) \cong \text{Hom}_{\text{cts}}(G, \mathbb{Q}/\mathbb{Z})$  corresponds to  $\sigma \mapsto \frac{1}{n}$ , and thus its action is by  $(\sigma^i, \sigma^j) \mapsto \pi^{\frac{i\%n - j\%n + (j-i)\%n}{n}}$ . In particular, our value is  $\sum_\tau \phi(\tau, \tau\sigma) = \sum_{i=0}^{n-1} \phi(\sigma^i, \sigma^{i+1}) = \phi(\sigma^{n-1}, 1) = \pi$   $\square$

The last results combine to give a proof that there is a homomorphism  $\phi_K : K^\times \rightarrow G_K^{\text{ab}}$  satisfying the properties in Theorem 1.1.1. It only remains to show that  $\phi_K$  induces bijections between the open subgroups of  $K^\times$  and of  $G_K^{\text{ab}}$ .

## 1.4 Norm Limitation

Let  $K$  be a non-Archimedean local field of characteristic not dividing  $n$ . Suppose that  $\mu_n \subseteq K$ . Denote  $G = \text{Gal}(K^{\text{ab}}/K)$ . Consider the short exact Kummer sequence  $0 \rightarrow \mu_n \rightarrow (K^{\text{ab}})^\times \xrightarrow{n} (K^{\text{ab}})^\times \rightarrow 0$ . By the long exact sequence in cohomology, and Hilbert 90, we get an isomorphism  $H^2(G, \mu_n) \cong H^2(K^{\text{ab}}/K)[n] \cong (\mathbb{Q}/\mathbb{Z})[n]$  and an isomorphism  $H^1(G, \mu_n) \cong H^0(K^{\text{ab}}/K)/n \cong K^\times/n$ . The first isomorphism gives us  $H^2(G, \mu_n \otimes \mu_n) \cong \mu_n$  by the cup product. It follows that the cup product  $H^1(G, \mu_n) \otimes H^1(G, \mu_n) \rightarrow H^2(G, \mu_n \otimes \mu_n)$  is equivalent to a natural bilinear, skew-commutative map  $(K^\times/n) \otimes (K^\times/n) \rightarrow \mu_n$ . We call this the Hilbert symbol.

**Lemma 1.4.1.**  $\phi_{K(a^{\frac{1}{n}})/K}(b)(a^{\frac{1}{n}}) = (a, b)a^{\frac{1}{n}}$ .

*Proof.* Consider the following commutative diagram. We omit  $G$  from the notation for brevity:

$$\begin{array}{ccccccc} \widehat{H}_T^{-2}(\mathbb{Z}) \otimes \widehat{H}_T^0((K^{\text{ab}})^\times)/n & \longrightarrow & \widehat{H}_T^{-2}(\mathbb{Z}) \otimes \widehat{H}_T^1(\mu_n) & \longrightarrow & \widehat{H}_T^0((K^{\text{ab}})^\times) \otimes \widehat{H}_T^1(\mu_n) & \longrightarrow & \widehat{H}_T^1(\mu_n) \otimes \widehat{H}_T^1(\mu_n) \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \widehat{H}_T^{-2}((K^{\text{ab}})^\times)/n & \longrightarrow & \widehat{H}_T^{-1}(\mu_n) & \longrightarrow & \widehat{H}_T^1((K^{\text{ab}})^\times \otimes \mu_n) & \longrightarrow & \widehat{H}_T^2(\mu_n \otimes \mu_n). \end{array}$$

Starting from  $\phi_K(b) \otimes a$  on the top left, following the top row and then down, and then applying the map

$$\widehat{H}_T^2(\mu_n \otimes \mu_n) \rightarrow \widehat{H}_T^2((K^{\text{ab}})^\times \otimes \mu_n) \xrightarrow{\text{inv} \otimes \text{id}} \mu_n$$

we get exactly  $(a, b)$ .

Going down and then one step right, we get the element  $\frac{\phi_K(b)(a^{\frac{1}{n}})}{a^{\frac{1}{n}}} \in \mu_n \cong \widehat{H}_T^{-1}(\mu_n)$ . So it remains to show that the composition

$$\mu_n \rightarrow \widehat{H}_T^{-1}(\mu_n) \xrightarrow{\cup u_{L/K}} \widehat{H}_T^1((K^{\text{ab}})^\times \otimes \mu_n) \rightarrow \widehat{H}_T^2(\mu_n \otimes \mu_n) \rightarrow \widehat{H}_T^2((K^{\text{ab}})^\times \otimes \mu_n) \xrightarrow{\text{inv} \otimes \text{id}} \mu_n$$

is the identity. Since a cup product with a generator of  $\widehat{H}_T^0(\mu_n)$  induces isomorphisms on all cohomologies of  $n$ -torsion  $G$ -modules, it suffices to show that the composition

$$\mathbb{Z}/n\mathbb{Z} \rightarrow \widehat{H}_T^{-1}(\mathbb{Z}/n\mathbb{Z}) \xrightarrow{\cup_{L/K}} \widehat{H}_T^1((K^{\text{ab}})^{\times}/n) \xrightarrow{\delta} \widehat{H}_T^2(\mu_n) \xrightarrow{\text{inv}} \mathbb{Z}/n\mathbb{Z}$$

is the identity. This can be checked.  $\square$

**Corollary 1.4.2.** *The Hilbert symbol is nondegenerate. Further,  $(a, b) = 1$  if and only if  $b$  is a norm in  $K(a^{\frac{1}{n}})$ .*

**Corollary 1.4.3.** *Suppose  $K$  is a non-Archimedean local field of characteristic not dividing  $n$ . Suppose that  $K$  contains  $\mu_n$ . Then elements of  $K$  which are norms in every  $\mathbb{Z}/n\mathbb{Z}$ -extension of  $K$  belong to  $(K^{\times})^n$ .*

**Theorem 1.4.4.** *Let  $K$  be a non-Archimedean local field. Then  $\bigcap_{L/K} \text{Nm}_K^L(L^{\times}) = 1$  where the intersection is over all finite extensions  $L/K$ .*

*Proof.* Denote  $D_K = \bigcap_{L/K} \text{Nm}_K^L(L^{\times})$ . For a finite extension  $K'/K$  it is clear that  $\text{Nm}_K^{K'}(D_{K'}) \subseteq D_K$ . However, for any nontrivial  $x \in D_K$  it is the case that the subset  $(\text{Nm}_K^{K'})^{-1}(\{x\}) \subseteq K'^{\times}$  intersects every norm subgroup of  $K'^{\times}$ , and a compactness argument shows that it must intersect  $D_{K'}$  as well. Therefore we have  $\text{Nm}_K^{K'}(D_{K'}) = D_K$ .

By the previous corollary it follows that  $D_K \subseteq (K^{\times})^n$  for every  $n$  that is not divisible by the characteristic of  $K$ . By the structure of non-Archimedean local fields, this implies that  $D_K$  is trivial.  $\square$

**Lemma 1.4.5.** *If  $U \subseteq K^{\times}$  is a norm group then any subgroup of  $K^{\times}$  containing  $U$  is also a norm group.*

*Proof.* This follows from the partial version of local class field theory we have proven so far.  $\square$

**Theorem 1.4.6** (Pre-Existence). *Every subgroup of finite index in  $K^{\times}$  is a norm group from some finite extension  $L/K$ .*

**Remark 1.4.7.** *It is true that  $L$  can be taken to be abelian over  $K$ , but right now we prove this weaker version.*

*Proof.* Let  $U \subseteq K^{\times}$  be a subgroup of finite index. As  $D_K = 0$ , there exists some  $L/K$  such that  $U \supset \text{Nm } L^{\times}$ . This implies  $U$  is a norm group.  $\square$

**Theorem 1.4.8** (Norm Limitation). *Let  $L/K$  be finite, not necessarily Galois. Let  $E/K$  be the largest abelian subextension of  $L$ . Then  $\text{Nm}_K^L(L^{\times}) = \text{Nm}_K^E(E^{\times})$ .*

*Proof.* For  $L/K$  Galois this is clear by the Artin map, as  $\text{Gal}(L/K)^{\text{ab}} \cong \text{Gal}(E/K)$ . In general, let  $\hat{L}$  be the Galois closure of  $L/K$ .

Consider the commutative diagram

$$\begin{array}{ccc} L^{\times} / \text{Nm } \hat{L}^{\times} & \xrightarrow{\sim} & \text{Gal}(\hat{L}/L)^{\text{ab}} \\ \downarrow \text{Nm} & & \downarrow \\ K^{\times} / \text{Nm } \hat{L}^{\times} & \xrightarrow{\sim} & \text{Gal}(\hat{L}/K)^{\text{ab}} \\ \downarrow & & \downarrow \\ K^{\times} / \text{Nm } E^{\times} & \xrightarrow{\sim} & \text{Gal}(E/K)^{\text{ab}}. \end{array}$$

The theorem follows from the right column being exact in the middle. This is a fact on groups:  $N^{\text{ab}} \rightarrow G^{\text{ab}} \rightarrow (G/N)^{\text{ab}}$  is exact. Note that we used  $\text{Gal}(E/K)^{\text{ab}} = \text{Gal}(L/K)^{\text{ab}}$ .  $\square$

**Remark 1.4.9.** *For the commutativity of the lower square, we need to show the compatibility of the cup product and the deflation map.*

This implies the full form of local class field theory: that in addition to the properties of  $\phi_K$ , there is a bijection between the open subgroups of  $K^\times$  and the abelian extensions of  $K$ .

## Chapter 2

# Brauer Groups

## 2.1 General Semisimple Theory

Let  $A$  be a finite  $k$ -algebra and consider finitely generated  $A$ -modules. An  $A$ -module is Simple if it has no nontrivial submodules. It is Semisimple if every submodule is a direct summand. It is indecomposable if it has no nontrivial direct summands.

**Theorem 2.1.1.** *Semisimplicity is preserved by subquotients.*

*Proof.* For quotients, this is clear. If  $N \leq M$  and  $M$  semisimple, then given  $P \leq N$  we have  $M = P \oplus Q = N \oplus K$ , and this implies  $N = P \oplus \ker(Q \rightarrow K)$   $\square$

It follows that semisimplicity is equivalent to being a direct sum, or just any sum, of simples: just take a simple submodule and add it to the direct sum.

**Theorem 2.1.2.** *Suppose  $\bigoplus P_i \cong \bigoplus Q_j$  for  $P_i, Q_j$  indecomposable  $A$ -modules. Then they can be paired into isomorphic pairs.*

*Proof.* First note that any automorphism of an indecomposable is invertible or nilpotent. As the sum of an invertible and nilpotent is invertible, it follows the sum of nilpotents is nilpotent. Then, it follows that each composition  $P_i \rightarrow Q_j \rightarrow P_i$  is either a sequence of isomorphisms or is a nilpotent endomorphism of  $P_i$ . Thus we can delete maps that are not isomorphisms. This finishes the proof  $\square$

Remark: In the case of  $A$  a general ring, this holds for direct sums of simple modules, as can be seen by filtering each component of one filtration through the other filtration.

$A$  is simple if it has no nontrivial two-sided ideals.  $A$  is central if its center (which is always a field!) is  $k$ .  $A$  is a central simple algebra (CSA) if it is both.

**Theorem 2.1.3.** *A simple algebra is semisimple over itself.*

*Proof.* Let  $S$  be a minimal left ideal of  $A$ . Then  $A = \sum_a Sa$  by simplicity, meaning  $A$  is a sum of simple modules and thus semisimple  $\square$

## 2.2 Central Simple Algebras

From now on, we restrict to  $A$  being a finite  $k$ -algebra.

**Theorem 2.2.1.** *If  $V$  is a faithful semisimple  $A$ -module, then  $C(C(A)) = A$  (centralizer taken in  $\text{End}_k(V)$ ).*

*Proof.* It suffices to show that for all  $v_1, \dots, v_n \in V, b \in C(C(A))$  there is  $a \in A$  so that  $av_i = bv_i$ . Suffices to show this for  $n = 1$  by considering  $V^n$ , in which  $C(A) = M_n(\text{End}_A(V))$  and thus the  $C(C(A))$  just grows. In that case, there is an  $A$ -linear projection  $V \rightarrow AV \subseteq V$  by semisimplicity, that must commute with  $B$ , so  $AV = BV$   $\square$

**Theorem 2.2.2.** *If  $A$  is simple,  $A \cong M_n(D)$  for  $D$  a division field. (this is clearly unique)*

*Proof.*  $A = S^n$  for a simple module  $S$ . Then  $A^{\text{opp}} = \text{End}_A(S^n) = M_n(\text{End}_A S) = M_n(D)$   $\square$

Remark: this also follows from  $A = \text{End}_D(S) = \text{End}_D(D^n) = M_n(D^{\text{opp}})$ .

**Theorem 2.2.3.**  $C(B \otimes B') = C(B) \otimes C(B')$

*Proof.* This is the intersection of  $C(B) \otimes A', A \otimes C(B')$   $\square$

**Theorem 2.2.4.**  $CSA \otimes SA = SA$ . In particular,  $CSA \otimes CSA = CSA$ .

*Proof.* We know the CSA is  $M_n(D)$  for  $D$  a central division algebra.  $M_n(D) \otimes SA = M_n(D \otimes SA)$ . To see that matrices over a simple algebra are simple, take a matrix, take out some  $E_{i,j}(\alpha)$ , then this can be made into any  $E_{k,l}(\beta)$  which obviously generate everything. So we may assume  $n = 1$ , and then  $D$ -operations can be used to reduce an element of  $D \otimes A$  to  $Z(D) \otimes A = k \otimes A$ , which finishes from simplicity of  $A$   $\square$

Note that for any CSA we have  $A \otimes A^{\text{opp}} = M_n(k)$  (because the map is injective, together with a dimension count).

**Theorem 2.2.5** (Noether Skolem). *Any two maps  $f, g : SA \rightarrow CSA$  are conjugate.*

*Proof.* First suppose those are maps  $f, g : A \rightarrow M_n(k)$ . Then their images describe the structure of an  $A$ -module for  $k^n$ , which must be  $S^m$ , and in particular isomorphic for  $f, g$  so they are conjugate. In the general case, we get that  $f \otimes 1_{A^{\text{opp}}}, g \otimes 1_{A^{\text{opp}}}$  are conjugate, meaning  $x(f(a) \otimes a^{\text{opp}}) = (g(a) \otimes a^{\text{opp}})x$ . Plugging initially  $a = 1$ , this shows that  $x$  can be written as  $\sum u \otimes v$  for  $v \in C(A^{\text{opp}}) = k$ . Thus, we get that  $f, g$  are really conjugate  $\square$

**Theorem 2.2.6.** *The only CSA's over an algebraically closed field are trivial.*

*Proof.* It suffices to prove a division ring  $D$  over  $\bar{k}$  is trivial. And indeed, any element of  $D$  generates a field extension of  $\bar{k}$ , which must be trivial  $\square$

**Theorem 2.2.7.** *A finite division algebra is a field.*

*Proof.* If the center is  $\mathbb{F}_q$ , Take a maximal subfield  $\mathbb{F}_{q^l} \subseteq D$ , then each element is conjugate to an element of this  $\mathbb{F}_{q^l}$ , which is impossible by cardinality considerations  $\square$

## 2.3 The Brauer Group

We define the Brauer Group  $B(k)$  as the set of CSA's over  $k$  with tensor as product, where the two algebras  $A, M_n(A)$  are equivalent. Since  $A \otimes A^{\text{opp}} \cong M_n(k)$ , this is indeed a group.

If  $L/K$  is a field extension, we get a group homomorphism  $\text{Br}(K) \xrightarrow{\otimes_K L} \text{Br}(L)$ . Choosing  $L = \bar{K}$  proves that all CSA's have a square dimension.

Define  $\text{Br}(L/K) = \ker(\text{Br}(K) \rightarrow \text{Br}(L))$ , and we say that  $\alpha \in \text{Br}(K)$  splits over  $L$  if it is in  $\text{Br}(L/K)$ . Thus  $\text{Br}(K) = \text{Br}(\bar{K}/K) = \bigcup_{L/K \text{ finite}} \text{Br}(L/K)$ .

**Theorem 2.3.1.** *Let  $A$  be a CSA and  $B \subseteq A$  a SA. Then  $C_A(B)$  is simple, of dimension  $\frac{\dim A}{\dim B}$ . In particular, this is an integer!*

*Proof.* There are two inclusions  $B \rightarrow A \otimes \text{End}_k(B)$ , by  $1 \otimes B$  and  $B \otimes 1$ . By Noether Skolem, they are conjugate, so their centralizers are isomorphic:  $C_A(B) \otimes \text{End}_k(B) \cong A \otimes B^{\text{opp}}$ . This finishes the proof  $\square$

**Corollary 2.3.2.** *If  $B \subseteq A$  and both are CSAs, then the natural map  $B \otimes C_A(B) \rightarrow A$  is an isomorphism.*

*Proof.* The map is injective, since the domain is simple. From a dimension count, we get the result  $\square$

Let  $A$  be a CSA and  $L \subseteq A$  be a field. We say  $L$  is a maximal subfield if  $L = C_A(L)$ , or equivalently  $\dim L = \sqrt{\dim A}$ , or equivalently  $L$  is a maximal commutative subalgebra.

**Proposition 2.3.3.** *a field  $L/K$  splits a CSA iff there is  $B \sim_{\text{Br}} A$  containing  $L$  as a maximal subfield. In particular, the maximal subfields of a CSA split it.*

*Proof.* Suppose  $L$  splits  $A$ . Then  $A^{\text{opp}} \otimes L \cong \text{End}_L(V) = C_{\text{End}_k(V)}(L)$ , so  $L \cong C_{\text{End}_k(V)}(A^{\text{opp}} \otimes L)$ . Take  $B = C_{\text{End}_k(V)}(A^{\text{opp}} \otimes 1)$ . Conversely,  $1 \otimes L \subseteq B \otimes B^{\text{opp}}$  has centralizer  $\text{End}_L(B) \cong B \otimes L$  (with the  $L$ -module structure of  $B$  being from the right)  $\square$

**Proposition 2.3.4.** *There is always a separable maximal subfield.*

*Proof.* Take a maximal separable subfield  $K$ . Its centralizer is a CSA over  $K$ , so wlog  $K = k$  and we should prove there is some separable subfield. Otherwise, every  $a \in A$  satisfies  $a^{p^r} \in k$  for a fixed  $r$ . But then  $a^{p^r} \in \bar{k}$  for  $a \in A_{\bar{k}} = M_n(\bar{k})$ , which is not true for  $n > 1$  with e.g.  $\text{diag}(1, \dots, 0)$   $\square$

## 2.4 Isomorphism with Second Cohomology

**Theorem 2.4.1.** *There is a natural isomorphism  $\text{Br}(L/K) \cong \widehat{H}_T^2(L/K)$ . Restriction corresponds to  $\text{Br}(E/K) \xrightarrow{\otimes L} \text{Br}(E/L)$ . Inflation corresponds to  $\text{Br}(L/K) \subseteq \text{Br}(E/K)$ .*

*Proof.* Take  $A \in \text{Br}(L/K)$ . If we require  $L$  be a maximal subfield of  $A$ , there is a unique choice for  $A$ . The distinct embeddings of  $L \subseteq A$  by Galois automorphism, together with Noether-Skolem, show there are  $e_\sigma \in A$  such that conjugation by them applies  $\sigma$  on  $L$ . They are defined up to  $L^\times$ . Define  $\phi(\sigma, \sigma\tau) = e_\sigma e_\tau e_{\sigma\tau}^{-1} \in L^\times$ . It is a cocycle, and changing  $e_\sigma \mapsto \lambda e_\sigma$  alters  $\phi$  by a generic coboundary.

As any other injection  $L \rightarrow A$  is conjugate, it will define the conjugate crossed homomorphism  $\phi'(\sigma, \sigma\tau) = x\phi(\sigma, \sigma\tau)x^{-1}$ , which are equal under the two distinct identifications of  $L$  with subalgebras (this is also true for conjugation with  $e_\sigma$ ). As a result, we see that  $A$  defines an element of  $\widehat{H}_T^2(L/K)$ . This defines a map  $\text{Br}(L/K) \rightarrow \widehat{H}_T^2(L/K)$ . We now prove a bunch of properties of this map.

- **Injectivity:** Suppose two algebras share cohomology cycles. We can alter those by coboundaries to make them share the exact same chain. This defines their entire algebraic structure, so they are isomorphic.
- **Surjectivity:** Note that abstractly defining  $e_\sigma a = \sigma(a)e_\sigma, e_\sigma e_\tau = \phi(\sigma, \sigma\tau)e_{\sigma\tau}$  results in a ring  $A(\phi)$  over  $K$  with dimension  $n$  over  $L$ . Clearly the  $e_\sigma$  are invertible. Using standard reduction operations, we see that  $Z(A) = K$ , and that nontrivial two-sided ideals must contain some  $e_\sigma$ , which generates  $A$ . Thus we get that the map  $\text{Br}(L/K) \rightarrow \widehat{H}_T^2(L/K)$  is surjective.
- **A Homomorphism:** Consider  $(A(\phi) \otimes_K A(\phi'))^{\text{opp}}, A(\phi\phi')$ . These two algebras act on  $A(\phi) \otimes_L A(\phi')$ : The first by multiplication from the right, the second by  $le''_\sigma(a \otimes a') = l(e_\sigma a \otimes e'_\sigma b)$  (verify this is well defined). The actions commute, so we get a map  $(A(\phi) \otimes A(\phi'))^{\text{opp}} \otimes A(\phi\phi') \rightarrow \text{End}_K(A(\phi) \otimes_L A(\phi'))$ . The dimensions match, so from simplicity this is an isomorphism. Thus  $A(\phi) \otimes A(\phi') \cong_{\text{Br}} A(\phi\phi')$ .
- **Restriction:** Let  $E/L/K$  be a tower, then we should prove  $L \otimes_K A_{E/K}(\phi|_{G \times G}) \sim A_{E/L}(\phi|_{H \times H})$  in  $\text{Br}(L)$ . Consider  $A_{E/K}(\phi|_{G \times G})$ , viewed as an  $L$ -vector space of dimension  $\#G\#H$ . There is a right  $L$ -action of  $L \otimes_K A_{E/K}(\phi|_{G \times G})$  by  $L$  from the left and  $A_{E/K}(\phi|_{G \times G})$  from the right. There is an obvious left  $L$ -action of  $A_{E/L}(\phi|_{H \times H})$ . These actions commute (and are well defined) by virtue of  $H$  fixing  $L$ . Thus we have a nontrivial homomorphism  $(L \otimes_K A_{E/K}(\phi|_{G \times G}))^{\text{opp}} \otimes_L (A_{E/L}(\phi|_{H \times H})) \rightarrow \text{End}_L(A_{E/K}(\phi|_{G \times G}))$ . This is what we needed.

- Inflation: We should prove  $A_{L/K}(\phi_{G/H}) \sim A_{E/K}(\phi_G)$  in  $\text{Br}(K)$ . These have dimensions  $[G : H]^2, [G]^2$ . Consider  $E \otimes_L A_{L/K}(\phi_{G/H})$ , a  $K$ -vector space of dimension  $\#G\#G/H$ . It has a right action of  $A_{L/K}(\phi_{G/H})$  on the second part. It has a left action of  $A_{E/K}(\phi_G)$  by  $ae_\sigma(b \otimes e_\tau) \mapsto a\sigma(b) \otimes e_{\sigma\tau}$ . These commute, so we are done as before.

□

As corollary, there is a canonical isomorphism  $\text{Br}(K) \rightarrow H^2(\overline{K}/K)$ .

## 2.5 Relation to Local Class Field Theory

**Theorem 2.5.1.** *Let  $K$  be a local field and  $D$  a central division algebra over  $K$  of dimension  $n^2$ . Then  $D$  contains a copy of each extension  $L/K$  of degree  $n$ .*

*Proof.* Let  $L/K$  have degree  $n$ . Take  $\alpha \in \widehat{H}_T^2(L/K)$  that corresponds to  $D$  (which is possible as  $D$  has order  $n$  in the cohomology). Then there is a maximal subfield  $L' \subseteq D$  whose crossed homomorphism is equivalent to  $\alpha$  in  $LL'$ . Thus  $\bar{\phi}(\sigma, \sigma\tau) = \bar{\alpha}(\sigma, \sigma\tau) \cdot f(\sigma)f(\tau)f(\sigma\tau)^{-1}$  for  $\sigma, \tau \in \text{Gal}(LL'/K)$ . Let  $H = \text{Gal}(LL'/L)$  and  $K = \text{Gal}(LL'/L')$ . Then we see  $\bar{\phi}, \bar{\alpha}$  are trivial when restricted to both  $H, K$  and thus when restricted to  $HK = \text{Gal}(LL'/L \cap L')$  (this uses Hilbert 90, to equalize the trivializations over  $H \cap K$ ). This implies  $D$  splits over  $L \cap L'$ , which is impossible if it has dimension  $< n$ . Therefore,  $L = L'$  □

As a corollary,  $\text{Br}(K) = \text{Br}(K^{\text{un}}/K)$ .

**Lemma 2.5.2.** *Let  $D$  be as before. Then there is a unique extension  $v_D$  of the valuation  $v_K$  to  $D$ . It has values in  $\frac{1}{n}\mathbb{Z}$ .*

*Proof.* Let us reduce to the case  $D$  is a field. Think of  $D$  as acting on an  $n^2$ -dimensional  $K$ -vector space, and define  $v_D = \frac{1}{n^2}v_K(\det a)$ . This is clearly multiplicative. To show this is a valuation, we should take  $v_D(\alpha) \geq 0$  and prove that  $v_D(\alpha + 1) \geq 0$ . Let  $L = K(\alpha) \subseteq D$ . Then  $v_D|_L = v_L$ .

Let  $f$  be the minimal polynomial of  $\alpha$ . Then it is irreducible, and  $\det a$  is its free term, and  $\det(a + 1)$  is an integral combination of its coefficients. Thus, we should only show all its coefficients are integral. This fact follows from the strong form of Hensel's lemma (for factorization into factors that are coprime mod  $v$ ), using the irreducibility of  $f$ . Thus,  $v_D$  is a valuation.

For uniqueness, suppose we had another  $v'_D$ . Take some  $\alpha$  with  $v_D(\alpha) > 0$ . Then, writing its minimal polynomial, we see it has integral coefficients and free coefficient in the maximal ideal, implying that  $v'_D(\alpha) > 0$  as well. Similarly,  $v_D(\alpha) = 0$  implies  $v'_D(\alpha) = 0$ . Together with multiplicativity, we can deduce that  $v_D = v'_D$  □

**Theorem 2.5.3.** *Let  $D$  be as before. Then its invariant in  $\mathbb{Q}/\mathbb{Z}$  can be computed by taking  $L \subseteq D$  the unramified extension, with the Frobenius  $\sigma$ , and returning  $v_D(e_\sigma) \in \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ .*

*Proof.* Denote this map  $\text{inv}'$  and note that it is well defined as  $e_\sigma$  is defined up to conjugation and  $L^\times$  (which has integral valuation as it is unramified). Take the cocycle  $\phi(\sigma^i, \sigma^j) = \begin{cases} 1, i + j < n \\ \pi_K^l \text{ else} \end{cases}$ . Then  $\text{inv}'_K(A(\phi)) = v_D(e_\sigma) = \frac{1}{n}v_K(e_\sigma^n) = \frac{1}{n}v_K(\pi_K^l) = \frac{l}{n} = \text{inv}_K(\phi)$ . This shows that  $\text{inv}_K$  agrees with the standard invariant on  $K^{\text{un}}/K$ , and thus on  $\overline{K}/K$  □

## Chapter 3

# Chebotarev's Density Theorem

### 3.1 Chebotarev's Theorem

**Theorem 3.1.1.** *If  $f(s) = \sum \frac{a_n}{n^s}$ , and  $s(x) = \sum_{n=0}^x a_n = O(x^b)$ , then  $f$  converges uniformly on  $\operatorname{Re} s \geq b + \varepsilon$ ,  $|\arg(s - b)| \leq \frac{\pi}{4} - \varepsilon$ .*

*Proof.*

$$\begin{aligned}
\left| \sum_{n_1 \leq n \leq n_2} \frac{a_n}{n^s} \right| &= \left| \sum_{[n_1, n_2]} \frac{s(n)}{n^s} - \sum_{[n_1-1, n_2-1]} \frac{s(n)}{(n+1)^s} \right| = \left| \sum_{[n_1, n_2-1]} s(n) \left( \frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right| + O(n_1^{b-\operatorname{Re} s}) \\
&\leq \sum_{[n_1, n_2-1]} |s(n)| \cdot \left| \int_n^{n+1} st^{-s-1} dt \right| + O(n_1^{b-\operatorname{Re} s}) \\
&\leq \sum_{[n_1, n_2-1]} C \cdot \left| \int_n^{n+1} st^{b-s-1} dt \right| + O(n_1^{b-\operatorname{Re} s}) \\
&\leq C|s| \cdot \left[ \frac{t^{b-\operatorname{Re} s}}{\operatorname{Re} b - s} \right]_{n_2}^{n_1+1} + O(n_1^{b-\operatorname{Re} s}) \\
&\leq \left( \frac{|s|}{\operatorname{Re} s - b} + 1 \right) O(n_1^{b-\operatorname{Re} s})
\end{aligned}$$

and  $\frac{|s|}{\operatorname{Re} s - b}$  is  $O(1)$  in our region □

Let  $\chi$  be a Dirichlet character of a number field  $K$  of degree  $d$ , i.e. a homomorphism  $\chi : C_m \rightarrow S^1$  for some modulus  $m$ . Define  $L_K(s, \chi) = \sum_I \frac{\chi(I)}{\operatorname{Nm}(I)^s}$  in  $\operatorname{Re} s > 1$ ; Later we will see that it converges in  $\operatorname{Re} s > 1 - \frac{1}{d}$ . It also has the Euler product  $L_K(s, \chi) = \prod_{\mathfrak{p}} \frac{1}{1 - \chi(\mathfrak{p}) \operatorname{Nm}(\mathfrak{p})^{-s}}$ .

Let  $\zeta(s) = L_{\mathbb{Q}}(s, \chi_0)$ , and note that, for  $\zeta_2 = 1 - \frac{1}{2^s} + \frac{1}{3^s} - \dots$ , we have  $\zeta_2 = \zeta - \frac{2}{2^s}\zeta$ , so  $\zeta$  is meromorphic on  $\operatorname{Re} s > 0$  with only possible poles (of degree 1) on  $\frac{1}{\log 2} \tau i \mathbb{Z}$ . A similar argument for  $\zeta_3 = 1 + \frac{1}{2^s} - \frac{2}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} - \dots$  shows that really, the only pole is at 1. The residue is 1 as  $\int_1^\infty x^{-s} dx = \frac{1}{s-1}$ .

#### 3.1.1 Class Number Formula

**Theorem 3.1.2.** *Let  $K$  be a number field of degree  $n$ , let  $m$  be a modulus of  $K$  and let  $\mathfrak{k}$  be an ideal class in  $C_m$ . Let  $\zeta_K(s, \mathfrak{k}) = \sum_{\mathfrak{a} \in \mathfrak{k}} \frac{1}{\operatorname{Nm} \mathfrak{a}^s}$  (sum over the integral ideals of  $\mathfrak{k}$ ). Then  $\zeta_K(s, \mathfrak{k})$  is meromorphic on  $\operatorname{Re} s > 1 - \frac{1}{n}$  with a single simple pole at  $s = 1$  with residue  $g_m = \frac{2^r \tau^s \operatorname{reg}(m)}{w_m \operatorname{Nm}(m) \Delta_K^{\frac{1}{2}}}$ , where  $\operatorname{reg}(m)$  is the volume of the parallelopiped for  $U_{m,1} = U \cap K_{m,1}$ , and  $w_m$  is the number of roots of unity in  $K_{m,1}$ , and  $\operatorname{Nm}(m) = \operatorname{Nm}(m_0) 2^{r(m)}$ .*

*Proof.* Let  $S(x, \mathfrak{k}) = \#\{a \in \mathfrak{k} | a \text{ integral, } \operatorname{Nm} a \leq x\}$ . We will show that  $S(x, \mathfrak{k}) = g_m x + O(x^{1-\frac{1}{n}})$ . It would then follow that  $\zeta_K(s, \mathfrak{k}) - g_m \zeta(s)$  has a Dirichlet series with partial sums  $O(x^{1-\frac{1}{n}})$ , so it is holomorphic on  $\operatorname{Re} s > 1 - \frac{1}{n}$ , proving the theorem. We now get to compute  $S(x, \mathfrak{k})$ .

Choose some integral  $b \in \mathfrak{k}^{-1}$  (coprime to  $m$ ). Then  $S(x, \mathfrak{k})$  also counts the set of elements  $\xi \in K_m^\times$  that are in  $b$  and with norm  $\leq x \operatorname{Nm}(b)$ , up to multiplication by  $U$ . Now consider the embedding of  $K$  into  $\mathbb{R}^n$  via the real and complex embeddings. Then  $U$  acts on this space, and suppose we have some homogeneous domain  $D \subseteq \mathbb{R}^n$ , invariant under  $w$ , so that every orbit (of elements which are nonzero on every coordinate) intersects it exactly  $w$  times. Then we should count the size of the intersection

of the lattice  $b$  with the bounded domain  $D(x \text{Nm}(b)) = (x \text{Nm}(b))^{\frac{1}{n}} D(1)$  and divide by  $w$  to get the solutions  $\xi \in K^\times$ .

We can estimate the subset with  $\xi \equiv 1(m)$  by multiplying with  $\frac{[U:U_{m,1}]}{\text{Nm}(m)} = \frac{\text{reg}(U_{m,1})w}{\text{Nm}(m) \text{reg}(U)w_m}$ , which is the fraction of residues mod  $m$  that can be made into 1 mod  $m$  after multiplication with a unit. The error produced by this estimate is proportional to the boundary of  $D(1)$  relative to the interior, which is  $O(x^{1-\frac{1}{n}})$  (a reasonable assumption on  $D$  that we will soon justify). This reduced us to the case  $m = 1$ .

How to construct  $D$ ? let  $g : K^\times \rightarrow \mathbb{R}^n$  be the log map, projected onto the  $H = \{\sum = 0\}$  hyperplane such that  $g(\lambda a) = g(a)$  for  $\lambda \in \mathbb{Z}$ . Let  $F$  be a fundamental domain to the lattice of units in  $H$ , and let  $D \subseteq \mathbb{R}^n$  be the inverse image of the log-projection. This domain is  $w$ -invariant, but its points are not preserved by any other unit, and it is homogeneous.

I claim that given a bounded open symmetric set  $D \subseteq \mathbb{R}^n$ , and a lattice  $L \subseteq \mathbb{R}^n$ , so that the boundary of  $D$  can be covered by finitely many Lipchitz images of cubes, we have  $|L \cap tD| = \frac{\text{Vol}(D)}{\Delta_L} t^n + O(t^{n-1})$ . This is rather easy to prove, by considering the set of parallelopipeds covering and covered by the set  $tD$  (and changing perspective, to shrink the lattice rather than enlarge the shape). Note that we can estimate the amount of parallelopipeds each Lipchitz square hits.

The determinant of the lattice  $b$ , in our case, equals  $\sqrt{\Delta_K} \text{Nm}(b)$ . Thus our set has size  $\frac{\text{Vol}(D(1))}{\sqrt{\Delta_K}} x + O(x^{1-\frac{1}{n}})$ , and it is only left to compute  $\text{Vol}(D(1))$  (and to assure its boundary is covered by finitely many Lipchitz images of squares).

For this, use polar coordinates. Let  $N_i = 1$  for real embeddings and 2 for complex. Then  $D$  is described by  $\log \rho_j - \frac{1}{n} \log \prod_{i=1}^{r+s} \rho_i^{N_i} = \sum c_q \log |\sigma_j \eta_q|$ , where  $\eta_q$  are a basis to the units lattice, and with the requirement that  $0 \leq c_q \leq 1$ . When restricting to  $D(1)$ , we further require  $0 < \prod_{i=1}^{r+s} \rho_i^{N_i} \leq 1$ . If this space is denoted  $P$ , then  $\text{Vol}(D(1)) = 2^r \tau^s \int_P \rho_{r+1} \dots \rho_{r+s} d\rho_{r+1} \dots d\rho_{r+s}$ .

Now change coordinates into the  $c_q$ 's and  $u = \prod_{i=1}^{r+s} \rho_i^{N_i}$ . Then  $P$  is identified with the unit cube. Let us compute the Jacobian  $J = (\partial \rho_i / \partial u | c_q)$ : we have  $\rho_i = u^{\frac{1}{n}} \exp(\sum c_q \log |\sigma_j \eta_q|)$ , so  $\frac{\partial \rho_j}{\partial u} = \frac{1}{n} \frac{\rho_j}{u}$ ,

and  $\frac{\partial \rho_j}{\partial c_q} = \log |\sigma_j \eta_q| \rho_j$ . Hence the Jacobian determinant is  $\frac{\prod_{1 \leq j \leq r+s} \rho_j}{nu} \cdot \begin{vmatrix} 1 & \log |\sigma_1 \eta_1| & \dots \\ 1 & \log |\sigma_2 \eta_1| & \dots \\ \dots & & \\ 1 & \log |\sigma_{r+s} \eta_1| & \dots \end{vmatrix}$ , which

becomes  $= \frac{\text{reg}(K)}{\rho_{r+1} \dots \rho_{r+s}}$  after adding all the rows to the final one, with appropriate coefficients (of 1 and 2). This finishes the computation  $\square$

Let  $\chi$  be a character on  $C_m$  and let  $L_K(s, \chi) = \sum_I \frac{\chi(I)}{\text{Nm}(I)^s}$  be its  $L$ -function.

**Corollary 3.1.3.**  $L_K(s, \chi)$  is analytic for  $\text{Re } s > 1 - \frac{1}{n}$  and  $\chi \neq \chi_0$ .

*Proof.* We have  $L(s, \chi) = \sum_{\mathfrak{f} \in C_m} \chi(\mathfrak{f}) \zeta(s, \mathfrak{f})$ , which may only have a pole at 1, but its residue would then be  $g_m \cdot \sum_{C_m} \chi(\mathfrak{f}) = 0$ , impossible  $\square$

### 3.1.2 Dirichlet Density

Let  $K$  be a number field and  $T$  a subset of its primes. If  $\sum_{\mathfrak{p} \in T} \frac{1}{\text{Nm}(\mathfrak{p})^s} - \frac{\delta}{s-1}$  is holomorphic around 1, we say  $T$  has Dirichlet density  $\delta$ .

Two densities generalized by the Dirichlet density:

1. Let  $\zeta_T(s) = \prod_{\mathfrak{p} \in T} \frac{1}{1 - \text{Nm}(\mathfrak{p})^{-s}}$ . If  $\zeta_T^m$  has a pole of degree  $n$  at 1, we say  $T$  has polar density  $\frac{n}{m}$ . This is a special case of Dirichlet, because  $\log \zeta_T(s) = \sum_{\mathfrak{p} \in T} \sum_{m \geq 1} \frac{1}{m \text{Nm}(\mathfrak{p})^{sm}}$ , and the part with  $m > 1$  converges absolutely around  $s = 1$  (indeed, we can bound  $\sum_{\mathfrak{p}, m \geq 2} \frac{1}{2 \text{Nm}(\mathfrak{p})^{sm}} \leq \sum_{\mathfrak{p}} \frac{1}{\text{Nm}(\mathfrak{p})^2}$ ).

2. The natural density is the limit of the uniform density on primes up to a value.

**Theorem 3.1.4.** *The natural density is a special case of Dirichlet.*

*Proof.* Let  $M(x) = \{\mathfrak{p} : \mathfrak{p} \in M, \text{Nm}(\mathfrak{p}) < x\}$ . Then

$$\sum_{\mathfrak{p} \in M(x)} \frac{1}{\text{Nm}(\mathfrak{p})^s} = \frac{M(x)}{x^s} + s \int_1^x \frac{M(t)}{t^{s+1}} dt$$

If the natural density exists and equals  $R$ , then  $M(x) \sim \frac{Rx}{\log x}$  by the prime number theorem (which also works for number fields). Thus

$$\delta(M) = \lim_{s \rightarrow 1^+} \frac{\lim_{x \rightarrow \infty} \frac{M(x)}{x^s} + s \int_1^x \frac{M(t)}{t^{s+1}} dt}{-\log(s-1)} = \lim_{s \rightarrow 1^+} \frac{s \int_1^\infty \frac{M(t)}{t^{s+1}} dt}{-\log(s-1)}$$

Which, by L'hospital, using  $(\frac{s}{t^{s+1}})' = \frac{1-s \log t}{t^{s+1}}$ , equals  $\lim_{s \rightarrow 1^+} (1-s) \int_1^\infty \frac{M(t) \cdot (1-s \log t)}{t^{s+1}} dt$ . The dominant term is  $\lim_{s \rightarrow 1^+} (s-1) \int_1^\infty \frac{\log t M(t)}{t^{s+1}} dt \sim \lim_{s \rightarrow 1^+} (s-1) \int_1^\infty \frac{R}{t^s} = R$   $\square$

Density is additive on disjoint sets. Clearly, all density is located at the split primes of  $K/\mathbb{Q}$ , and given an extension  $L/K$ , the set of primes that split in  $L$  has density  $\frac{1}{[L:K]}$  (for this part assume wlog that  $L/K$  is Galois).

As a cute corollary, if  $f \in K[x]$  splits mod all but finitely many primes, then it splits. Also, the set of primes splitting in  $L$  determines  $L$ . As another corollary, the Frobenius elements generate the Galois (as their fixed field  $L^H$  splits all but finitely many primes). As another corollary, if  $\mu_n \subseteq K$ , then an element which is an  $n$ th power almost everywhere, is an  $n$ th power.

## 3.2 The $L$ -values at 1

Let  $m$  be a modulus and consider the collection of all characters on  $C_{K,m}$ . We have

$$\sum_{\chi} \log L(s, \chi) \sim \sum_{\chi, \mathfrak{p}} \frac{\chi(\mathfrak{p})}{\text{Nm}(\mathfrak{p})^s} = |C_{K,m}| \sum \frac{1}{\text{Nm}(\mathfrak{p})^s}$$

Where the final sum is on primes that vanish in  $C_m$ . But when  $s \rightarrow 1^+$  this is just  $\frac{1}{s-1}$  times the Dirichlet density of the norms from the ray class field  $L_m/K$ , which is concentrated on the split primes, and thus equals  $\frac{1}{[C_{K,m}]}$ . Thus  $\sum_{\chi} \log L(s, \chi) \sim \frac{1}{s-1}$  around  $s = 1$ .

**Corollary 3.2.1.**  $L(1, \chi) \neq 0$ .

*Proof.* In the sum  $\sum_{\chi} \log L(s, \chi)$  there must be exactly one pole of residue 1 and it comes from  $\chi = \chi_0$   $\square$

In fact, even without using class field theory, we could deduce from here that there is at most one  $\chi$  such that  $L(1, \chi) = 0$ . This can also be used to prove the second inequality for abelian extensions.

**Theorem 3.2.2.** *If  $\mathfrak{k}$  is a class of  $C_{K,m}$ , then  $\delta(\mathfrak{k}) = \frac{1}{\#C_m}$ .*

*Proof.* We have  $\sum_{\chi} \chi(\mathfrak{k})^{-1} \log L(s, \chi) = |C_{K,m}| \cdot \sum_{\mathfrak{p} \in \mathfrak{k}} \frac{1}{\text{Nm}(\mathfrak{p})^s} \sim |C_{K,m}| \cdot \delta(\mathfrak{k}) \cdot \frac{1}{s-1}$ . But we know that the only interesting term from the left comes from  $\chi = \chi_0$   $\square$

### 3.3 Chebotarev

**Theorem 3.3.1** (Chebotarev). *Let  $L/K$  be an extension of number fields and  $C \subseteq G = \text{Gal}(L/K)$  a conjugacy class. Then the Dirichlet density of primes  $\mathfrak{p}$  with  $(\mathfrak{p}, L/K) \subseteq C$  is  $\frac{\#C}{\#G}$ .*

*Proof.* For the abelian case, we note that every abelian extension is contained in a ray class field, and for those we just proved the statement. So now let  $L/K$  be a general extension. Wlog  $C = \sigma^G$  for  $\sigma \in G$  of order  $f$ . Let  $M = L^\sigma$ , then  $L/M$  is cyclic of order  $f$ . Let  $T_L$  be the set of primes of  $L$  whose Frobenius in  $L/M$  is  $\sigma$ , let  $T_M$  be the set of primes in  $M$  whose Frobenius in  $L/M$  is  $\sigma$  and are split over  $K$ , and let  $T_K$  be the set whose density we seek. Then  $\delta(T_M) = \frac{1}{f}$  by the abelian Chebotarev. We always assume the primes are unramified from now.

The map  $T_L \rightarrow T_M$  is defined because, for  $\mathfrak{p}_L$ , we know the Galois of  $L_{\mathfrak{p}}/K_{\mathfrak{p}}$  is generated by  $\sigma$ , which fixes  $M_{\mathfrak{p}}$ , so  $M_{\mathfrak{p}} = K_{\mathfrak{p}}$  i.e. the image is in  $T_M$ . This map is injective as  $f(\mathfrak{p}_L/\mathfrak{p}_M) = f$  so that  $\mathfrak{p}_L$  is the only prime over  $\mathfrak{p}_M$ . It is surjective as, for every  $\mathfrak{p}_L/\mathfrak{p}_M \in T_M$  we have  $(\mathfrak{p}_L, L/K) = (\mathfrak{p}_L, L/K)^{f(\mathfrak{p}_M/\mathfrak{p}_K)} = (\mathfrak{p}_L, L/M) = \sigma$ . So it is a bijection.

The map  $T_L \rightarrow T_K$  is obviously defined. It is surjective as for every  $\mathfrak{p}_L/\mathfrak{p}_K \in T_K$  we have  $(\mathfrak{p}_L, L/K) \in \sigma^G$ , so there is some lift for  $\mathfrak{p}_K$  which lands on  $\sigma$ . The amount of such  $\mathfrak{p}_L$  is  $C_G(\sigma)/G(\mathfrak{p}_L) = \frac{n}{cf}$ .

From here, we deduce the theorem by

$$f_{T_K}(s) = \sum_{\mathfrak{p}_K \in T_K} \frac{1}{\text{Nm}(\mathfrak{p}_K)^s} = \frac{n}{cf} \sum_{\mathfrak{p}_M \in T_M} \frac{1}{\text{Nm}(\mathfrak{p}_M)^s} \sim \frac{n}{cf} \cdot \frac{1}{f(s-1)}$$

□

## Chapter 4

# Global Class Field Theory

## 4.1 Statements of Global Class Field

### 4.1.1 Definitions

Given a collection of locally compact spaces with an open compact subspace,  $(K_i, \mathcal{O}_i)$ , we can define their restricted product  $\prod' K_i$  as the direct limit of the product spaces  $U_I = \prod_{i \in I} K_i \times \prod_{i \notin I} \mathcal{O}_i$ , for  $I$  finite. As a set, this consists of the elements of the product that are in  $\mathcal{O}_i$  almost always. Note that the restricted product is locally compact (in contrast to  $\prod K_i$ ), because the  $U_I \subseteq \prod' K_i$  are open.

We define the ideles as  $\mathbb{I}_K = \prod'_v (K_v^\times, \mathcal{O}_v^\times)$ , and the Adeles as  $\mathbb{A}_K = \prod'_v (K_v, \mathcal{O}_v)$ , for a number field  $K$ . Those are locally compact groups. Facts:

- There is a map  $\mathbb{I}_K \rightarrow \mathbb{A}_K$ , but inversion isn't continuous on the image, so it isn't an embedding.
- For every prime  $v$  of  $K$ , there is an embedding  $K_v^\times \subseteq \mathbb{I}_K$ .
- There is a short exact sequence  $0 \rightarrow \prod_P \mathcal{O}_P^\times \times (\mathbb{R}^\times)^r \times (\mathbb{C}^\times)^s \rightarrow \mathbb{I}_K \rightarrow I_K \rightarrow 0$ .
- $\mathbb{I}_K$  contains  $K^\times$  as a discrete subgroup. Indeed, suppose  $1 \neq a_n \in K^\times$ . Then eventually they live in the same  $U_I$ , so we may assume  $a_n \in \mathcal{O}_K$  and that they are close to 1 in the infinite places. But this is impossible by the product formula for  $a - 1$ .

The quotient  $\mathbf{C}_K = \mathbb{I}_K / K^\times$  is called the Idele class group.

The idele class group has a norm map into  $\mathbb{R}^+$ , whose kernel is compact. Indeed, using  $K^\times$  we can reduce into the direct products of units (up to a finite set of possibilities on the primes, coming from representatives of the class group), and using the units we can reduce the real and complex parts to 1.

Given an extension  $L|K$ , a prime  $v$  of  $K$  and a prime  $w$  of  $L$  lying over  $v$ , we get the local Artin map  $\phi_v : K_v^\times \rightarrow D(w) = \text{Gal}(L_w/K_v) \subseteq \text{Gal}(L|K)$ . Consider this map with respect to some other  $w' = \sigma w$ ; Then we get local Artin  $K_v^\times \rightarrow \text{Gal}(L_w|K_v), \text{Gal}(L_{w'}|K_v)$ . The  $K$ -isomorphism  $L \xrightarrow{\sigma} L$  becomes a  $K_v$ -isomorphism  $L_w \xrightarrow{\sigma} L_{w'}$  whose effect in  $\text{Gal}(L/K)$  is conjugation by  $\sigma$ . However, we assumed  $L/K$  is abelian, so this conjugation is trivial, and we conclude that  $\phi_v : K_v^\times \rightarrow \text{Gal}(L/K)$  is well defined.

Now, we can define  $\phi_{L/K} : \mathbb{I}_K \rightarrow \text{Gal}(L|K)$  by  $\phi_{L/K}(a) = \prod_v \phi_v(a_v)$ . This is the unique character on  $\mathbb{I}$  acting as  $\phi_v$  on the individual  $K_v$ 's. It is well defined because  $L_w|K_v$  is generally unramified and  $a_v$  is generally a unit. Note that  $\phi_{L/K}$  is continuous (from the continuity of  $\phi_v$ , which follows from  $\text{Nm}(L_w)$  being open).

Those glue to the global  $\phi_K : \mathbb{I}_K \rightarrow \text{Gal}(K^{\text{ab}}/K)$ .

### 4.1.2 Theorems

**Theorem 4.1.1** (Reciprocity Law). *Let  $K$  be a number field. Then  $\phi_K$  factors through the Idele Class Group, meaning it vanishes on principal ideles; and for every finite abelian  $L|K$ , the norm group  $\text{Nm } \mathbf{C}_L$  is open of finite index in  $\mathbf{C}_K$ , and  $\phi_{L/K}$  induces an isomorphism  $\mathbf{C}_K / \text{Nm } \mathbf{C}_L \cong \text{Gal}(L|K)$ .*

**Theorem 4.1.2** (Existence). *Every open  $N \subseteq \mathbf{C}_K$  of finite index is a norm group from a unique abelian extension.*

It follows there is a bijection between the finite abelian extensions of  $K$  and the open finite-index subgroups of  $\mathbf{C}_K$ .

**Claim 4.1.3.** *The norm groups are open of finite index in  $\mathbf{C}_K$ .*

*Proof.* Suppose we have a norm element. Give it a representative in some  $U_I$  which is close to 1 in all infinite and ramified primes. Then anything close to this representative, which is in the same  $U_I$ , is a norm on the infinite, and ramified, and  $I$  primes (as norm groups for local fields are open) and also on the unramified primes outside  $I$  (as units are norms). This proves openness; A similar argument, together with finiteness of the class group, shows finite-index  $\square$

## 4.2 Proofs

### 4.2.1 Idele Cohomologies

Let  $L|K$  be a finite Galois extension of number fields. Let  $n = [L : K]$ ,  $n_v = [L_w : K_v]$  for any  $w|v$ .

We may think of  $\mathbf{C}_L$  as a  $G = \text{Gal}(L|K)$ -module. Recall, by the Tate theorem, that if  $\hat{H}_T^1(G, \mathbf{C}_L) = 0$ , and  $\hat{H}_T^2(G, \mathbf{C}_L)$  are cyclic of order  $[L : K]$ , for all abelian  $L|K$ , with a natural choice for generators  $u_{L|K}$  that restrict to one another, then  $\hat{H}_T^*(G, \mathbb{Z}) \cong \hat{H}_T^{*+2}(G, \mathbf{C}_L)$  defined by product with the unit, which for  $* = -2$  gives the desired result.

Consider  $L \otimes_K K_v \cong \prod_{w|v} L_w$ . This is a  $G$ -module, where on the left viewpoint the action is on  $L$ , and on the right viewpoint the action is by  $(\alpha_w) \mapsto (\sigma \alpha_{\sigma^{-1}w})$ . We get a similar action on  $\prod_{w|v} L_w^\times$ .

It now follows that  $\prod_{w|v} L_w^\times \cong \text{Ind}_{G_{w_0}}^G L_{w_0}^\times$ , and so  $H^*(G, \prod_{w|v} L_w^\times) \cong H^*(G_{w_0}, L_{w_0}^\times)$  by Shapiro. We see that for  $w|v$ , the  $G_w, L_w, U_w$  are defined up to a non-canonical isomorphism (because it is unclear whether to conjugate by  $G_w$ ), but their cohomologies are defined up to a canonical isomorphism. Thus, when writing their cohomologies, we allow ourselves to denote them  $G^v, L^v, U^v$  without specifying the  $w$ .

**Theorem 4.2.1.**  $\hat{H}_T^*(G, \mathbb{I}_L) \cong \bigoplus_v \hat{H}_T^*(G^v, L^{v \times})$

*Proof.* Consider now the  $G$ -action on  $\mathbb{I}_L$  induced by the  $\prod_{w|v} L_w^\times$ s. Clearly  $\mathbb{I}_L^G \cong \mathbb{I}_K$ , so we have a norm map  $\mathbb{I}_L \rightarrow \mathbb{I}_K$ . Also, for a finite set  $S$ , the sets  $\mathbb{I}_{L,S} = \prod_{v \in S} \prod_{w|v} L_w^\times \times \prod_{v \notin S} \prod_{w|v} U_w$  are open  $G$ -stable subsets that cover  $\mathbb{I}_L$ . Thus  $\hat{H}_T^*(G, \mathbb{I}_L) \cong \lim_S \hat{H}_T^*(G, \mathbb{I}_{L,S}) \cong \bigoplus_v \hat{H}_T^*(G^v, L^{v \times})$  (as  $U_w$  are cohomologically free for  $w|v$  unramified, and we assume  $S$  contains all ramifications)  $\square$

In particular,  $\hat{H}_T^1(G, \mathbb{I}_L) = 0$ , and  $\hat{H}_T^2(G, \mathbb{I}_L)$  is a direct sum of cyclic groups.

There is a map  $\text{Nm} : \prod_{w|v} L_w^\times \rightarrow K_v^\times$  defined by taking norm on each component and multiplying. As any two  $L_w$ s are  $K_v$ -isomorphic, the image of this map is the image of any single  $L_w^\times$ , and we denote it  $\text{Nm } L^{v \times}$ .

**Theorem 4.2.2.**  $\text{Nm}(\mathbb{I}_L)$  is an open subgroup of  $\mathbb{I}_K$ .

*Proof.* If  $S$  contains the infinite primes and the ramified primes of  $L/K$ , and  $T$  is the lift of  $S$  to  $L$ , then  $\text{Nm}(\mathbb{I}_{L,T}) = \prod_{v \in S} V_v \times \prod_{v \notin S} U_v^\times$ , for some open  $V_v \subseteq K_v^\times$   $\square$

If  $S$  is a finite set of primes of  $K$ , we can consider  $U(S)$ , the set of  $S$ -units, whose valuation vanishes in primes outside  $S$ . For example, the usual units correspond to the infinite primes. Then an extension to Dirichlet's unit theorem says  $U(S) \cong \mathbb{Z}^{s-1} \times U(S)_{\text{tor}}$ .

**Theorem 4.2.3.** If  $G$  is cyclic,  $S$  is a set of primes in  $K$  containing ramifications and infinites, and  $T$  is its lift, then  $h(U(T)) = \frac{1}{n} \prod_{v \in S} n_v$ .

*Proof.* Consider  $\text{Hom}(T, \mathbb{R})$ . This is a real vector space. It contains the  $G$ -lattice  $\text{Hom}(T, \mathbb{Z})$  and the  $G$ -lattice which is the image of  $f : U(T) \rightarrow \text{Hom}(T, \mathbb{R})$ , where  $f(u) = (\log |u|_w)$ , direct sum with an invariant  $(1, \dots, 1)$ . (It being a lattice follows from the unit theorem). Call these lattices  $M, N$ . Then

$M \otimes \mathbb{R} \cong N \otimes \mathbb{R}$  as  $G$ -modules, but this is a statement about the solvability of a linear system of equations over  $\mathbb{Q}$ , and thus  $M \otimes \mathbb{Q} \cong N \otimes \mathbb{Q}$  and we will think of them in the same  $\mathbb{Q}^n$ . But then finite-index manipulations show  $h(M) = h(N)$ .

Finally,  $h(M) = h(G, \bigoplus_{v \in S} \text{Ind}_{G^v}^G \mathbb{Z}) \cong \prod_{v \in S} h(G^v, \mathbb{Z}) = \prod_v n_v$ , and  $h(N) = n \cdot h(\text{im}(f)) = n \cdot h(U(T))$   $\square$

### 4.2.2 First Inequality for Cyclic Extensions

From Hilbert 90 and the long exact sequence, we know that  $\mathbf{C}_L^G = \mathbf{C}_K$ . Clearly,  $\mathbb{I}_K = K^\times \mathbb{I}_S$  for  $S$  a finite set of primes generating  $C_K$ .

**Theorem 4.2.4.** *If  $G$  is cyclic,  $h(\mathbf{C}_L) = n$*

*Proof.* Choose  $S$  large enough (with infinites, ramifications, whose lifts generate  $C_L$ ). Let  $T$  be its lift. Then  $\mathbf{C}_L = \mathbb{I}_T / (\mathbb{I}_T \cap K^\times) = \mathbb{I}_T / U(T)$ .

This implies the first inequality for cyclic extensions:  $\#\hat{H}_T^0(\mathbf{C}_L) \geq n$ .

As a corollary, for cyclic (thus solvable) extensions, there are infinitely many primes that do not split. Indeed, the norm subgroup contains the subgroup with 1 on all nonsplit primes, which together with  $K^\times$  approximates everything by CRT. From here it follows that Frobenius elements generate  $G$ , even if we take out a finite amount of them.

### 4.2.3 Second Inequality

We begin with two lemmas. The second is technical but useful.

**Lemma 4.2.5.** *If  $K$  is a local field, then  $(K^\times : K^{\times n}) = n \cdot \frac{|\mu_n|}{|n|_v}$ .*

*Proof.* For  $K$  Archimedean this is trivial. Otherwise,  $(K^\times : K^{\times n}) = n \cdot (U : U^n)$ . Since the logarithm identifies finite-index subgroups of  $U_K, \mathcal{O}_K$ , we see that  $h(U_K) = h(\mathcal{O}_K)$ , viewing both as trivial  $\mathbb{Z}/n$ -modules. But this gives us  $\frac{(U : U^n)}{|\mu_n|} = \frac{1}{|n|_v}$   $\square$

**Lemma 4.2.6.** *Let  $p$  be a rational prime. Let  $S, T$  be disjoint sets of primes in a number field  $K$ . Let  $E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \in T} K_v^\times \times \prod_{v \notin S \cup T} U_v^\times$ . Assume that:*

- $S$  contains the infinites and the components of  $p$ .
- $S \cup T$  generates  $C_K$ .
- $K^\times \cap E = U(S \cup T)^p$ .

*Then  $(\mathbb{I}_K : K^\times E) = p^{s+t}$ , where  $s = |S|, t = |T|$ .*

*Proof.* We have  $(\mathbb{I}_K : K^\times E) = (K^\times \mathbb{I}_{S \cup T} : K^\times E) = \frac{(\mathbb{I}_{S \cup T} : E)}{(K^\times \cap \mathbb{I}_{S \cup T} : K^\times \cap E)} = \frac{(\mathbb{I}_{S \cup T} : E)}{(U(S \cup T) : K^\times \cap E)}$ . By the previous lemma, the numerator equals  $\prod_{v \in S} p \frac{|\mu_p|}{|p|_v} = \frac{p^{2s}}{\prod_v |p|_v} = p^{2s}$ . By the third assumption, the denominator equals  $(U(S \cup T) : U(S \cup T)^p)$ , which is  $p^{s+t}$  because of the unit theorem  $\square$

Now we get to proving the second inequality. Together with it, we prove more things on the Galois cohomologies of idele class groups.

**Theorem 4.2.7.** *Let  $L/K$  be a Galois extension of number fields, with Galois group  $G$ . Then we have  $\#\hat{H}_T^0(G, \mathbf{C}_L), \#\hat{H}_T^2(G, \mathbf{C}_L) | n$  and  $\hat{H}_T^1(G, \mathbf{C}_L) = 0$ .*

*Proof.* We prove this by a sequence of reductions.

1. Reduction to  $G$  a  $p$ -group: Recall  $\text{Res} : \hat{H}_T^*(G, M) \rightarrow \hat{H}_T^*(P, M)$  for  $P$  a  $p$ -syllow subgroup is injective on the  $p$ -part.
2. Reduction to  $G$  cyclic of prime order  $p$ : For  $H^1$ , by the spectral sequence we have an exact sequence  $0 \rightarrow H^1(G/H, M^H) \rightarrow H^1(G, M) \rightarrow H^1(H, M)$ . By using the  $H^1$  case we get another exact sequence  $0 \rightarrow H^2(G/H, M^H) \rightarrow H^2(G, M) \rightarrow H^2(H, M)$ , reducing also the  $H^2$  statement. For  $H^0$ , note that  $(\mathbf{C}_K : \text{Nm } \mathbf{C}_L) | (\mathbf{C}_K : \text{Nm } \mathbf{C}_E)(\mathbf{C}_E : \text{Nm } \mathbf{C}_L)$ .
3. Reduction to the  $H^0$  statement: Recall that  $h(\mathbf{C}_L) = n$ .
4. Reduction to the case  $\zeta_p \in K$ : Upon replacing  $L|K$  by  $L(\zeta_p)|K(\zeta_p)$ , We see that the composition  $\mathbf{C}_K / \text{Nm } \mathbf{C}_L \rightarrow \mathbf{C}_{K(\zeta)} / \text{Nm } \mathbf{C}_{L(\zeta)} \xrightarrow{\text{Nm}} \mathbf{C}_K / \text{Nm } \mathbf{C}_L$  is multiplication by  $m = [K(\zeta_p)|K]$  which is coprime to  $p$ , thus an isomorphism (as  $p$ -powers are norms). Thus the second Nm map is a surjection, affirming the reduction.

We will now prove the second inequality on  $H^0$  for  $\zeta \in K$  and  $L = K \left( a_1^{\frac{1}{p}}, \dots, a_r^{\frac{1}{p}} \right)$  (although the reduction led us to  $r = 1$ ). Let  $S$  be a set of  $K$ -primes containing the infinites, the primes over  $p$  and  $a_i$  (i.e. the ramifications), and generators for  $C_K$ . Then (by the unit theorem)  $U(S) \cong \mathbb{Z}^{s-1} \times U(S)_{\text{tor}}$ , so  $U(S)/p \cong (\mathbb{Z}/p)^s$ . Let  $M = K(U(S)^{\frac{1}{p}})$ .

Let  $T'$  be a set of  $M$ -primes, none of which cover a primes of  $S$ , whose Frobenius elements over  $L$  form an  $\mathbb{F}_p$ -basis for  $\text{Gal}(M|L)$ . Note that their Frobenius over  $K$  is equal to their Frobenius over  $L$ , as each prime must totally split in at least one of  $M|L, L|K$ . Let  $T$  be the set of  $K$ -primes below  $T'$ . Note that  $r + t = s$ .

It then follows that an  $S$ -unit which is a  $p$ -power in  $K_v$  for all  $v \in T$ , is actually a  $p$ -power in  $L$  (and vice versa): Indeed,  $a$  is a  $p$ -power iff  $a^{\frac{1}{p}} \in U(S)$  iff  $a^{\frac{1}{p}}$  is preserved by the  $T$ -Frobenius iff  $a^{\frac{1}{p}} \in K_v$  for all  $v \in T$ .

Let  $E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \in T} K_v^{\times} \times \prod_{v \notin S \cup T} U_v^{\times}$ . This consists of norms, because  $K_v^{\times} / \text{Nm } L_w^{\times}$  are  $p$ -torsion groups by local class field,  $L_w = K_v$  for  $v \in T$ , and all units are norms.

Now  $(\mathbf{C}_K : \text{Nm } \mathbf{C}_L) = (\mathbb{I}_K : K^{\times} \text{Nm } \mathbb{I}_L)$ , so it suffices to show  $(\mathbb{I}_K : K^{\times} E) | p^r$ . We will deduce this from the technical lemma once we will show that  $E \cap K^{\times} = U(S \cup T)^p$ , so this is our goal now.

Let  $b \in K^{\times}$  be an  $S \cup T$ -unit, which is a  $p$ th power over any  $K_v$  for  $v \in S$ . We should show it is a  $p$ th power.

Note that, by what we have shown before, the kernel of  $U(S) \rightarrow \prod_{v \in T} U_v^{\times} / U_v^{\times p}$  is  $U(S) \cap L^{\times p}$ , which has index  $[M : L] = p^t = \prod_{v \in T} (U_v^{\times} : U_v^{\times p})$  by Kummer. Thus the map is surjective.

Let  $K' = K(b^{\frac{1}{p}})$ . It suffices to show  $K' = K$ , so assume otherwise. Consider  $D = \prod_{v \in S} K_v^{\times} \times \prod_{v \in T} U_v^{\times p} \times \prod_{v \notin S \cup T} U_v^{\times}$ . It comes from  $K'$ -norms: over  $S$  the  $b^{\frac{1}{p}}$  adds nothing, over  $T$  the  $p$ -powers are norms by local class field again, and elsewhere the extension is unramified so all units are norms. Thus  $(\mathbb{I}_K : K^{\times} D) \geq p$  by the first inequality for cyclic extensions. But  $\mathbb{I}_K = \mathbb{I}_S K^{\times}$ , and we know that  $U(S) \rightarrow \mathbb{I}_S / D$  is surjective, so  $\mathbb{I}_K = \mathbb{I}_S K^{\times} = D U(S) K^{\times} = D K^{\times}$ , contradicting the last inequality and completing the proof  $\square$

#### 4.2.4 Reciprocity

This section is analogous to how we bootstrapped local class field from unramified extensions. This time, we will bootstrap from cyclic cyclotomic extensions.

Choose a maximal cyclic cyclotomic extension of  $\mathbb{Q}$  and denote it by  $\mathbb{Q}^c$  (the choice comes from annoying things at 2). From now, we say that an extension  $L/K$  is cyclic cyclotomic if  $L \subseteq K\mathbb{Q}^c$ .

**Theorem 4.2.8.** *If  $L/K$  is cyclic cyclotomic, then  $\phi_{L/K}|_{K^\times} = 1$ .*

*Proof.* We know that  $\phi_{K\mathbb{Q}(\zeta)/K} = \phi_{\mathbb{Q}(\zeta)/\mathbb{Q}} \circ \text{Nm}_{\mathbb{Q}}^K$ , so wlog  $K = \mathbb{Q}$  and  $L = \mathbb{Q}(\zeta_n)$ . Also,  $\phi_{EL/K} = \phi_{E/K} \times \phi_{L/K}$ , so wlog  $n = l^r$  is a prime power. Now, we just need to recall how the local Artin works:  $\phi_\infty(a) = [\text{sgn}(a)]$ ,  $\phi_p(up^s) = [p^s]$ , and  $\phi_l(ul^s) = [u^{-1}]$ . This finishes the proof  $\square$

**Corollary 4.2.9.** *If  $L/K$  is cyclic cyclotomic, and  $\alpha \in H^2(L/K)$ , then  $\sum \text{inv}(\alpha_v) = 0$ .*

*Proof.* Consider the diagram

$$\begin{array}{ccccc} K^\times & \longrightarrow & \mathbb{I}_K & \xrightarrow{\phi_{L/K}} & G^{\text{ab}} \\ \downarrow \cup \delta_\chi & & \downarrow \cup \delta_\chi & & \downarrow \chi \\ H^2(L/K) & \longrightarrow & H^2(G, \mathbb{I}_L) & \xrightarrow{\sum \text{inv}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

where the right square commutes by the local statement of  $\chi(\phi_K(a)) = \text{inv}(\chi \cup a)$ . by cyclicity, the left vertical map is an isomorphism. Then we finish as the top composition was just shown to vanish  $\square$

**Theorem 4.2.10.** *Suppose  $L/K$  is a cyclic cyclotomic extension of number fields. Then  $H^2(G, \mathbf{C}_L)$  is canonically isomorphic to  $\mathbb{Q}/\mathbb{Z}[n]$ .*

*Proof.* We have an exact sequence  $0 \rightarrow H^2(L/K) \rightarrow \bigoplus_v H^2(L^v/K_v) \rightarrow H^2(G, \mathbf{C}_L) \rightarrow 0$ . Note that  $n = \text{lcm}(n_v)$  (from the Frobenius elements generating the Galois). As the middle map is a direct sum of  $\mathbb{Z}/n_v$  for  $\text{gcd}(n_v) = n$ , and from the second inequality  $\#H^2(G, \mathbf{C}_L) \leq n$ , it follows that  $H^2(G, \mathbf{C}_L) \cong \mathbb{Q}/\mathbb{Z}[n]$   $\square$

We denote this isomorphism by  $\text{inv} : H^2(G, \mathbf{C}_L) \rightarrow \mathbb{Q}/\mathbb{Z}[n]$ . Then from the local statements it follows that it commutes with inflation (in a cyclic cyclotomic tower), and finally that it glues to the absolute map  $\text{inv} : H^2(G_{K\mathbb{Q}^c/K}, \mathbf{C}_{K\mathbb{Q}^c}) \rightarrow \mathbb{Q}/\mathbb{Z}$ . Also, the restriction acts by multiplication by the index, and the corestriction acts as the identity.

**Theorem 4.2.11.** *The inflation map  $\text{inv} : H^2(G_{K\mathbb{Q}^c/K}, \mathbf{C}_{K\mathbb{Q}^c}) \rightarrow H^2(G_K, \mathbf{C}_{\overline{K}})$  is an isomorphism, so there is an absolute canonical isomorphism  $\text{inv} : H^2(G_K, \mathbf{C}_{\overline{K}}) \rightarrow \mathbb{Q}/\mathbb{Z}$ . This is independent from the choice of  $\mathbb{Q}^c$ .*

*Proof.* Consider the diagram

$$\begin{array}{ccccc} C_n & \longrightarrow & H^2(\mathbf{C}_{K\mathbb{Q}^c}) & \xrightarrow{\text{Res}} & H^2(\mathbf{C}_{L\mathbb{Q}^c}) \\ \downarrow & & \downarrow \text{Inf} & & \downarrow \text{Inf} \\ H^2(\mathbf{C}_{L/K}) & \longrightarrow & H^2(\mathbf{C}_{\overline{K}}) & \xrightarrow{\text{Res}} & H^2(\mathbf{C}_{\overline{L}}) \end{array}$$

Then the second inequality (for a general extension this time), together with injectivity of the inflation (that follows from  $H^1(\mathbf{C}_L) = 0$ ) tells us the left vertical map is an isomorphism. As  $H^2(\mathbf{C}_{\overline{K}})$  is glued from all  $H^2(\mathbf{C}_{L/K})$ , this proves the claim. For independence from the choice of  $\mathbb{Q}^c$ , note that we just showed the map  $\bigoplus H^2(L^v/K_v) \rightarrow H^2(\mathbf{C}_{\overline{K}})$  is surjective, and the  $\text{inv}$  can be obtained by lifting an element by it and summing its components  $\square$

**Corollary 4.2.12.** *There is an exact sequence  $0 \rightarrow \text{Br}(K) \rightarrow \bigoplus \text{Br}(K_v) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$ .*

**Corollary 4.2.13.** *There is an exact square*

$$\begin{array}{ccc}
H^2(G_{L/K}, I_L) & \longrightarrow & \bigoplus_{\mathfrak{p}} H^2(G_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}, L_{\mathfrak{p}}^{\otimes \infty}) \xrightarrow{\text{inv}_{\mathfrak{p}}} \bigoplus_{\mathfrak{p}} \mathbb{Q}/\mathbb{Z} \\
\downarrow & & \downarrow \Sigma \\
H^2(G_{L/K}, \mathbf{C}_L) & \xrightarrow{\text{inv}} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

*Proof.* It suffices to show this for  $L/K$  cyclic cyclotomic, for which this is the definition  $\square$

**Theorem 4.2.14** (reciprocity). *The map  $\phi_K$  vanishes on principal ideles.*

*Proof.* Recall the diagram where we proved  $\sum \text{inv} = 0$  for cyclic cyclotomic extensions. Now we know the bottom composition vanishes for all extensions  $L/K$ , and since  $\chi$  can be chosen arbitrarily, this shows the top composition vanishes  $\square$

### 4.2.5 Existence

By the reciprocity law, we see that a group containing a norm group is a norm group.

**Lemma 4.2.15.** *Let  $\mu_n \subseteq K$  be a number field. Let  $S$  contain the infinite primes, the primes dividing  $n$ , and class group generators. Then any  $a \in K$  which is an  $n$ th power in  $S$  and unit elsewhere is an  $n$ th power.*

*Proof.* Consider  $L = K(a^{\frac{1}{n}})$ . This extension is totally split over  $S$  and unramified over other primes. Thus  $\text{Nm } \mathbb{I}_L \supset \mathbb{I}_S$ , and we get  $L \cong K$  from reciprocity  $\square$

**Lemma 4.2.16** (Kummer). *Let  $p$  be a prime and  $K$  a number field containing  $\mu_p$ . Let  $S$  be a big set of primes, and consider  $L = K[U(S)^{\frac{1}{p}}]$ . Then  $\text{Nm } \mathbf{C}_L \leq \mathbf{C}_K$  is the subgroup  $\mathbf{C}_K^p \cdot U_{K,S}$ , where  $U_{K,S}$  consists of units outside  $S$  and 1 on  $S$ .*

*Proof.* Locally we know  $K_v^{\times p} \subseteq \text{Nm } L^{v \times}$  from local class field. Letting  $E = \prod_{v \in S} K_v^{\times p} \times \prod_{v \notin S} U_v$ , we get  $E \subseteq \text{Nm } \mathbb{I}_L$ . By the technical lemma from the section on the second inequality, together with the previous lemma, we deduce that  $(\mathbb{I}_K : K^{\times} E) = p^s$ . But  $(\mathbb{I}_K : K^{\times} \text{Nm } \mathbb{I}_L) = p^s$  from reciprocity, so  $EK^{\times} = \text{Nm } \mathbb{I}_L K^{\times}$   $\square$

**Lemma 4.2.17.** *Suppose  $p$  prime and  $\mu_p \subseteq K$ . Then every open subgroup  $U \subseteq \mathbf{C}_K$  with finite  $p$ -torsion quotient is a norm group.*

*Proof.* We have  $\text{Nm } \mathbf{C}_L = \mathbf{C}_K^p \cdot U_{K,S}$ . Now let  $U' \subseteq \mathbb{I}_K$  be the inverse image of  $U$ . Then  $U' \supset \prod_{v \in S} 1 \times \prod_{v \notin S} U_v$  for some big  $S$ . Thus  $U' \supset \text{Nm } \mathbb{I}_{K(U(S)^{\frac{1}{p}})} K^{\times}$  (using the  $p$ -torsion condition). This finishes the proof  $\square$

**Theorem 4.2.18** (Pre-Existence). *Every open subgroup of finite index in  $\mathbf{C}_K$  is a norm group (not necessarily from an abelian extension, for now)*

*Proof.* Let  $p | (\mathbf{C}_K : U)$ . It suffices to show the inverse image  $\text{Nm}^{-1}$  to some extension is a norm group, so assume  $\mu_p \subseteq K$ . Let  $U \subseteq U_1$  have index  $p$  in  $\mathbf{C}_K$ , so  $U_1 = \text{Nm } \mathbf{C}_L$ . In fact,  $L$  is cyclic of degree  $p$ . Then,  $(\mathbf{C}_L : \text{Nm}^{-1}(U)) = \frac{(\mathbf{C}_K : U)}{(\mathbf{C}_K : U_1)}$  has smaller index so it is a norm group by induction  $\square$

Now, note that  $\phi$  commutes with inflations from the local case. This means we can repeat exactly the same proof for norm limitation, proving it in the global case. This gives the full form of the existence theorem: Every open subgroup of finite index is the norm from a unique abelian extension.

### 4.2.6 Universal Norm Group

Let  $D_K = \bigcap \text{Nm}_{L/K} \mathbf{C}_L \leq \mathbf{C}_K$ . Unlike the local case, it is nonzero, but we can still prove divisibility.

**Theorem 4.2.19.**  *$D_K$  is divisible.*

*Proof.* Let  $p$  be prime. Let  $L/K$  be an extension containing  $p$ th roots of unity and let  $S$  be a large set of primes. The norm group of  $L \left( U_S^{\frac{1}{p}} \right) / L$  is  $(\mathbf{C}_L)^p \cdot U_{K,S}$  by Kummer, hence  $D_L \leq (\mathbf{C}_L)^p \cdot U_{K,S}$ . Denoting  $X^0 = X[[\cdot]]$  we get  $D_L^0 \leq (\mathbf{C}_L^0)^p \cdot U_{K,S}$ . This lives inside the compact  $\mathbf{C}_L^0$ . By that compactness, we get  $D_L^0 \subseteq (\mathbf{C}_L^0)^p$  (as there is a net of approximations of the division by  $p$ , which has to have a partial limit). We have  $D_K^0 = \text{Nm}_{L/K} D_L^0$  by compactness, and thus  $D_K^0 \leq (\text{Nm} \mathbf{C}_L^0)^p$ . Denote  $a^{\frac{1}{p}}$  as the set of  $p$ th roots for  $a \in D_K^0$ . Then the two closed sets  $\text{Nm} \mathbf{C}_L^0$  and  $a^{\frac{1}{p}}$  intersect. By compactness we get that  $D_K^0$  is divisible, which suffices  $\square$

Note that  $D_K^0 = \bigcap \text{Nm}_{L/K} \mathbf{C}_L^0$ . Note that there is a complete correspondence between open subgroups of  $\mathbf{C}_K$  and  $\mathbf{C}_K^0$ , and since  $\mathbf{C}_K^0$  is compact, we find that all open subgroups of  $\mathbf{C}_K$  are of finite index (and hence are norm groups).

**Theorem 4.2.20.**  *$D_K$  is the connected component of the identity in  $\mathbf{C}_K$ .*

*Proof.* This follows from a topological groups theorem: the intersection of open subgroups in a locally compact totally disconnected group is the identity. For this, note there is a compact open neighborhood  $U$  of 1 (take any precompact neighborhood, and use the disconnectedness to separate an inner compact open subset), make it symmetric, and then a clever compactness argument finds a subset  $V \subseteq U$  such that  $UV \subseteq U$ , and this suffices  $\square$

### 4.2.7 Comparing with the Tate isomorphism

We begin with a technical computation.

Let us figure out how to represent  $u \in H^2(\mathbf{C}_L)$  as a crossed homomorphism (where there is no problem assuming  $L/K$  is cyclic cyclotomic). Recall that  $\text{Ind}(L_{v_0}) \cong \prod L_w^\times$  takes  $\rho \mapsto a_\rho$  to  $(\rho a_{\rho^{-1}})_{\rho v_0}$ . We know that the isomorphism  $\bigoplus H^2(L^v/K_v) \cong H^2(\mathbb{I}_L)$  identifies a crossed homomorphism  $f : G_v^2 \rightarrow L^{v \times}$  with  $F : G^2 \rightarrow \prod_{w|v} L_w^\times$ , which is the induction, and deriving this gives us  $F(g, h) = (\rho \psi(\rho^{-1}) f(\psi(\rho^{-1})^{-1} \psi(\rho^{-1} g), \psi(\rho^{-1})^{-1} \psi(\rho^{-1} h)))_{\rho v_0}$ , where  $\psi : G \rightarrow H$  satisfies  $\psi(hx) = h\psi(x)$ . This is then pushed into  $\mathbf{C}_L$ .

Thus, if  $u \in H^2(\mathbf{C}_L)$  has invariant  $\frac{1}{n}$ , then it is induced from a sum  $\sum a_v u_v$  for  $\text{inv}(u_v) = \frac{1}{n_v}$  and  $\sum \frac{a_v}{n_v} = \frac{1}{n}$ . Wlog we may assume the  $v$  are unramified. Those  $u_v$  act by  $u_v(\sigma_v^i, \sigma_v^j) = \pi_v^{\frac{i\%n_v - j\%n_v + (j-i)\%n_v}{n_v}}$ . Therefore, our  $u$  acts by

$$g, gh \mapsto \left( \pi_v^{1_{\log \sigma_{w_0}(\psi(\rho^{-1})^{-1} \psi(\rho^{-1} g)) + \log \sigma_{w_0}(\psi(\rho^{-1} g)^{-1} \psi(\rho^{-1} gh))} \geq n_v} \right)_{w=\rho w_0|v} = \left( \pi_v^{1_{\log \sigma_w(\psi(g)) + \log \sigma_w(\psi(g)^{-1} \psi(gh))} \geq n_v} \right)_{w|v}$$

**Theorem 4.2.21.** *The isomorphism  $\phi_K : \mathbf{C}_K / \text{Nm} \mathbf{C}_L \rightarrow \text{Gal}(L/K)^{\text{ab}}$  defined by the product of the local Artin is inverse to the global Tate isomorphism.*

*Proof.* Denote the inverse to the Tate isomorphism by  $\Phi : \mathbf{C}_K / \text{Nm} \mathbf{C}_L \rightarrow \text{Gal}(L/K)^{\text{ab}}$ . Let  $\chi : G_{L/K}^{\text{ab}} \rightarrow \mathbb{Q}/\mathbb{Z}$  be some continuous character. Then, as in the local case,  $\chi(\Phi_{L/K}(a)) = \delta(\chi \cup \Phi_{L/K}(a))$  and  $\text{inv}_{L/K}(a \cup \delta_\chi) = \text{inv}_{L/K}(\delta(\chi \cup \Phi_{L/K}(a)) \cup u)$ . Since  $\text{inv}_{L/K}(u) = \frac{1}{n}$ , those are equal. From the inv being inflation invariant, we get  $\Phi_{L|K}|_E = \Phi_{E|K}$ , meaning the Tate isomorphism commutes with

inflations, as does the  $\phi = \prod_v \phi_v$  from the local statement. This in particular reduces the statement of equality to abelian extensions (as taking the maximal abelian doesn't change either side, and the map is inflation). So from now,  $L/K$  is abelian. Now by both isomorphisms commuting with corestriction we may assume  $L/K$  is cyclic of prime power order.

The Tate isomorphism is induced by cup product with some  $u \in H^2(\mathbf{C}_L)$ , with invariant  $\frac{1}{n}$ . Taking some large unramified place  $v$ , we can multiply our  $u$  by  $\frac{n}{n_v}$  to get a nice representative  $u' = (\pi_v^{1_{\log_{\sigma_w}(\psi(g)) + \log_{\sigma_w}(\psi(g)^{-1}\psi(gh))} \geq n_v})_{w|v}$ .

The Tate isomorphism, multiplied by  $\frac{n}{n_v}$ , takes an element  $\sigma$  to  $\sum_{\tau \in G} u(\tau, \tau\sigma_v)$ , just as in the local case. Substituting the previous formula, we get that the Tate multiplied by  $\frac{n}{n_v}$  is equivalent on  $\sigma$  to  $\sum_{\tau \in G} (\pi_v^{1_{\log_{\sigma_w}(\psi(\tau)) + \log_{\sigma_w}(\psi(\tau)^{-1}\psi(\tau\sigma))} \geq n_v})_{w|v}$ . We can sum on the power of  $\sigma_w$  in the left of  $\tau$ , which leaves us with  $\pi_v^{\sum_i \log_{\sigma_w} \psi(g_i\sigma)} = \pi_v^{\log_{\sigma_w} \text{Ver}_{\langle \sigma_w \rangle}(\sigma)} = \phi_{w|v}^{-1}(\text{Ver}_{\langle \sigma_w \rangle}(\sigma))|_{w|v}$ . Note that this is independent of  $w$  by conjugating. Since we have assumed  $L/K$  abelian, this is indeed  $\frac{n}{n_v} \phi_v^{-1}(\sigma)$ , as expected. So the isomorphisms agree after multiplication by  $\frac{n}{n_v}$ . If we had  $\text{lcm}(n_v) = n$  we would win. But as we said, the extension can be assumed to be of prime power order, where this indeed holds as the Frobenius elements generate the group  $\square$

### 4.3 Ray Class Field

Let  $K$  be a number field. A modulus is a collection  $m$  of primes in  $S$  with (nonnegative) multiplicities. Real primes can only have multiplicity 0,1 and complex cannot appear. Let  $m_0, m_\infty$  be the finite and infinite parts of  $m$ . Let  $I(m)$  be the free group on finite primes outside  $m_0$ , and  $K(m) \leq K^\times$  the subset of values with valuation 0 on every finite prime outside  $m_0$ . Let  $K_{m,1} \leq K(m)$  be the collection of values that are 1 mod  $m_0$  and positive in all valuations of  $m_\infty$ . Let  $C_{K,m}$ , the ray class group of  $m$ , be the cokernel of  $K_{m,1} \rightarrow I(m)$  (which is the map that takes a value to the formal sum of its primes). Let  $U_{m,1} = U_K \cap K_{m,1}$ . Then the spectral sequence for

$$\begin{array}{ccccccc} U_{m,1} & \longrightarrow & K_{m,1} & \longrightarrow & I(m) & \longrightarrow & C_{K,m} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow \\ U_K & \longrightarrow & K_m & \longrightarrow & I(m) & \longrightarrow & C_K \end{array}$$

gives the exact sequence  $0 \rightarrow U_K/U_{m,1} \rightarrow K_m/K_{m,1} \rightarrow C_{K,m} \rightarrow C_K \rightarrow 0$ . Thus the ray class group is finite of size  $h_m = \frac{h \cdot \phi(m)}{[U_K : U_{m,1}]}$ , where  $\phi(m) = \phi(m_0)2^{r(m)}$ .

**Theorem 4.3.1.** *There is a natural quotient map  $C_K \rightarrow C_{K,m}$ . All finite quotients of  $C_K$  factor through some ray class group. If a finite quotient of  $C_K$  factors through  $C_{K,m}$  and through  $C_{K,m'}$  then it factors through  $C_{K, \gcd(m, m')}$ .*

*Proof.* If we let  $W_m = \prod_{\mathfrak{p} \notin m} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \in m_0} U_{\mathfrak{p}}^{(n)} \times \prod_{\mathfrak{p} \in m_\infty} (\mathbb{R}^+)_{\mathfrak{p}}$ , then it is not hard to see that  $C_K/W_m \cong C_{K,m}$ . From here it is easy to see all the statements  $\square$

For an extension of local fields  $L/K$ , we define the conductor  $f(L/K) = \prod_v \mathfrak{p}_v^{f(L^v/K_v)}$  (recall the definition of conductor in the local case). Thus, again,  $L/K$  is unramified iff  $f(L/K) = 1$ . If  $L/K$  is abelian, then the last result shows this is equivalent to the minimal modulus  $f$  such that  $C_K \rightarrow \text{Gal}(L/K)$  factors through  $C_{K,f}$ .

**Theorem 4.3.2.** *Let  $m$  be a modulus of  $K$ . Then there is a unique abelian extension  $L_m/K$  unramified outside  $m$  such that  $\text{Gal}(L_m/K) \cong C_{K,m}$  and this correspondence takes a prime  $\mathfrak{p} \notin m$  into its Frobenius. This is the ray class field for  $m$ . When  $m = 1$  this is the Hilbert class field.*

*Proof.* The existence is a consequence of global class field theory. Uniqueness is not hard □

Note that  $f(L_m/K)$  is the minimal  $f|m$  such that  $C_{K,f} = C_{K,m}$ .

**Corollary 4.3.3.** *The ray class field of  $m$  is the maximal abelian extension of conductor dividing  $m$ , and its subfields are precisely the extensions of conductor dividing  $m$ . In particular, the Hilbert class field is the maximal abelian unramified extension.*

**Corollary 4.3.4** (Kronecker-Weber). *Every abelian extension of  $\mathbb{Q}$  is contained in a cyclotomic extension.*

*Proof.* The ray class field for  $(m)\infty$  is the cyclotomic  $\mathbb{Q}(\zeta_m)$  □

**Theorem 4.3.5** (Principal Ideal). *Any ideal of  $K$  becomes principal in the Hilbert class field of  $K$ .*

*Proof.* Let  $L/K$  be the Hilbert class field for  $m$ , and  $\tilde{L}/L$  be the Hilbert class field for  $L$ . Let  $G = \text{Gal}(\tilde{L}/K)$ .

As  $\tilde{L}/K$  is unramified, we see that  $L$  is the largest abelian subextension of  $\tilde{L}$ . Then we have a commutative square

$$\begin{array}{ccc} Cl_K = \mathbf{C}_K / \text{Nm } \mathbf{C}_{\tilde{L}} & \xrightarrow{\sim} & G^{\text{ab}} \\ \downarrow & & \downarrow \text{Ver} \\ Cl_L = \mathbf{C}_L / \text{Nm } \mathbf{C}_{\tilde{L}} & \xrightarrow{\sim} & (G')^{\text{ab}} \end{array}$$

and our purpose is to show that the left vertical arrow vanishes. So this becomes the following group-theoretic claim:

**Theorem 4.3.6.** *The Verlagerung map  $G^{\text{ab}} \rightarrow (G')^{\text{ab}}$  vanishes.*

*Proof.* See Neukirch, Algebraic number theory, theorem VI.7.6 (page 410) □

□

**Remark 4.3.7.** *The map  $(G')^{\text{ab}} \rightarrow G^{\text{ab}}$  obviously vanishes, so we get that both restriction and corestriction maps between  $Cl_K, Cl_L$  vanish.*

## 4.4 Quadratic forms

We deal with nondegenerate quadratic forms. If a quadratic form represents zero, it represents everything.

Note that  $x^2 - ay^2 - bz^2$  represents 0 iff  $a$  is a norm from  $K(\sqrt{b})$ , that is  $(a, b)_K = 1$ .

**Claim 4.4.1.** *The form  $x^2 - by^2 - cz^2 + acw^2$  represents 0 iff  $c$  is in the image of  $\text{Nm} : K(\sqrt{a}, \sqrt{b}) \rightarrow K(\sqrt{ab})$ .*

*Proof.* This means  $c = \frac{\text{Nm}_{\sqrt{b}}(x + \sqrt{b}y)}{\text{Nm}_{\sqrt{a}}(z + \sqrt{a}w)}$ , which establishes one condition. It suffices to show that a norm  $K(\sqrt{a}, \sqrt{b}) \rightarrow K(\sqrt{ab})$  is a product of an  $\sqrt{a}$  norm and a  $\sqrt{b}$  norm. Denote the Galois elements by  $1, \sigma, \tau, \sigma\tau$ . Then we are given  $c = z \cdot \sigma\tau z$ . Thus  $\text{Nm}_{\sqrt{a}}(z \cdot \tau z) = c^2$ , which by Hilbert 90 implies  $\frac{z \cdot \tau z}{c} = \frac{x}{\sigma x}$  for  $\tau x = x$ . This implies that  $\frac{z}{x}$  is  $\sigma$ -invariant, which finishes the proof  $\square$

**Claim 4.4.2.** *If  $L/K$  is a cyclic extension of number fields, then elements which are norms locally are norms.*

*Proof.* Since  $\hat{H}_T^{-1}(\mathbf{C}_L) = \hat{H}_T^1(\mathbf{C}_L) = 0$ , there is an injection  $\hat{H}_T^0(L^\times) \rightarrow \hat{H}_T^0(\mathbb{I}_L)$  or  $\hat{H}_T^0(L/K) \rightarrow \bigoplus_v \hat{H}_T^0(L^v/K_v)$   $\square$

**Theorem 4.4.3** (Hasse-Minkowski). *Let  $q$  be a form of degree  $n$  over a number field  $K$ . Then, if  $n \geq 3$  it represents 0 almost everywhere, and if it represents  $a$  locally everywhere then it represents  $a$ .*

*Proof.* For the first part, wlog  $n = 3$ , then of course  $(a, b)_v = 1$  almost everywhere. For the second, wlog  $a = 0$ , and then for  $n \leq 4$ , the statement follows in a similar fashion, using the fact on local norms in cyclic extensions.

In the general case, write  $q = ax^2 + by^2 - q'$ . We know that  $q'$  represents 0 almost everywhere, and in the finite set where it doesn't, choose  $c_v$  so that both  $ax^2 + by^2, q'$  represent it. Lift those to a common  $c$  which is very close to all  $c_v$  and is represented by  $ax^2 + by^2$ . In particular,  $c/c_v$  are squares in  $K_v$ . It follows that  $cx^2 - q'$  represents 0 everywhere, so it represents 0 by induction. Thus both  $ax^2 + b^2, q'$  represent  $c$   $\square$

**Theorem 4.4.4.** *A quadratic form of degree 4 over a local field represents all nonzero values.*

*Proof.* Representing it as  $x^2 - by^2 - cz^2 - acw^2$ , and using local class field, we see that all  $c$  are the product of norms from the two norm groups, i.e.  $q$  represents 0, whenever those norm groups are distinct. Thus we care about the situation  $b = a\lambda^2$ , i.e.  $a = b$ . Then the form is norm  $H(b, c)^\times \rightarrow K^\times$ . But from local Brauer theory this represents the norm groups of all quadratic extensions, so we are done  $\square$

As a trivial corollary, a local quadratic in 5 variables represents 0.

**Theorem 4.4.5.** *Let  $U, W$  be two isometric nondegenerate subspaces of a quadratic space  $(V, Q)$ . Then  $U^\perp, W^\perp$  are isometric.*

*Proof.* If  $U, W$  are not lines, split them as  $U = U' \oplus U'', W = W' \oplus W''$  with pairwise isometries, then by induction  $U^\perp \oplus U'' \cong W^\perp \oplus W''$ , and again by induction  $U^\perp \cong W^\perp$ . So wlog  $U, W$  are lines  $ku, kw$ . By  $Q(u + w) + Q(u - w) = 4Q(u)$  we may assume  $Q(u - w) \neq 0$ , thus we get the isometry  $\tau(x) = x - \frac{2B(x, u-w)}{Q(u-w)}(u - w)$ , which takes  $u$  to  $w$  as  $Q(u - w) = Q(u) + Q(w) - 2B(u, w) = 2Q(u) - 2B(u, w) = 2B(u, u - w)$   $\square$

In other words: we now have that  $a \oplus c \cong b \oplus c$  implies  $a \cong b$ .

**Theorem 4.4.6** (Extra Hasse-Minkowski). *If two quadratic forms are equivalent locally everywhere, they are equivalent.*

*Proof.* If one represents  $a$ , then it represents it locally, thus the other represents it locally, and by the standard Hasse-Minkowski the other represents it. Then the previous theorem allows us to reduce the dimension  $\square$

**Theorem 4.4.7.** *An integer  $n$  is the sum of three squares iff  $n \not\equiv 7(8)$ .*

*Proof.* Consider the quadratic  $x^2 + y^2 + z^2 - nw^2$ . We show this represents 0 locally everywhere. At odd primes, this is easy as  $x^2 + y^2 + 1 = 0$  has a solution. At 2, we should only find a solution mod 8, which is possible exactly under this condition.

Note that this only shows the sum of three rational squares. So let us take this rational point  $x = a/b$  on the sphere and approximate it by the integral point  $y$ . Let  $x - y = \frac{v}{b}$ . Let  $f(p) = p_0^2 + p_1^2 + p_2^2$ . Consider  $F(\lambda) = f(y + \lambda v) - n = A\lambda^2 + B\lambda + C$  which is an integral quadratic. It has one root  $\frac{1}{b}$ , so the other root is  $C/(A/b)$ . Note that  $A/b$  is integral, so we just have to show  $|A/b| < |b|$ . But  $|A/b^2| = f(x - y) < 1$ , which finishes the proof  $\square$