LECTURES
on
COHOMOLOGICAL CLASS FIELD THEORY

Number Theory II | 18.786 | Spring 2016
Taught by Sam Raskin at MIT

Oron Propp

Last updated August 21, 2017

Contents

Preface

These notes are for the course Number Theory II (18.786), taught at MIT in the spring semester of 2016 by Sam Raskin. The original course page can be found online here[1]; in addition to these notes, it includes an annotated bibliography for the course, as well as problem sets, which are frequently referenced throughout the notes. Note that these problem sets are an essential part of the course, and often introduce important material not covered in these notes (though much is listed the index).

My approach in writing these notes was generally to reproduce as closely as possible the content of Sam's lectures, though I have occasionally filled in details or restructured things slightly to make them more clear to myself. I began typing up my handwritten notes for the course during the semester, but around half of the work was done in the summer after my sophomore year when I had more free time. As such, these notes are often rough in places, though my guess is that their quality improves the farther in one reads. Of course, any mistakes in these notes are solely mine, and not Sam's; please do not hesitate to contact me with any typos, errors, or other comments at `opropp@mit.edu`.

The course began in lectures 2–5 with an analysis of the quadratic case of Class Field Theory via Hilbert symbols, in order to give a more hands-on introduction to the ideas of Class Field Theory. In lectures 6–13, we developed the cohomological machinery necessary for our later treatment of Class Field Theory. Next, in lectures 14–18, we proved the main theorem of Local Class Field Theory; I would like to acknowledge Marc Hoyois for delivering Lecture 16 in Sam's absence. Finally, in lectures 19–23, we proved the main theorem of Global Class Field Theory; this is arguably the most difficult part of the course. The course concluded with two lectures delivered by Professor Bjorn Poonen, the first on quadratic forms and the Hasse–Minkowski theorem, and the second on Witt cancellation and the Brauer–Manin obstruction; unfortunately, I have not yet gotten around to typing these up.

I would like to thank Sam for teaching this course, for very thoughtfully answering my many questions on the material, for encouraging me to complete and upload these notes, and for his comments on an earlier draft thereof. Please note that lectures 1 and 16 are very closely adapted from Sam's own lecture notes, which he graciously provided to me.

I hope these notes can prove useful to you, and that you enjoy this course as much as I did!

[1] `http://math.mit.edu/~sraskin/cft/index.html`

LECTURE 1

Introduction

In this class, we will begin by studying the quadratic version of Class Field Theory (CFT), with an emphasis on explicit CFT. We will then develop a cohomological approach to CFT. Finally, we may discuss additional topics, such as explicit CFT (in greater depth), the Fontaine-Herr approach to Local Class Field Theory (LCFT), algebraic groups, or Tate duality.

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

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

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

THEOREM 1.1 (Kronecker–Weber). *Every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$ for some n, where ζ_n is a primitive nth root of unity.*

That is, if the splitting field of $f \in \mathbb{Q}[x]$ has an abelian Galois group, then all (equivalently, some) roots of f can be written as rational functions of ζ_n for some n. As a brief reminder, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ (i.e., the Euler totient function), and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, with an element $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting as $\zeta_n \mapsto \zeta_n^m$. CFT is essentially equivalent to the Kronecker–Weber theorem for $\mathbb{Q}$, but gives additional (though inexplicit) control of the situation for general number fields.

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

$$\sqrt{2} = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \overline{\zeta_8} = \frac{1+i}{\sqrt{2}} + \frac{1-i}{\sqrt{2}},$$
$$\sqrt{-3} = \zeta_3 - \zeta_3^{-1} = \zeta_3 + \overline{\zeta_3} = \frac{-1+\sqrt{-3}}{2} + \frac{-1-\sqrt{-3}}{2},$$

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

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

THEOREM 1.2 (Hasse Principle). *Let K be a number field, and*

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

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

$$q(x_1, \dots, x_n) = y$$

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

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

We now turn to the statements of the main theorems of CFT, which perhaps are not yet so inspiring. Let K a local field, so that either K is archimedean, in which case $K = \mathbb{R}, \mathbb{C}$, or K is nonarchimedian, in which case $K/\mathbb{Q}_p$ or $K = \mathbb{F}_{p^n}((t))$ for some p and n. Let K^{sep} denote its separable closure. Observe that if K is any field with abelian extensions $K^{\mathrm{sep}}/K_1/K$ and $K^{\mathrm{sep}}/K_2/K$ (which are necessarily Galois), then the compositum $K_1 \cdot K_2$ is also abelian, justifying the following definition:

DEFINITION 1.3. The *maximal abelian extension* K^{ab}/K is the compositum of all abelian extensions $K^{\mathrm{sep}}/K'/K$, and $\mathrm{Gal}^{\mathrm{ab}}(K) := \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the abelianization of the *absolute Galois group* $\mathrm{Gal}(K) := \mathrm{Gal}(K^{\mathrm{sep}}/K)$.

We also recall the following definition:

DEFINITION 1.4. For a group G, the inverse limit

$$\widehat{G} := \varprojlim_{\substack{H \lhd G \\ [G:H] < \infty}} G/H$$

over quotients by finite-index normal subgroups is the *profinite completion* of G.

We can now state the main theorem of Local Class Field Theory:

THEOREM 1.5 (Main Theorem of LCFT). *For any finite extension $K/\mathbb{Q}_p$, there is a canonical isomorphism*

$$\mathrm{Gal}^{\mathrm{ab}}(K) \simeq \widehat{K^\times}$$

of profinite groups.

EXAMPLE 1.6. The first-order structure of $K^\times$ is given by the short exact sequence

$$1 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{v} \mathbb{Z} \to 0, \tag{1.1}$$

where v is the valuation homomorphism taken with respect to the maximal ideal $\mathfrak{p}_K \subseteq \mathcal{O}_K$ (i.e., it sends a uniformizer of $\mathcal{O}_K$ to 1); the ring of integers $\mathcal{O}_K^\times$ is profinite and open in $K^\times$. The second-order structure of $K^\times$ is given by the inverse limit

$$\mathcal{O}_K^\times = \varprojlim_n \mathcal{O}_K^\times/(1+\mathfrak{p}_K^n),$$

so that (1.1) becomes

$$1 \to \mathcal{O}_K^\times \to \widehat{K^\times} \xrightarrow{\hat{v}} \widehat{\mathbb{Z}} \to 0$$

after taking profinite completions.

Now, for any finite Galois extension L/K, there is an action of $\mathrm{Gal}(L/K)$ on L that preserves $\mathcal{O}_L$ and $\mathfrak{p}_L$. Thus, it descends to an action on $k_L := \mathcal{O}_L/\mathfrak{p}_L$ fixing $k_K := \mathcal{O}_K/\mathfrak{p}_L$; these are finite fields, say $k_L = \mathbb{F}_{q^n}$ and $k_K = \mathbb{F}_q$ for some prime-power q. We therefore have a map

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(k_L/k_K) = \mathbb{Z}/n\mathbb{Z},$$

which is an isomorphism if L/K is unramified; the group $\mathrm{Gal}(k_L/k_K)$ is generated by the Frobenius automorphism $x \mapsto x^q$. Taking inverse limits over all such L/K then yields a homomorphism

$$\mathrm{Gal}(K) \to \mathrm{Gal}(k) = \widehat{\mathbb{Z}}$$

given by the Frobenius elements, which factors through $\mathrm{Gal}^{\mathrm{ab}}(K)$ by the universal property of abelianization. Under LCFT, this map coincides with the map $\hat{v}$ above.

Now, recall that the *ring of adèles* of a number field F is defined as the direct limit

$$\mathbb{A}_F := \varinjlim_S \left(\prod_{v \in S} F_v \times \prod_{v \notin S} \mathcal{O}_{F_v} \right)$$

over finite sets S of places F. It comes with a diagonal embedding

$$F \hookrightarrow \mathbb{A}_F,$$

by which F is discretely embedded (think $\mathbb{Z} \hookrightarrow \mathbb{R}$). Morally, $\mathbb{A}_F$ amalgamates all local information about F, while this embedding encodes its global aspects. Inside $\mathbb{A}_F$ lies the group $\mathbb{A}_F^\times$ of units, topologized via the direct limit

$$\mathbb{A}_F^\times = \varinjlim_S \left(\prod_{v \in S} F_v^\times \times \prod_{v \notin S} \mathcal{O}_{F_v}^\times \right),$$

with S as before (and all terms open in $\mathbb{A}_F^\times$), rather than the finer subspace topology. We are now ready to state the main theorem of Global Class Field Theory (GCFT):

THEOREM 1.7 (Main Theorem of GCFT). *For any finite extension $F/\mathbb{Q}$, there is a canonical isomorphism*

$$\mathrm{Gal}^{\mathrm{ab}}(F) \simeq \widehat{\mathbb{A}_F^\times/F^\times}$$

of profinite groups.

These two main theorems are compatible in the following manner. If v is a place of a global field F with algebraic closure $\overline{F}$, then we have maps

$$\begin{array}{ccc} F & \hookrightarrow & F_v \\ \downarrow & & \downarrow \\ \overline{F} & \hookrightarrow & \overline{F}_v, \end{array}$$

which induce (injective) maps

$$\begin{aligned} \mathrm{Gal}(F_v) &\to \mathrm{Gal}(F), \\ \mathrm{Gal}^{\mathrm{ab}}(F_v) &\to \mathrm{Gal}^{\mathrm{ab}}(F). \end{aligned}$$

The diagram

$$\begin{array}{ccc} F_v^\times & \xrightarrow{x\mapsto(1,\dots,1,x,1,\dots)} & \mathbb{A}_F^\times/F^\times \\ \downarrow{\scriptstyle \mathrm{LCFT}} & & \downarrow{\scriptstyle \mathrm{GCFT}} \\ \mathrm{Gal}^{\mathrm{ab}}(F_v) & \longrightarrow & \mathrm{Gal}^{\mathrm{ab}}(F), \end{array}$$

whose vertical arrows are obtained by composing the the natural map from each group to its profinite completion with the respective identifications of the main theorems of Local and Global CFT, then commutes.

We will begin by spending several weeks setting up CFT for quadratic extensions of local fields and $\mathbb{Q}$, since this nicely captures what is exciting about the subject, and is more hands-on than the cohomological approach we will develop afterwards. To start, let K be any field of characteristic $\mathrm{char}(K) \neq 2$. Let $\mathrm{Gal}_2(K)$ be the maximal quotient of $\mathrm{Gal}(K)$ in which $g^2 = 1$ for all $g \in \mathrm{Gal}(K)$. It is necessarily abelian, so there is a surjection

$$\mathrm{Gal}^{\mathrm{ab}}(K) \twoheadrightarrow \mathrm{Gal}_2(K),$$

and it carries the structure of an $\mathbb{F}_2$-vector space.

Claim 1.8. *There is a canonical isomorphism*

$$\mathrm{Gal}_2(K) \simeq (K^\times/(K^\times)^2)^\vee := \mathrm{Hom}(K^\times/(K^\times)^2, \mathbb{Z}/2\mathbb{Z})$$

of $\mathbb{F}_2$-vector spaces.

Proof. We first construct such a map as follows: given $\sigma \in \mathrm{Gal}_2(K)$, define $\chi_\sigma \in (K^\times/(K^\times)^2)^\vee$ by

$$\begin{aligned} \chi_\sigma \colon K^\times/(K^\times)^2 &\to \mathbb{Z}/2\mathbb{Z}, \\ d &\mapsto \begin{cases} 0 & \text{if } \sigma(\sqrt{d}) = \sqrt{d}, \\ 1 & \text{if } \sigma(\sqrt{d}) = -\sqrt{d}. \end{cases} \end{aligned}$$

It is easy to see that this is, in fact, a homomorphism: given $\sigma_1, \sigma_2 \in \mathrm{Gal}_2(K)$ and $d \in K^\times/(K^\times)^2$, we have

$$(\sigma_1\sigma_2)(\sqrt{d}) = (-1)^{\chi_{\sigma_1}(d)}(-1)^{\chi_{\sigma_1}(d)}\sqrt{d},$$

which implies that

$$\chi_{\sigma_1\sigma_2} = \chi_{\sigma_1} + \chi_{\sigma_2}.$$

Now, since both the source and target are profinite 2-torsion abelian groups, it suffices to show that this map is an isomorphism after taking continuous duals. As usual, we have

$$\mathrm{Hom}_{\mathrm{cts}}((K^\times/(K^\times)^2)^\vee, \mathbb{Z}/2\mathbb{Z}) = K^\times/(K^\times)^2,$$

and giving a continuous map $\mathrm{Gal}_2(K) \to \mathbb{Z}/2\mathbb{Z}$ is the same as giving a quadratic extension $K^{\mathrm{sep}}/F/K$, which has the form $K(\sqrt{d})$ with $d \in K^\times$ defined up to multiplication by a square. □

Example 1.9. In the case $K = \mathbb{Q}$, this result gives an isomorphism

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 \xrightarrow{\simeq} \bigoplus_p \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z},$$

where the direct sum ranges over all primes p. However, it's not at all clear how to compare this group to the profinite completion

$$\left[\mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{A}_{\mathbb{Q}}^\times)^2\right]^\wedge,$$

as the main theorem of GCFT would have us do.

Now, if K is a local field, then LCFT predicts that $K^\times/(K^\times)^2$ is canonically self-dual; the pairing

$$(\cdot,\cdot)\colon K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \{1,-1\}$$

realizing this duality is called the *Hilbert symbol*. Our goal in the next few lectures will be to construct it and show that this is indeed the case.

LECTURE 2

Hilbert Symbols

Let K be a local field over $\mathbb{Q}_p$ (though any local field suffices) with $\mathrm{char}(K) \neq 2$. Note that this includes fields over $\mathbb{Q}_2$, since it is the characteristic of the field, and not the residue field, with which we are concerned. Recall from the previous lecture the duality

$$\mathrm{Gal}_2(K) := \mathrm{Gal}^{\mathrm{ab}}(K)/\{g^2 : g \in \mathrm{Gal}^{\mathrm{ab}}(K)\} \simeq \mathrm{Hom}\left(K^\times/(K^\times)^2, \mathbb{Z}/2\mathbb{Z}\right), \tag{2.1}$$

where $\mathrm{Gal}_2(K)$ and $\mathrm{Gal}^{\mathrm{ab}}(K)$ are profinite groups, the latter being the Galois group of the maximal abelian extension of K, and $K^\times/(K^\times)^2$ is a vector space of finite or infinite dimension over the two-element field $\mathbb{Z}/2\mathbb{Z}$ (in dualizing, the direct sum of copies of $\mathbb{Z}/2\mathbb{Z}$ comprising $K^\times/(K^\times)^2$ is changed to a product, reflecting the profinite nature of the left-hand side).

Also recall that LCFT states that $K^\times \to \mathrm{Gal}^{\mathrm{ab}}(K)$ is a profinite completion, and therefore that $\mathrm{Gal}_2(K) \simeq K^\times/(K^\times)^2$ in contrast to (2.1). Thus, LCFT predicts that there exists a canonical pairing of the following form:

DEFINITION 2.1. Let the *Hilbert symbol*

$$(\cdot,\cdot)\colon K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \{1,-1\}$$

be defined by

$$(a,b) := \begin{cases} 1 & \text{if there exist } x,y \in K \text{ such that } ax^2+by^2=1, \\ -1 & \text{otherwise,} \end{cases}$$

for $a, b \in K^\times$.

REMARK 2.2. This definition is only well-behaved for local fields. Also note that (a,b) really is defined modulo multiplication by squares in a and b, as these can be absorbed in x and y.

PROPOSITION 2.3. *The Hilbert symbol satisfies the following properties:*

(1) Bimultiplicativity. *For all $a,b,c \in K^\times$,*

$$(a,bc) = (a,b)\cdot(a,c).$$

(2) Non-degeneracy. *For all $a \in K^\times$, if $(a,b) = 1$ for all $b \in K^\times$, then $a \in (K^\times)^2$.*

Note that $(a,b) = (b,a)$ trivially. Bimultiplicativity says that we can solve $ax^2+by^2=1$ if and only if either we can solve both $ax^2+by^2=1$ and $ax^2+cy^2=1$ separately, or we can't solve either equation. This is a bit strange, and turns out to only hold in general for local fields.

EXAMPLE 2.4. Let $K := \mathbb{R}$. Then we can solve $ax^2 + by^2 = 1$ as long as a and b are not both negative. As such, we have $\mathbb{R}^\times/(\mathbb{R}^\times)^2 = \{1, -1\}$, since $(\mathbb{R}^\times)^2 = \mathbb{R}_{>0}$, and so the pairing $\{1, -1\} \times \{1, -1\} \to \{1, -1\}$ is indeed non-degenerate.

We now ask: when is $x \in K^\times$ a square? When $K = \mathbb{R}, \mathbb{C}$, the answer is clear. When, for instance, $x \in \mathbb{Q}_2^\times$, then we may write $x = 2^{v(x)}y$ where $y \in \mathbb{Z}_2^\times$, and x is a square if and only if $v_2(x)$ is even and y is a square (which, as will be shown in Problem 1(c) of Problem Set 1, is true if and only if $y \equiv 1 \bmod 8$).

Let $\mathfrak{p} \subseteq \mathcal{O}_K$ be the unique maximal ideal, $k := \mathcal{O}_K/\mathfrak{p}$ be the residue field with $\mathrm{char}(k) = p$, an odd prime, and $\pi \in \mathfrak{p}$ a uniformizer, that is, $\pi \notin \mathfrak{p}^2$.

CLAIM 2.5. *Let $x \in K^\times$, and write $x = \pi^{v(x)}y$, where $y \in \mathcal{O}_K^\times$. Then the following are equivalent:*

(1) x is a square;
(2) $v(x)$ is even and y is a square;
(3) $y \bmod \mathfrak{p}$ is a square in $K^\times$.

Note that we may reduce to $x \in \mathcal{O}_K^\times$. We offer two proofs:

PROOF (VIA HENSEL'S LEMMA). All explanations aside from that from the final condition are clear. So suppose $x \bmod \mathfrak{p}$ is a square in $\mathcal{O}_K^\times$. By Hensel's Lemma, the polynomial $p(t) = t^2 - x \in \mathcal{O}_K[t]$ has a root $r \in \mathcal{O}_K$ if it has a root $\bar{r}$ modulo $\mathfrak{p}$ such that $\bar{p}'(\bar{r}) \neq 0$, i.e., the derivative is nonzero. But the first condition holds by assumption, and in this case $p'(t) = 2t$ which is surely nonzero as $x = 0$, and therefore $\sqrt{x} = 0$, hence the second condition holds as well. □

PROOF (EXPLICIT). Consider the map $x \overset{\sigma}{\mapsto} x^2$, by which

$$\mathcal{O}_K^\times \xrightarrow{\sigma} S \subseteq \mathcal{O}_K^\times, \quad S := \{x \in \mathcal{O}_K^\times : x \text{ is a square mod } \mathfrak{p}\}.$$

We'd like to show that σ is surjective, that is, every element of $\mathcal{O}_K$ that is a square mod $\mathfrak{p}$ is a square in $\mathcal{O}_K^\times$. Now, observe that $\mathcal{O}_K^\times$ is a filtered abelian group with complete filtration (see Definition 2.7 below)

$$\mathcal{O}_K^\times \supseteq 1 + \mathfrak{p} \supseteq 1 + \mathfrak{p}^2 \supseteq 1 + \mathfrak{p}^2 \supseteq \cdots,$$

where the $1 + \mathfrak{p}^n$ are all open subgroups of $\mathcal{O}_K^\times$. Clearly $\mathcal{O}_K^\times/(1 + \mathfrak{p}) = k^\times$, and similarly $(1 + \mathfrak{p})/(1 + \mathfrak{p}^2) \simeq k$ as for any $1 + a\pi, 1 + b\pi \in 1 + \mathfrak{p}$, where $a, b \in \mathcal{O}_K/\mathfrak{p}$, we have $(1 + a\pi)(1 + b\pi) = 1 + (a + b)\pi + ab\pi^2$, and since $ab\pi^2 \in \mathfrak{p}^2$, we are left with $1 + (a + b)\pi$ in the associated graded term, hence multiplication simply corresponds to addition in k. Similarly, for each $n \geq 1$, we have $(1 + \mathfrak{p}^n)/(1 + \mathfrak{p}^{n+1}) \simeq k$ by a similar argument, since $n + 1 \leq 2n$. Now, σ acts on the filtration as

$$\begin{array}{ccccccc} \mathcal{O}_K^\times & \supseteq & 1 + \mathfrak{p} & \supseteq & 1 + \mathfrak{p}^2 & \supseteq & \cdots \\ \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} & & \downarrow{\scriptstyle \sigma} & & \\ \mathcal{O}_K^\times & \supseteq & S & \supseteq & 1 + \mathfrak{p} & \supseteq & 1 + \mathfrak{p}^2 \supseteq \cdots, \end{array}$$

where the inclusion $1 + \mathfrak{p} \subseteq S$ holds since 1 is trivially a square. Now, the map

$$\mathcal{O}_K^\times/(1 + \mathfrak{p}) = k^\times \xrightarrow{\sigma} (k^\times)^2 = S/(1 + \mathfrak{p})$$

on Gr_0 is trivially surjective (and has a small kernel). Moreover, for each $n \geq 1$, the map on Gr_n is

$$(1 + \mathfrak{p}^n)/(1 + \mathfrak{p}^{n+1}) \xrightarrow{\sigma} (1 + \mathfrak{p}^n)/(1 + \mathfrak{p}^{n+1}),$$

which, since for any $x \in k$ we have

$$(1+\pi^2 x)^2 = 1 + 2x\pi^n + x^2\pi^{2n} \equiv 1 + 2x\pi^n \bmod \mathfrak{p}^{n+1}$$

as $2n \geq n+1$, is equivalent to the map $k \xrightarrow{x \mapsto 2x} k$, which is an isomorphism because $\#k = p$ is an odd prime. Thus, σ is surjective on each graded term, so by Proposition 2.9, the map $\mathcal{O}_K^\times \xrightarrow{\sigma} S$ is surjective, as desired. □

REMARK 2.6. In general, the tools we have to deal with $\mathcal{O}_K^\times$ are the $\mathfrak{p}$-adic exponential map, and this filtration, which, though an abstract formalism, has the advantage of being simpler than $\mathcal{O}_K^\times$, as the quotients are all isomorphic to finite fields. As a general principle, we can understand many things about A via its associated graded $\mathrm{Gr}_* A$.

DEFINITION 2.7. Let A be an abelian group. A *filtration* on A is a descending sequence of subgroups

$$A =: F_0 A \supseteq F_1 A \supseteq F_2 A \supseteq \cdots,$$

and it is said to be *complete* if $A \xrightarrow{\sim} \varprojlim_n A/F_n A$. The groups $\mathrm{Gr}_n A := F_n A / F_{n+1} A$ are the *associated graded terms* of the filtration.

EXAMPLE 2.8. The groups

$$\mathcal{O}_K \simeq \varprojlim_n \mathcal{O}_K/\mathfrak{p}^n \quad \text{and} \quad \mathcal{O}_K^\times \simeq \varprojlim_n \mathcal{O}_K^\times/(1+\mathfrak{p}^n)$$

are complete filtrations.

PROPOSITION 2.9. *Let $f\colon A \to B$ be a homomorphism of completely filtered abelian groups, i.e., $f(F_n A) \subset F_n B$ for each $n \geq 0$. If the induced map*

$$F_n A / F_{n+1} A \to F_n B / F_{n+1} B$$

is surjective (resp. injective), then f is surjective (resp. injective).

PROOF. Assume that the associated graded maps are surjective and that both filtrations are complete, as in the explicit proof of Claim 2.5. Suppose we have some $x \in B$, and we'd like to solve the equation $f(y) = x$ for $y \in A$. We can solve the equation $f(y_0) \equiv x \bmod F_1 B$, so that $x - f(y_0) \in F_1 B$. Then, since the associated graded map is surjective by assumption, we can solve the equation $f(\epsilon_1) \equiv x - f(y_0) \bmod F_2 B$, where $\epsilon_1 \in F_1 A$ describes an "error term" lifted from $\mathrm{Gr}_1 A$. Observe that, since f is a homomorphism, we have

$$f(y_1) = f(y_0 + \epsilon_1) = f(y_0) + f(\epsilon_1) \equiv x \bmod F_2 B,$$

where we have defined $y_1 := y_0 + \epsilon_1$. This is an equation of the same form as before, and we may iterate to find a "compatible" system of y_n such that $f(y_n) = x \bmod F_{n+1} B$ for each $n \geq 0$, where by "compatible" we mean that for each n we have $y_n \equiv y_{n+1} \bmod F_{n+1} A$. But then there is an induced element $y \in \varprojlim A/F_n A = A$ corresponding to $(y_0, y_1, \ldots)$ under the inverse limit (note that the y_n stabilize modulo $F_n A$ for large enough n), which satisfies the initial equation $f(y) = x$ since both filtrations are complete by assumption. □

REMARK 2.10. Though simple and abstract, many things (such as the previous claim) can be proved easily with the preceding proposition. The advantage of the approach via Hensel's Lemma is that here we needed to use the fact that the squaring map σ is a homomorphism, which is not true in general. Still, this

approach was able to tell us which elements of $\mathcal{O}_K^\times$ are squares in local fields of odd residual characteristic.

The upshot is that when K is a local field of odd residual characteristic, we have $[K^\times : (K^\times)^2] = 4$ since $[\mathcal{O}_K^\times : (\mathcal{O}_K^\times)^2] = 2$, and similarly for $2\mathbb{Z} \subseteq \mathbb{Z}$, so $K^\times/(K^\times)^2$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as it has a basis $\{\pi, r\} \subset \mathcal{O}_K^\times$, where π is a uniformizer and r is not a square modulo $\mathfrak{p}$ (so certainly π and r don't differ by a square).

We now reformulate the Hilbert symbol in terms of norms over extension fields; in contrast to the original definition, here we will view it asymmetrically. Suppose a is not a square, so that $K(\sqrt{a})$ is a degree 2 extension of K (note that if a is a nonzero square, then we need only understand $K(\sqrt{a})$ to be the corresponding étale extension of K, isomorphic to $K \times K$).

Claim 2.11. *We have $(a, b) = 1$ if and only if b is a norm for the extension $K(\sqrt{a})/K$, i.e., there is some element of $K(\sqrt{a})$ whose norm is b.*

Proof. Assume b is a norm, that is, there exist $\alpha, \beta \in K$ such that

$$\alpha^2 - \beta^2 a = \mathrm{N}(\alpha + \beta\sqrt{a}) = b,$$

hence $\alpha^2 = a\beta^2 + b$. Then if $\alpha \neq 0$, we have

$$a\left(\frac{\beta}{\alpha}\right)^2 + b\left(\frac{1}{\alpha}\right)^2 = 1,$$

so $(a, b) = 1$. If $\alpha = 0$, then $b + \beta^2 a = 0$. Letting

$$x := \frac{1}{2}\left(1 + \frac{1}{a}\right) \quad \text{and} \quad y := \frac{1}{2\beta}\left(1 - \frac{1}{a}\right),$$

we have

$$ax^2 + by^2 = a \cdot \frac{1}{4} \cdot \frac{(a+1)^2}{a^2} + (-\beta^2 a) \cdot \frac{1}{4\beta^2} \cdot \frac{(a-1)^2}{a^2} = \frac{(a+1)^2 - (a-1)^2}{4a} = 1,$$

so again $(a, b) = 1$.

The forward implication is a trivial reversal of the argument for nonzero α. □

We state, without proof, the main result about Hilbert Symbols. It's important that that the image of $L^\times$ under the norm is not too big (not everything), and not too small. We will see that this theorem is equivalent to the non-degeneracy of Hilbert Symbols.

Theorem 2.12. *If L/K is a quadratic extension of local fields, then the norm $\mathrm{N}\colon L^\times \to K^\times$ is a homomorphism, and $\mathrm{N}(L^\times) \subseteq K^\times$ is a subgroup of index 2.*

Example 2.13. Consider $\mathbb{C}/\mathbb{R}$.

LECTURE 3

Norm Groups with Tame Ramification

Let K be a field with $\mathrm{char}(K) \neq 2$. Then

$$\begin{aligned} K^\times/(K^\times)^2 &\simeq \{\text{continuous homomorphisms } \mathrm{Gal}(K) \to \mathbb{Z}/2\mathbb{Z}\} \\ &\simeq \{\text{degree 2 étale algebras over } K\} \end{aligned}$$

which is dual to our original statement in Claim 1.8 (this result is a baby instance of Kummer theory). Note that an étale algebra over K is either $K \times K$ or a quadratic extension $K(\sqrt{d})/K$; the former corresponds to the trivial coset of squares in $K^\times/(K^\times)^2$, and the latter to the coset defined by $d \in K^\times$.

If K is local, then LCFT says that $\mathrm{Gal}^{\mathrm{ab}}(K) \simeq \widehat{K^\times}$ canonically. Combined (as such homomorphisms certainly factor through $\mathrm{Gal}^{\mathrm{ab}}(K)$), we obtain that $K^\times/(K^\times)^2$ is finite and canonically self-dual. This is equivalent to asserting that there exists a "sufficiently nice" pairing

$$(\cdot,\cdot)\colon K^\times/(K^\times)^2 \times K^\times/(K^\times)^2 \to \{1,-1\},$$

that is, one which is *bimultiplicative*, satisfying

$$(a,bc) = (a,b)(a,c), \quad (ab,c) = (a,c)(b,c),$$

and *non-degenerate*, satisfying the condition

$$\text{if } (a,b) = 1 \text{ for all } b, \text{ then } a \in (K^\times)^2.$$

We were able to give an easy definition of this pairing, namely,

$$(a,b) = 1 \iff ax^2 + by^2 = 1 \text{ has a solution in } K.$$

Note that it is clear from this definition that $(a,b) = (b,a)$, but unfortunately neither bimultiplicativity nor non-degeneracy is obvious, though we will prove that they hold in this lecture in many cases. We have shown in Claim 2.11 that a less symmetric definition of the Hilbert symbol holds, namely that for all a,

$$(a,b) = 1 \iff b \text{ is a norm in } K(\sqrt{a})/K = K[t]/(t^2 - a),$$

which if a is a square, is simply isomorphic to $K \times K$ and everything is a norm. At the end of Lecture 2, we made the following claim, and remarked that it was important that this subgroup of norms was "not too big" (not everything) and "not too small," and that K be local.

CLAIM 3.1. *These "good properties," i.e., bimultiplicativity and non-degeneracy, hold for the Hilbert symbol if and only if, for all quadratic extensions L/K, $\mathrm{N}(L^\times) \subseteq K^\times$ is a subgroup of index 2, that is, $K^\times/\mathrm{N}(L^\times) = \mathbb{Z}/2\mathbb{Z}$.*

PROOF. Assume that for all degree two extensions L/K, we have $\mathrm{N}L^\times \subseteq K^\times$ a subgroup of index 2. Let $a \in K^\times$. We'd like to show that

$$(a,\cdot)\colon K^\times \to \{1,-1\} \tag{3.1}$$

is a homomorphism, which is equivalent to the first equation of bimultiplicativity (the other follows by symmetry). If a is a square, then this is clear because its image is identically 1 (we may let $(x, y) = (1/\sqrt{a}, 0)$). If a is not a square, then let $L := K(\sqrt{a})$; by Claim 2.11, we know that $(a, b) = 1$ if and only if $b \in \mathrm{N}(L^\times)$. Now, the Hilbert symbol with a factors as

$$K^\times \twoheadrightarrow K^\times/\mathrm{N}L^\times \simeq \{1, -1\},$$

where the isomorphism is canonical because both groups have order 2; we are using the fact that the group of norms has index 2 to construct the final bijection of order-2 groups preserving the identity, since otherwise the quotient would be too big. The projection is trivially a homomorphism.

Now, to show non-degeneracy, let $a \notin (K^\times)^2$. Then there exists some $b \in K^\times$ which is not a norm from $L := K(\sqrt{a})$, which is true if and only if $(a, b) = -1$, so non-degeneracy holds by contrapositive.

To show the converse, observe that if $a \notin (K^\times)^2$, then the map in (3.1) is surjective by non-degeneracy, and a homomorphism by bimultiplicativity. Hence its kernel, which is $\mathrm{N}(K(\sqrt{a})^\times) \subseteq K^\times$, must have index $\#\{1, -1\} = 2$. □

Example 3.2. Again, the basic case is $\mathbb{C}/\mathbb{R}$, where the group of norms is just $\mathbb{R}$, which has index 2.

Now it remains to show the following:

Theorem 3.3. *If L/K is a quadratic extension of local fields with $\mathrm{char}(K) \neq 2$, then $\mathrm{N}L^\times \subseteq K^\times$ is a subgroup of index 2.*

Note that the following proof does not cover the ramified case in residual characteristic 2.

Proof. Let $L := K(\sqrt{d})$ (where d is as a was before), so that L only depends on d up to multiplication by squares. Then we have two cases: where $v(d) = 0$, which is true if and only if $\mathcal{O}_K^\times$, and where $v(d) = 1$, which is true if and only if d is a uniformizer (as we can repeatedly cancel factors of π^2; note here v is the valuation as usual).

Case 1. Here d is a square, and $\sqrt{d} \in \mathcal{O}_K^\times$. This extension is not necessarily unramified, but we'll only do the unramified case and leave the ramified case for next week. An example of ramification is $\mathbb{Q}_2(\sqrt{3})/\mathbb{Q}_2$ (or $\mathbb{Q}_2(\sqrt{2})$, $\mathbb{Q}_2(\sqrt{-1})$, etc.); the extension $\mathbb{Q}_2(\sqrt{5})/\mathbb{Q}_2$ is unramified. We need the following:

Claim 3.4. *$\mathrm{N}(\mathcal{O}_L^\times) = \mathcal{O}_K^\times$, and more generally, $x \in K^\times$ is a norm if and only if $v(x)$ is even (so uniformizers in K are not norms).*

Proof. We make use of the "filtration trick." We have the following filtrations, which are preserved by the norm homomorphism:

$$\begin{array}{ccccccc} \mathcal{O}_L^\times & \supseteq & 1 + \mathfrak{p}_L & \supseteq & 1 + \mathfrak{p}_L^\times & \supseteq & \cdots \\ \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \\ \mathcal{O}_K^\times & \supseteq & 1 + \mathfrak{p}_K & \supseteq & 1 + \mathfrak{p}_K^\times & \supseteq & \cdots. \end{array}$$

On the associated graded terms, we first have

$$\begin{array}{ccc} \mathcal{O}_L^\times/(1+\mathfrak{p}_L) & \xrightarrow{\mathrm{N}} & \mathcal{O}_K^\times/(1+\mathfrak{p}_K) \\ \| & & \| \\ k_L^\times & \xrightarrow{\mathrm{N}} & k_K^\times. \end{array}$$

Since we are in the unramified case, k_L/k_K is a degree-two extension like L/K. To show that the norm map is surjective on the associated graded terms, we can show that it is surjective on the residue fields, that is:

Claim 3.5. *The norm map*

$$\mathrm{N}\colon \mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times, \quad x \mapsto x^{q+1} = \mathrm{Frob}(x)\cdot x,$$

is surjective (note that since $\mathrm{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q) \simeq \mathbb{Z}/2\mathbb{Z}$*,* $x \mapsto x^q$ *is an automorphism fixing* $\mathbb{F}_q$*; in a Galois extension, the field norm is defined as the product of all Galois conjugates of an element).*

Proof 1. The unit group of a finite field must be cyclic, so the map corresponds to

$$\mathbb{Z}/(q^2-1)\mathbb{Z} \to \mathbb{Z}/(q-1)\mathbb{Z} \subseteq (q^2-1)\mathbb{Z}, \quad n \mapsto (q+1)n.$$

□

Proof 2 (for $p \neq 2$). If $x \in \mathbb{F}_q^\times$, then $x = \mathrm{N}(\sqrt{-x})$, and $\sqrt{-x} \in \mathbb{F}_{q^2}^\times$ since $\mathbb{F}_{q^2}$ is the unique degree two extension of $\mathbb{F}_q$. □

Proof 3. We have $\#\mathbb{F}_{q^2}^\times = q^2-1$, $\#\mathbb{F}_q^\times = q-1$, and $\#\mathrm{Ker}(\mathrm{N}) \leq (q^2-1)/(q-1) = q+1$, but the polynomial $x^{q+1}-1$ has exactly $q+1$ roots in $\overline{\mathbb{F}}_q$ since $\mathbb{F}_{q^2}/\mathbb{F}_q$ is a separable extension (finite fields are perfect). □

Thus, the map on the first associated graded term Gr_0 is surjective. On subsequent terms, we have

$$\begin{array}{ccc} (1+\mathfrak{p}_L^n)/(1+\mathfrak{p}_L^{n+1}) & \xrightarrow{\mathrm{N}} & (1+\mathfrak{p}_K^n)/(1+\mathfrak{p}_K^{n+1}) \\ \| & & \| \\ k_L & \xrightarrow{\mathrm{T}} & k_K. \end{array}$$

To check that this diagram commutes, note that because we have assumed that L/K is unramified, π is also a uniformizer of L (for instance $\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p$ is a ramified extension, and p is no longer a uniformizer of $\mathbb{Q}_p(\sqrt{p})$). Thus, under the norm map, we have

$$1+a\pi^n \xmapsto{\mathrm{N}} (1+a\pi^n)(1+\sigma a\pi^n) = 1+(a+\sigma a)\pi^n + a\sigma a\pi^{2n} \equiv 1+\mathrm{T}a\pi^n \bmod \pi^{n+1}.$$

Again, we make the following claim:

Claim 3.6. *The trace map*

$$\mathrm{T}\colon \mathbb{F}_{q^2} \to \mathbb{F}_q, \quad x \mapsto x + x^q = x + \mathrm{Frob}(x)$$

is surjective.

Proof 1. The kernel of the trace map corresponds to the roots of the Artin–Schreier polynomial $x^q + x$, which is separable, and therefore has q roots, implying $\#\mathrm{Ker}(\mathrm{T}) = q$ and $\#\mathrm{Coker}(\mathrm{T}) = q^2/q = q = \#\mathbb{F}_q$. □

PROOF 2. If q is prime to 2, then for any $x \in \mathbb{F}_q$, we have $x = \mathrm{T}(x/2)$ (proceed as above). Otherwise, if $q = 2^r$, then over $\mathbb{F}_2$, $x^2 + x + 1$ is the only monic irreducible polynomial, and $\mathbb{F}_4$ is the splitting field of this polynomial. In general, for the extension $\mathbb{F}_{2^{n+1}}/\mathbb{F}_{2^n}$, the splitting polynomial is $x^2+x+\alpha$, where we choose some α for which it's irreducible. This works for precisely half of the choices for α because the additive homomorphism

$$\mathbb{F}_{2^n} \xrightarrow{x \mapsto x^2+x} \mathbb{F}_{2^n}$$

has kernel $\mathbb{F}_2$, and therefore its image is of index 2. Any root of these polynomials will have trace 1, since they are monic, and to get an element of any other trace, simply multiply by any element of $\mathbb{F}_{2^n}$ (as the trace map is $\mathbb{F}_{2^n}$-linear). □

PROOF 3. The trace map on an extension L/K is surjective if and only if the extension is separable, which is true in this case because finite fields are perfect. □

Thus, since both the trace and norm maps are surjective for finite fields, the norm map is surjective on all associated graded terms, which by Proposition 2.9, implies that the norm map is surjective on $\mathcal{O}_L^\times$, which proves the claim. □

Now, to complete the proof of Case 1, we'd like to show that $x \in K^\times$ is a norm if and only if its valuation is even. To this end, observe that for any $y \in L^\times$, we have $N(y) = y \cdot \sigma y$, and $v(y\sigma(y)) = 2v(y)$, since $\mathrm{Gal}(L/K)$ preserves valuations. For the converse direction, simply note that π^2 is a norm. Hence if $v(d) = 0$, then $\mathrm{N}L^\times \subseteq K^\times$ is a subgroup of index 2, as desired.

Case 2. Here $v(d) = 1$, and again, $\mathrm{char}(K) \neq 2$. This ensures tame ramification, since we are working with a quadratic extension (the ramification index is not divisible by p; we will handle the wildly ramified case (where it is divisible by p) in the next lecture. We claim that $\mathrm{N}(\mathcal{O}_L^\times) \subseteq \mathcal{O}_K^\times$ has index 2 (explicitly, that $\mathrm{N}(\mathcal{O}_L^\times) = (\mathcal{O}_K^\times)^2$), and there exists some $\pi \in \mathcal{O}_K$ that is both a uniformizer and a norm. Clearly, this suffices to show that the group of norms of $L^\times$ has index 2 in $K^\times$.

Let $L := K(\sqrt{d})$, where $v(d) = 1$ and thus d is not a square. Then $N(\alpha + \beta\sqrt{d}) = \alpha^2 - d\beta^2$, and if $x \in (\mathcal{O}_K^\times)^2$, then $x \in N(\sqrt{x})$, so x is a norm. Conversely,

$$v(\alpha^2 - d\beta^2) = 0 = \min\{v(\alpha^2), v(\beta^2 + 1)\} = v(\alpha^2),$$

since the former is even and the latter odd, hence the two are unequal. It follows that $\alpha, \beta \in \mathcal{O}_K^\times$, so $x = \alpha^2 - d\beta^2$ is a square mod $\mathfrak{p}$, and this is true if and only if x is a square in $\mathcal{O}_K^\times$. Finally, since $-d = N(\sqrt{d})$, it follows that there exists a uniformizer of K that is a norm.

So the upshot is that $x \in K^\times$ is a norm for $K(\sqrt{d})$ if and only if $(-d)^{-v(x)}x$, an integral unit, is a square mod $\mathfrak{p}$, so the theorem holds in this case. □

We conclude that we can treat the case of tame ramification (which, for our purposes, includes the unramified case) by guessing explicitly what $\mathrm{N}L^\times \subseteq K^\times$ is. Wild ramification is much trickier. All of this amounts to explicit formulae for the Hilbert symbol, as we saw on Problem 2 of Problem Set 1. There is also such a formula for $\mathbb{Q}_2$, and with elbow grease, we can prove that all "good" properties of the Hilbert symbol hold in this case (see for instance [**Ser73**]).

LECTURE 4

GCFT and Quadratic Reciprocity

Last time, we reduced non-degeneracy and bimultiplicativity of the Hilbert symbol $(\cdot,\cdot)$ to showing that for all quadratic extensions L/K, with K a local field, $\mathrm{N}L^\times \subseteq K^\times$ is a subgroup of index 2. We showed that this holds for unramified extensions and when $p = \mathrm{char}(\mathcal{O}_K/\mathfrak{p})$ is odd (the case when $p = 2$ was more-or-less shown in Problem 1 of Problem Set 1). In this lecture, we will perform a similar analysis in the global setting, that is, for $F = \mathbb{Q}$.

We compare the following two facts: first, that

$$\mathrm{Gal}^{\mathrm{ab}}(\mathbb{Q})/2 \simeq \mathrm{Hom}(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2, \{1,-1\}) = \mathrm{Hom}(\mathbb{Q}^\times, \{1,-1\}),$$

where the set of primes and -1 form a basis for this group as an $\mathbb{F}_2$-vector space. And second, that CFT predicts that

$$\mathbb{A}_\mathbb{Q}^\times/\mathbb{Q}^\times \simeq \mathrm{Gal}^{\mathrm{ab}}(\mathbb{Q})$$

as a canonical isomorphism of profinite completions. Thus, we expect

$$\mathrm{Hom}(\mathbb{Q}^\times, \{1,-1\}) = \mathrm{Gal}^{\mathrm{ab}}(\mathbb{Q})/2 \simeq \mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2. \tag{4.1}$$

Recall the following definition:

Definition 4.1. The *ring of adèles* is defined as

$$\mathbb{A}_\mathbb{Q} := \varinjlim_S \prod_{p\notin S} \mathbb{Z}_p \times \prod_{p\in S} \mathbb{Q}_p,$$

where the S are finite sets of places (primes and ∞) of $\mathbb{Q}$, ordered by inclusion, and $\mathbb{Q}_\infty = \mathbb{R}$. The *group of idèles* is the multiplicative group of the ring of adèles,

$$\mathbb{A}_\mathbb{Q}^\times = \varinjlim_S \prod_{p\in S} \mathbb{Z}_p^\times \times \prod_{p\in S} \mathbb{Q}_p^\times,$$

with S as before.

Example 4.2. We have $\widehat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$, where p ranges over all primes, and $\widehat{\mathbb{Z}}\times\mathbb{R} \subseteq \mathbb{A}_\mathbb{Q}$ embedded as a subring, in which we may diagonally embed any $n \neq 0$. Similarly, $\widehat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$, and $\widehat{\mathbb{Z}}^\times \times \mathbb{R}^\times \subseteq \mathbb{A}_\mathbb{Q}^\times$. However, 2 and $1/2$ won't be in $\widehat{\mathbb{Z}}^\times \times \mathbb{R}^\times$ as they aren't in $\mathbb{Z}_2^\times$, and the same holds for any rational number. If we add the rationals in to compensate, i.e., $\widehat{\mathbb{Z}}^\times \times \mathbb{Q}^\times \times \mathbb{R}^\times \to \mathbb{A}_\mathbb{Q}^\times$, then -1 is repeated in $\mathbb{Q}^\times$ and $\mathbb{R}^\times$, so we must replace $\mathbb{R}^\times$ with $\mathbb{R}_{>0}$ (see Problem 1 of Problem Set 2).

We'd like a pairing $\mathbb{A}_{\mathbb{Q}}^{\times} \times \mathbb{Q}^{\times} \to \{1, -1\}$ from the idèles and rationals to $\mathbb{Z}/2\mathbb{Z}$, that should factor through the squares:

$$\begin{array}{ccc} \mathbb{A}_{\mathbb{Q}}^{\times} \times \mathbb{Q}^{\times} & \longrightarrow & \{1, -1\} \\ \downarrow & \nearrow & \\ \mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times} / (\mathbb{A}_{\mathbb{Q}}^{\times})^2 \times \mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^2. & & \end{array}$$

Here the copy of $\mathbb{Q}^{\times}$ in the left term of the product is the diagonally embedded "principal idèles," through which this pairing should also factor in order to realize (4.1). This map should induce an isomorphism (which is, in a sense, "non-degeneracy")

$$\mathbb{Q}^{\times} \backslash \mathbb{A}_{\mathbb{Q}}^{\times} / (\mathbb{A}_{\mathbb{Q}}^{\times})^2 \xrightarrow{\sim} \mathrm{Hom}(\mathbb{Q}^{\times} / (\mathbb{Q}^{\times})^2, \{1, -1\}),$$

that is, the map shouldn't be identically one or "anything crazy like that."

So fix

$$x = (x_p)_p \in \mathbb{A}_{\mathbb{Q}}^{\times},$$

where p may be either prime or ∞, and define the desired pairing by

$$y \mapsto \prod_p (x_p, y)_p,$$

where we are regarding y as a p-adic unit, and $(\cdot, \cdot)_p$ denotes the Hilbert symbol at p, i.e., on $\mathbb{Q}_p$. Now, it's not even clear *a priori* that this infinite product is well-defined, and for this we introduce the following lemma:

LEMMA 4.3. *$(x_p, y)_p = 1$ for all but finitely many p.*

PROOF. Indeed, for all but finitely many p, we have $p \neq 2, \infty$, $x_p \in \mathbb{Z}_p^{\times}$, and $y \in \mathbb{Z}_p^{\times}$, which imply that $(x_p, y)_p = 1$ by the identities shown with the tame symbol (since the valuations of x_p and y are both 0). □

Now, this map is definitely bimultiplicatives, as each term is, and similarly definitely factors modulo squares, i.e., it is a map

$$\mathbb{A}_{\mathbb{Q}}^{\times} / (\mathbb{A}_{\mathbb{Q}}^{\times})^2 \to \{1, -1\}$$

since if we multiply by squares on either side, the Hilbert symbols don't change. Thus, this map factors modulo $\mathbb{Q}^{\times}$ on the first factor if and only if the following claim holds:

CLAIM 4.4. *For all $x, y \in \mathbb{Q}^{\times}$, we have $\prod_p (x, y)_p = 1$ (that is, this map is invariant by multiplying by a factor of $\mathbb{Q}^{\times}$ in the first factor, which by bimultiplicativity, means we pick up such a factor).*

REMARK 4.5. This is true for all number fields (using general places). In this lecture, we will see how this represents (approximately) a repackaging of quadratic reciprocity. This property is a sort of "conspiring" between the primes: "the p-adic fields are talking to each other behind the scenes; even though they are separate, they ensure that the product is 1." The word for such "conspiracies" is "reciprocity law."

PROOF (OF CLAIM). First of all, since the map is invariant under multiplication by squares, we can assume $x = \pm p_1 \cdots p_r$ and $y = \pm q_1 \cdots q_s$. Then bimultiplicativity implies that we can take $x \in \{-1, 2, p\}$ and $y \in \{-1, 2, q\}$, where p and

q denote odd primes. We prove the claim for the case were p and q are distinct odd primes.

We'd like to show that

$$(p,q)_\infty \times \prod_\ell (p,q)_\ell = 1,$$

where ℓ ranges over all primes. The first term is 1 since both p and q are positive, and we can likewise ignore ℓ on odd primes distinct from p and q, so this reduces to showing that

$$(p,q)_2 \cdot (p,q)_p \cdot (p,q)_q = 1.$$

Now, as shown on Problem 2(b) of Problem Set 1,

$$(p,q)_p = \left(\frac{(-1)^{v_p(p)v_p(q)} \frac{q^{v_p(p)}}{p^{v_p(q)}}}{p} \right) = \left(\frac{q}{p}\right),$$

and similarly, $(p,q)_q = \left(\frac{p}{q}\right)$, where we recall that

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{if } n \text{ is a square mod } p, \\ -1 & \text{otherwise,} \end{cases}$$

where n is prime to p. Furthermore,

$$(p,q)_2 := (-1)^{\varepsilon(p)\varepsilon(q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

which is equal to 1 unless $p \equiv q \equiv 3 \bmod 4$. Thus, we have reduced to elementary congruence conditions, and this is precisely the statement of quadratic reciprocity. □

Remark 4.6. Quadratic reciprocity allows for efficient computation of Legendre symbols via successive reduction.

Proof (of Quadratic Reciprocity). Regard the Legendre symbol as a map

$$\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{1,-1\},$$

and reinterpret $\mathbb{F}_p^\times$ as $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, so that this is the unique nontrivial quadratic character of the Galois group. This character is encoded in a unique quadratic subfield of $\mathbb{Q}(\zeta_p)$ (over $\mathbb{Q}$). We'd like to write this field as $\mathbb{Q}(\sqrt{d})$ for some d. We want some

$$x = \sum_{n=1}^{p-1} x_n \zeta_p^n \in \mathbb{Q}(\zeta_p)$$

such that for all $m \in (\mathbb{Z}/p\mathbb{Z})^\times$,

$$\sum_{n=1}^{p-1} x_n \zeta_p^{mn} = m \cdot x = \left(\frac{m}{p}\right) \cdot x = \sum_{n=1}^{p-1} \left(\frac{m}{p}\right) x_n \zeta_p^n,$$

as a Galois action, since $x_n \in \mathbb{Q}$ is fixed and the action is $\zeta_p \mapsto \zeta_p^m$. That is, the Galois group translates x by ± 1, implying that $x \in \mathbb{Q}(\zeta_d)$, our quadratic subfield.

This equality implies that $x_{mn} = \left(\frac{m}{p}\right) \cdot x_m$. By repeatedly solving this equation, we end up with this element (called a "Gauss sum")

$$x = G := \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n.$$

We know by design that $G^2 \in \mathbb{Q}$, but now we'd like to know which (in fact, we will see that it is either p or $-p$).

Suppose that $\chi\colon k^\times \to \mathbb{C}^\times$ is a multiplicative character, and $\psi\colon k \to \mathbb{C}^\times$ is an additive character, where K is any finite field. Let

$$G_{\chi,\psi} := \sum_{x \in k^\times} \chi(x)\psi(x).$$

REMARK 4.7. As a fun analogy, the gamma function is defined by

$$\Gamma(\chi_s) := \int_{\mathbb{R}_{>0}} e^{-t} t^s \, \frac{dt}{t},$$

and this is like a Gauss sum with $\psi(t) := e^{-t}$ and $\chi_s(t) := t^s$.

We need the following lemma:

LEMMA 4.8. *$G_{\chi,\psi} \cdot G_{\chi^{-1},\psi^{-1}} = \#k$ if χ and ψ are both not the identity.*

PROOF. We have

$$\begin{aligned} G_{\chi,\psi} \cdot G_{\chi^{-1},\psi^{-1}} &= \sum_{x,y \in k^\times} \chi(x)\psi(x)\chi^{-1}(y)\psi^{-1}(y) \\ &= \sum_{x,y \in k^\times} \chi(x/y)\psi(x-y) \\ &= \sum_{z,y \in k^\times} \chi(z)\psi(y(z-1)), \end{aligned}$$

where we have made the change of variables $z := x/y$, so that $x = zy$. Now, if $z \neq 1$, then $y(z-1)$ assumes all values in $k^\times$, so the fact that $\sum_{w \in k} \psi(w) = 0$ holds (by non-degeneracy). Thus, we obtain

$$\begin{aligned} G_{\chi,\psi} \cdot G_{\chi^{-1},\psi^{-1}} &= \sum_{z \in k^\times} \chi(z) \sum_{y \in k^\times} \psi(y(z-1)) \\ &= \sum_{z \in k^\times \setminus \{1\}} \chi(z)(-\psi(0)) + \chi(1) \sum_{y \in k^\times} \psi(0) \\ &= \chi(1) + 1 \cdot \sum_{y \in k^\times} 1 \\ &= 1 + \#k^\times \\ &= \#k, \end{aligned}$$

since $\sum_{w \in k^\times} \chi(w) = 0$ similarly. □

Now, we'd like to know what $G_{\chi^{-1},\psi^{-1}}$ is for ψ corresponding to a power of ζ_p and χ the multiplicative Legendre character. We have

$$G_{\chi^{-1},\psi^{-1}} = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{-n}$$

$$\begin{aligned}
&= \sum_{n=1}^{p-1} \left(\frac{-n}{p}\right) \zeta_p^n \\
&= \left(\frac{-1}{p}\right) \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n \\
&= \left(\frac{-1}{p}\right) G.
\end{aligned}$$

Thus,

$$G_{\chi,\psi} \cdot G_{\chi^{-1},\psi^{-1}} = G \cdot \left(\frac{-1}{p}\right) G = p,$$

and so

$$G^2 = \left(\frac{-1}{p}\right) \cdot p = (-1)^{(p-1)/2} \cdot p,$$

and G is the square root of either p of $-p$, depending on the condition.

Now, recall that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is unramified at $q \neq p$, and that we have an isomorphism

$$\begin{aligned}
\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) &\simeq (\mathbb{Z}/p\mathbb{Z})^\times, \\
\mathrm{Frob}_q &\mapsto q \bmod p.
\end{aligned}$$

Thus, $\left(\frac{q}{p}\right) = 1$ if and only if Frob_q fixes G; in fact,

$$\begin{aligned}
\mathrm{Frob}_q(G) = \mathrm{Frob}_q \left(\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^n\right) &= \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{qn} = \sum_{n=1}^{p-1} \left(\frac{n/q}{p}\right) \zeta_p^n \\
&= \sum_{n=1}^{p-1} \left(\frac{qn}{p}\right) \zeta_p^n = \sum_{n=1}^{p-1} \left(\frac{q}{p}\right)\left(\frac{n}{p}\right) \zeta_p^n \\
&= \left(\frac{q}{p}\right) G.
\end{aligned}$$

Moreover,

$$G^{q-1} = (G^2)^{(q-1)/2} = ((-1)^{(p-1)/2} \cdot p)^{(q-1)/2} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \bmod q,$$

so

$$\left(\frac{q}{p}\right) G^2 = G^{q+1} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) G^2 \bmod q.$$

After dividing through by $G^2 = (-1)^{(p-1)/2} \cdot p$ (which is invertible modulo q), we have

$$\left(\frac{q}{p}\right) \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \bmod q,$$

that is,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

as desired. □

LECTURE 5

Non-Degeneracy of the Adèle Pairing and Exact Sequences

Recall that we wanted a non-degenerate pairing, for which

$$\begin{aligned} \mathbb{Q}^\times \backslash \mathbb{A}_\mathbb{Q}^\times / (\mathbb{A}_\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 &\to \{1, -1\} \\ ((x_p), r) &\mapsto \prod_p (x_p, r)_p \end{aligned} \tag{5.1}$$

was a candidate (as before, p ranges over all primes and ∞). Well-definedness of this pairing reduced to the reciprocity law

$$\prod_p (x, y)_p = 1 \quad \text{for} \quad x, y \in \mathbb{Q}^\times.$$

We saw that when $x = p$ and $y = q$ were odd primes, this reduced to quadratic reciprocity,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

which we proved by considering the character

$$\chi \colon \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \xrightarrow{\left(\frac{\cdot}{p}\right)} \{1, -1\}.$$

We saw that this corresponded to a unique quadratic subextension of $\mathbb{Q}(\zeta_p)$,

$$\mathbb{Q}(\sqrt{\pm p}) = \mathbb{Q}\left(\sqrt{\left(\frac{-1}{p}\right)p}\right),$$

where the key point was that the Gauss sum

$$G := \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a = \sqrt{\left(\frac{-1}{p}\right)p}.$$

More generally, if $F/\mathbb{Q}$ is Galois with Galois group G, and a prime q of $\mathbb{Q}$ is unramified, then $[\mathrm{Frob}_q] \mapsto [1] \in G$ (where these are conjugacy classes) if and only if q splits in F. Thus,

$$\left(\frac{q}{p}\right) = 1 \iff \left(\frac{\left(\frac{-1}{p}\right)p}{q}\right) = 1,$$

since the right side is equivalent to the splitting of q in the extension $\mathbb{Q}(\sqrt{\pm p})$, which implies that

$$\left(\frac{q}{p}\right) = \left(\frac{\left(\frac{-1}{p}\right)p}{q}\right) = \left(\frac{\left(\frac{-1}{p}\right)}{q}\right)\left(\frac{p}{q}\right) = \left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

which yields the desired result.

Similarly, we may obtain the reciprocity result in other cases, such as:

PROPOSITION 5.1. *We have*

$$\prod_p (2,\ell)_p = 1,$$

where ℓ is an odd prime and p ranges over all primes (note that $(2,\ell)_\infty = 1$ trivially).

PROOF. As before, $(2,\ell)_p = 1$ if $p \neq 2, \ell$, and using the tame symbol,

$$(2,\ell)_\ell = \left(\frac{(-1)^{v(\ell)v(2)} \frac{2^{v(\ell)}}{\ell^{v(2)}}}{\ell} \right) = \left(\frac{2}{\ell} \right).$$

By the formula obtained in Problem 2(d) of Problem Set 1, we have

$$(2,\ell)_2 = (-1)^{\epsilon(1)\epsilon(\ell)+v(2)\theta(\ell)+v(\ell)\theta(1)} = (-1)^{\theta(\ell)},$$

where

$$(-1)^{\theta(\ell)} := \begin{cases} 1 & \text{if } \ell \equiv 1, -1 \bmod 8, \\ -1 & \text{if } \ell \equiv 3, -3 \bmod 8, \end{cases}$$

which corresponds to the canonical isomorphism from ℓ^2 in $\mathbb{Z}/16\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$. Thus, we'd like to show that

$$\left(\frac{2}{\ell} \right) = (-1)^{\theta(\ell)}.$$

To know whether or not 2 is a square modulo ℓ, we'd like a convenient expression for $\sqrt{2}$, i.e., a cyclotomic embedding of $\mathbb{Q}(\sqrt{2})$ (in which ℓ splits if and only if $\left(\frac{2}{\ell}\right) = 1$). Recall that if ζ_8 is a primitive eighth root of unity, then we may take $\zeta_8 = \sqrt{2}/2 + i\sqrt{2}/2$, and so

$$\zeta_8 + \zeta_8^{-1} = \zeta_8 + \bar{\zeta}_8 = 2\,\mathrm{Re}(\zeta_8) = \sqrt{2}.$$

Algebraically, we may show this identity by noting that

$$(\zeta_8 + \zeta_8^{-1})^2 + 2 + \zeta_8^2 + \zeta_8^{-2} = 2 + \zeta_4 + \zeta + 4^{-1} = 2,$$

since ζ_4 and ζ_4^{-1} are precisely i and $-i$. This gives $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$, and a character

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)) = (\mathbb{Z}/8\mathbb{Z})^\times \xrightarrow{\chi} \{1, -1\}.$$

We claim that $\left(\frac{2}{\cdot}\right) = \chi = (-1)^{\theta(\cdot)}$. Clearly $\mathrm{Ker}\left((-1)^{\theta(\cdot)}\right) = \{1, -1\}$, and an element $n \in (\mathbb{Z}/8\mathbb{Z})^\times$ is in $\mathrm{Ker}(\chi)$ if and only if it fixes $\sqrt{2} = \zeta_8 + \zeta_8^{-1}$, i.e.

$$\zeta_8 + \zeta_8^{-1} \mapsto \zeta_8^n + \zeta_8^{-n} = \zeta_8 + \zeta_8^{-1},$$

which only holds when $n = 1$ (both terms are fixed) or $n = -1$ (the terms are switched). Thus, the two kernels are the same, and therefore the two functions are equal. □

Note that we could also argue without using Galois groups. If we suppose that $\zeta_8 + \zeta_8^{-1} \in \overline{\mathbb{F}}_\ell$, then so show that $\zeta_8 + \zeta_8^{-1} \in \mathbb{F}_\ell$, we must simply check that $\zeta_8 + \zeta_8^{-1} = (\zeta_8 + \zeta_8^{-1})^\ell = \zeta_8^\ell + \zeta_8^{-\ell}$, i.e., it is fixed under the action of the Frobenius element, and thus we obtain the same conditions as before.

Other symbols are relatively tedious to check, for instance, $\prod_p (2,2)_p = 1$ is simple as $(2,2)_2 = 1$ as shown in Problem 2(d) of Problem Set 1, and $\prod_p (-1,\ell)_p = 1$ is

solved by noting that $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Thus, we have checked the well-definedness of our initial pairing (5.1). We'd now like to check that our pairing is non-degenerate. Note that we don't really need reciprocity for this, as the arguments are easier.

PROPOSITION 5.2. *The map*

$$\chi\colon \mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2 \xrightarrow{\sim} \mathrm{Hom}(\mathbb{Q}^\times, \{1,-1\}) \simeq \mathrm{Gal}_2(\mathbb{Q})$$

defined in (5.1) is an isomorphism (note that it does not matter that the pairing defines maps from $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ as the homomorphisms on the right absorb squares).

PROOF. In Problem 1(a) of Problem Set 2, we showed that

$$\mathbb{A}_\mathbb{Q}^\times = \widehat{\mathbb{Z}}^\times \times \mathbb{R}_{>0} \times \mathbb{Q}^\times,$$

where the first two terms are embedded via local places and the last term is embedded diagonally. Modding out by $\mathbb{Q}^\times$ removes the last term, and modding out by squares removes the second term, so we obtain

$$\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2 = \prod_p \mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2 \tag{5.2}$$

by the Chinese Remainder Theorem, where p ranges over all primes; when p is odd, $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ is an order-2 group generated by any quadratic non-residue, and $\mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \simeq (\mathbb{Z}/8\mathbb{Z})^\times$ has order 4 and is generated by -1 and 5. Also,

$$\mathbb{Q}^\times/(\mathbb{Q}^\times)^2 = \{\pm p_1\cdots p_r : p_i \text{ primes}\} = \mathbb{Z}/2\mathbb{Z} \times \bigoplus_p \mathbb{Z}/2\mathbb{Z}$$

with p as before, where the first copy of $\mathbb{Z}/2\mathbb{Z}$ corresponds to sign. We will see that, dualizing, these copies of $\mathbb{Z}/2\mathbb{Z}$ all (nearly) match up.

Suppose p is an odd prime, and let r be a quadratic non-residue at p, i.e., a non-trivial element of $\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$. Then

$$(\chi(r)(\pm q))_p = (r, \pm q)_p = \left(\frac{r^{v(\pm q)}/(\pm q)^{v(r)}}{p}\right) = \begin{cases} 1 & \text{if } q \neq p, \\ -1 & \text{if } q = p, \end{cases}$$

is the value of χ on the pth term of $\mathbb{Q}^\times\backslash\mathbb{A}_\mathbb{Q}^\times/(\mathbb{A}_\mathbb{Q}^\times)^2$, where q is a prime. For the last basis element, we have $\chi(r)(-1) = 1 = (r,-1)_p$. Thus, the obvious (topological) basis elements at p match up; now we must ask what happens at $p = 2$. A natural guess is the idèle defined by $r = -1$ or $r = 5$ at 2 and $r = 1$ elsewhere, since 5 corresponds to the unique unramified quadratic extension of $\mathbb{Q}_2$ by Problem 2(b) of Problem Set 2. Computing yields

$$\begin{aligned} \chi(5,1,1,\ldots)(q) &= (5,q)_2 = 1, \\ \chi(5,1,1,\ldots)(-1) &= (5,-1)_2 = 1, \\ \chi(5,1,1,\ldots)(2) &= (5,2)_2 = (-1)^{\theta(5)} = -1, \end{aligned}$$

so indeed, this basis element perfectly matches up to the basis element at 2. Here we have denoted idèles by tuples whose coordinates are taken with respect to the isomorphism (5.2), with primes ordered as usual. Then

$$\chi(-1,1,1,\ldots)(-1) = -1 = (-1,-1)_2$$

completes the proof. Now, the bases actually don't perfectly match up, since pairing with another odd prime p yields symbols corresponding to whether or not -1 is

a square modulo p, but we can easily express one basis in terms of the other by correcting for the $(-1,1,1,\ldots)$ basis element, using "upper triangular matrices" (essentially, we have an infinite matrix with ones along the diagonal, except at $(-1,1,1,\ldots)$, which corresponds to a more complicated element in the basis given for $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$).

Here's a slightly more serious argument. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \prod_{p\neq 2} \mathbb{Z}/2\mathbb{Z} & \longrightarrow & \mathbb{Q}^\times \backslash \mathbb{A}_{\mathbb{Q}}^\times / (\mathbb{A}_{\mathbb{Q}}^\times)^2 & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow \simeq & & \downarrow & & \downarrow \simeq & & \\ 0 & \longrightarrow & \{\varphi \colon \mathbb{Q}^\times \to \mathbb{Z}/2\mathbb{Z} \mid \varphi(-1) = 1\} & \longrightarrow & \mathrm{Hom}(\mathbb{Q}^\times, \mathbb{Z}/2\mathbb{Z}) & \xrightarrow{\varphi \mapsto \varphi(-1)} & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 0. \end{array}$$

The first copy of $\mathbb{Z}/2\mathbb{Z}$ corresponds to the idèle $(5,1,1,\ldots)$, and the other copies correspond to quadratic non-residues at each p; in the rightmost copy of $\mathbb{Z}/2\mathbb{Z}$, we obtain the image of $(-1,1,1,\ldots)$. The maps into $\mathbb{Z}/2\mathbb{Z}$ are both quotients, and the vertical map on the right is an isomorphism because it is non-trivial; the vertical map on the left is an isomorphism because everything matches up perfectly as we saw earlier. Thus, the map in the middle is an isomorphism, as desired. □

Now we return to the problem of showing that for any quadratic extension of local fields L/K, we have $\#(K^\times/\mathrm{N}L^\times) = 2$. Recall that this statement is equivalent to the bimultiplicativity and non-degeneracy of the Hilbert symbol, and that we've proved this in the case of odd primes and unramified and tamely ramified extensions, but we couldn't prove it for wildly ramified extensions or for extensions over $\mathbb{Q}_2$, aside from $\mathbb{Q}_2$ itself. Our present goal will be to prove this more generally: that is, to show that if L/K is a cyclic extension of degree n, i.e., that it is Galois with group $\mathbb{Z}/n\mathbb{Z}$, then $\#(K^\times/\mathrm{N}L^\times) = n$. To further place this in a more general context, if L/K is a finite abelian extension, then we actually expect

$$\mathrm{Gal}(L/K) \simeq K^\times/\mathrm{N}L^\times$$

canonically, so we expect more than an equality of numbers. We will show this using the methods of exact sequences and homological algebra, to which we now turn.

As it turns out, short exact sequences are really great tools for determining the orders of finite abelian groups. Suppose we have the short exact sequence

$$0 \to M \overset{g}{\hookrightarrow} E \overset{f}{\twoheadrightarrow} N \to 0.$$

Then $M = \mathrm{Ker}(f)$ and $N = \mathrm{Coker}(g) = E/M$; in terms of filtrations, M and N are like the associated graded terms. Indeed, we can think of M and N as the "atoms" and E as a "molecule," whose fine structure determines its "reactions". It's clear that if M and N are finite, then so is E, and $\#E = \#M\#N$. The problem with wild ramification is that we don't have a filtration on $L^\times$.

One problem is that many operations don't preserve short exact sequences. For instance, if $n \geq 1$ is an integer, modding out by n does not preserve $\#(E/nE)$.

Example 5.3. (1) If we have the exact sequence

$$0 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{x \mapsto (x,0)} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \xrightarrow{(x,y) \mapsto y} \mathbb{Z}/n\mathbb{Z} \to 0,$$

then modding out by n preserves it.

(2) If we have the exact sequence

$$0 \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{x \mapsto xn} \mathbb{Z}/n^2\mathbb{Z} \xrightarrow{1 \mapsto 1} \mathbb{Z}/n\mathbb{Z} \to 0,$$

then modding out by n changes the exact sequence to

$$\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \xrightarrow{\mathrm{id}} \mathbb{Z}/n\mathbb{Z} \to 0.$$

We have the same "atoms," but they form a different "molecule." In the last case, the order was n^2 after modding out, whereas here it is n.

A central thesis of homological algebra is that we can correct this by extending exact sequences. Poetically, the altered exact sequence is like visible light; it's missing the infrared spectrum, which we will be able to see by extending the exact sequences. Specifically, this corresponds to n-torsion: $\mathbb{Z}/n^2\mathbb{Z}$ does not has as much n-torsion as $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which is all n-torsion.

For a module M, let $M[n] \subseteq M$ denote $\mathrm{Ker}(n\colon M \to M)$. Then we obtain a longer exact sequence

$$0 \to M[n] \to E[n] \to N[n] \xrightarrow{\delta} M/n \to E/n \to N/n \to 0,$$

where for $x \in N[n]$, $\delta(x) = ny$ for any $y \in E$ with $f(y) = x$; note that $f(ny) = nx = 0$, so $\delta(x) \in M \subseteq E$ as desired. We will show that this is an exact sequence in the next lecture.

LECTURE 6

Exact Sequences and Tate Cohomology

Last time we began discussing some simple homological algebra; our motivation was to compute the order of certain finite abelian groups (in particular, $K^\times/\mathrm{N}(L^\times)$, where L/K is a cyclic extension of local fields). Recall the following definition:

DEFINITION 6.1. A sequence

$$\cdots \to X^{n-1} \xrightarrow{d^n} X^n \xrightarrow{d^{n+1}} X^{n+1} \to \cdots$$

is *exact* if for each n, we have $\mathrm{Ker}(d^{n+1}) = \mathrm{Im}(d^n)$, where we refer to the 'd^i' as *differentials*.

To solve this equation, one typically shows that if d^{n+1} kills an element, then it is in the image of d^n. We saw that for a short exact sequence

$$0 \to M \hookrightarrow E \twoheadrightarrow N \to 0,$$

we have $M = E/N$ and $\#E = \#M \cdot \#N$, so short exact sequences are an effective way of measuring the size of abelian groups. We also saw that for any such short exact sequence and $n \geq 1$, there is a long exact sequence

$$0 \to M[n] \to E[n] \to N[n] \xrightarrow{\delta} M/n \to E/n \to N/n \to 0, \tag{6.1}$$

where we recall that

$$M[n] := \{x \in M : nx = 0\} = \mathrm{Tor}_1(M, \mathbb{Z}/n) = H_1(M \otimes_L \mathbb{Z}/n),$$

which denote the torsion subgroup and first homology group, respectively, and similarly for E and N. The boundary map δ lifts an element $x \in N[n]$ to $\tilde{x} \in E$, so that $n\tilde{x} \in M$ since $nx = 0$ in N, and then maps $n\tilde{x}$ to its equivalence class in M/n. It remains to check the following claims:

CLAIM 6.2. *The boundary map δ is well-defined.*

PROOF. Suppose $\tilde{\tilde{x}}$ is another lift of x. Then $\tilde{x} - \tilde{\tilde{x}} \in M$ as its image in N is zero, hence $n(\tilde{x} - \tilde{\tilde{x}}) \in nM$, so $n\tilde{x} = n\tilde{\tilde{x}}$ in M/nM. □

CLAIM 6.3. *The sequence in (6.1) is exact.*

PROOF. This is clear at all maps aside from the boundary map. If $\delta(x) = n\tilde{x} = 0$ in M/n for some $x \in N[n]$ with lift $\tilde{x} \in E$, then $\tilde{x} \in M$, and therefore $x = 0$ in N. Hence $x \in N[n]$ and so $\tilde{x} \in E[n]$ by exactness. Similarly, if $x \in M/n$ has image zero E/n, then $\tilde{x} = ny$ for some $y \in E$, where $\tilde{x}$ is a lift of x to M. Projecting down to N, we see that $0 = n\bar{y}$ by exactness, and therefore $\bar{y} \in N[n]$. So $ny \in M$, again by exactness, and $\delta(\bar{y}) = ny = x$ as classes in M/n, as desired. □

We have the following useful lemma:

LEMMA 6.4. *Suppose*

$$0 \to X^0 \xrightarrow{d^1} X^1 \xrightarrow{d^2} \cdots \xrightarrow{d^{n-1}} X^{n-1} \xrightarrow{d^n} X^n \to 0$$

is exact, and all X^i are finite. Then

$$\#X^0 \cdot \#X^2 \cdots = \#X^1 \cdot \#X^3 \cdots .$$

PROOF. We proceed by induction on n. The result is clear for $n = 1$, so suppose it holds for $n - 1$. Form the exact sequences

$$0 \to X^0 \to \cdots \to X^{n-1} \xrightarrow{d^{n-1}} \operatorname{Im}(d^{n-1}) \to 0$$

and

$$0 \to \operatorname{Im}(d^{n-1}) \to X^{n-1} \xrightarrow{d^n} X^n \to 0.$$

Suppose n is even. Then

$$\begin{aligned}
\#X^0 \cdot \#X^2 \cdots \#X^n &= \#X^0 \cdot \#X^2 \cdots \#X^{n-1} \cdot \frac{\#X^{n-1}}{\#\operatorname{Im}(d^{n-1})} \\
&= \#X^1 \cdot \#X^3 \cdots \#\operatorname{Im}(d^{n-1}) \cdot \frac{X^{n-1}}{\#\operatorname{Im}(d^{n-1})} \\
&= \#X^1 \cdot \#X^3 \cdots \#X^{n-1},
\end{aligned}$$

by the inductive hypothesis. The proof for odd n is similar. □

DEFINITION 6.5. Let M be an abelian group with M/n and $M[n]$ finite. Then

$$\chi(M) := \chi_n(M) := \frac{\#(M/n)}{\#(M[n])}$$

is the *Euler characteristic* of M.

EXAMPLE 6.6.
(1) If M is finite, then $\chi(M) = 1$. To see this, observe that
$$0 \to M[n] \to M \xrightarrow{n} M \to M/n \to 0$$
is exact, and so by Lemma 6.4, $\#(M[n]) \cdot \#M = \#M \cdot \#(M/n)$.
(2) If $M = \mathbb{Z}$, then $\chi(M) = n$, since $M[n] = 0$ and $M/n = \mathbb{Z}/n$ has order n.

The following lemma is an important fact about Euler characteristics:

LEMMA 6.7. *For a short exact sequence*

$$0 \to M \to E \to N \to 0,$$

if χ exists for two of the three abelian groups, then it exists for the third, and $\chi(M) \cdot \chi(N) = \chi(E)$, where "exists" means that (say for M) M/n and $M[n]$ are both finite.

PROOF. We have an exact sequence

$$0 \to M[n] \to E[n] \to N[n] \to M/n \to E/n \to N/n \to 0.$$

More generally, note that if $X^{n-1} \xrightarrow{d^{n-1}} X^n \xrightarrow{d^n} X^{n+1}$ is exact, then X^n is finite if X^{n-1} and X^{n+1} are, since there is a short exact sequence

$$0 \to \operatorname{Im}(d^{n-1}) = \operatorname{Ker}(d^n) \to X^n \to \operatorname{Im}(d^n) \to 0,$$

where the outer two groups are finite and therefore $\#X^n = \#\mathrm{Ker}(d^n) \cdot \#\,\mathrm{Im}(d^n)$ is too. Thus, all groups in the sequence are finite, and

$$\#(M[n]) \cdot \#(N[n]) \cdot \#(E/n) = \#(E[n]) \cdot \#(M/n) \cdot \#(N/n)$$

by Lemma 6.4, which yields the desired expression. □

As an application, let us compute $\#(K^\times/(K^\times)^n)$. Observe that

$$\chi(K^\times) = \frac{\#(K^\times/(K^\times)^n)}{\#(K^\times[n])},$$

where the denominator is the number of nth roots of unity in K. Moreover, we have an exact sequence

$$0 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

and so by Lemma 6.7, $\chi(K^\times) = \chi(\mathcal{O}_K^\times)\chi(\mathbb{Z}) = n\chi(\mathcal{O}_K^\times)$. Thus, we'd really like to compute $\chi(\mathcal{O}_K^\times)$.

A good heuristic to use is that if $\mathcal{O}_K^\times$ contains some open, that is, finite index, subgroup Γ, then $\Gamma \simeq \mathcal{O}_K^+$, which is true if $\mathrm{char}(K) = 0$ by p-adic exponentials. It then follows that

$$\chi(\mathcal{O}_K^\times) = \chi(\Gamma)\chi(\mathcal{O}_K^\times/\Gamma) = \chi(\Gamma) = \chi(\mathcal{O}_K) \tag{6.2}$$

under addition, since $\mathcal{O}_K^\times/\Gamma$ is finite by assumption. Then $\mathcal{O}_K[n] = 0$ additively (since $\mathcal{O}_K$ is an integral domain), and $\chi(\mathcal{O}_K) = \#(\mathcal{O}_K/n) = |n|_K^{-1}$, where $|x|_K := q^{-v(x)}$ denotes the normalized (i.e., $v(\pi) = 1$ for a uniformizer π) absolute value inside K, and q denotes the order of the residue field. The resulting formula

$$\#(K^\times/(K^\times)^n) = \frac{n \cdot \#(K^\times[n])}{|n|_K} \tag{6.3}$$

recovers that already proven in Problem 1(b) of Problem Set 1 for $n = 2$ (though the same methods would also work for general n). The proof without exponentials uses the fact that, for large enough N,

$$1 + \mathfrak{p}^N \xrightarrow{x \mapsto x^n} 1 + \mathfrak{p}^{N+v(n)}$$

is an isomorphism (which can be shown using filtrations; this is the multiplicative version of the additive statement we had earlier).

We now introduce the notion of Tate cohomology for cyclic groups.

Definition 6.8. If G is a (not necessarily finite) group, then a *G-module* A is an abelian group, with G acting on A by group automorphism. Equivalently, there is a homomorphism $G \to \mathrm{Aut}(A)$, where the action of G satisfies

(1) $g \cdot (a + b) = g \cdot a + g \cdot b$,
(2) $(gh) \cdot a = g \cdot (h \cdot a)$,

for all $g, h \in G$ and $a, b \in A$.

Example 6.9. If L/K is an extension of fields with $G := \mathrm{Gal}(L/K)$, then L and $L^\times$ are G-modules, since field automorphisms preserve both operations. This will be the main example concerning us.

Now, assume G is finite, and let A be a G-module.

DEFINITION 6.10. The *first Tate cohomology group* is

$$\hat{H}^0(G, A) := A^G/\mathrm{N}(A),$$

where

$$A^G := \{a \in A : g \cdot a = a \text{ for all } g \in G\}$$

denotes the set of fixed points.

Note that the norm map is defined as

$$\mathrm{N}\colon A \to A, \quad a \mapsto \sum_{g \in G} g \cdot a,$$

so we really do need the assumption that G be finite. Moreover, this expression shows that the norm map factors through $A^G \subseteq A$.

EXAMPLE 6.11.
(1) Returning to Example 6.9 with $A = L$, we have $A^G = K$, and $\mathrm{N}\colon L \to K$ is the field trace, hence $\hat{H}^0(L/K) = K/\mathrm{T}(L) = 0$, since L/K must be separable.
(2) If $A = L^\times$, then $(L^\times)^G = K^\times$, and $\hat{H}^0(L^\times) = K^\times/\mathrm{N}(L^\times)$. Thus, our earlier problem is now rephrased as computing $\hat{H}^0(G, L^\times)$ for L/K a cyclic extension of local fields.
(3) If A is any abelian group, then we say that G acts on A trivially if $g \cdot a = a$ for all $g \in G$ and $a \in A$. Then $\hat{H}^0(G, A) = A/\#G$. Thus, the notion of Tate cohomology entirely generalizes our previous discussion.

DEFINITION 6.12. A *map* (or *G-morphism*, or any other reasonable nomenclature) of G-modules $A \xrightarrow{f} B$ is a group homomorphism preserving the action of G, that is, $f(g \cdot a) = g \cdot f(a)$ for all $g \in G$ and $a \in A$.

A *(short) exact sequence of G-modules* is a (short) exact sequence of abelian groups, but where all maps are G-morphisms.

EXAMPLE 6.13. $1 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v} \mathbb{Z} \to 1$ is a short exact sequence of G-modules, where $G := \mathrm{Gal}(L/K)$ and G acts trivially on $\mathbb{Z}$ and on $\mathcal{O}_L^\times$ via the Galois action.

Now, let

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

by a short exact sequence of G-modules. Then we obtain an exact sequence

$$\hat{H}^0(G, A) \xrightarrow{\alpha} \hat{H}^0(G, B) \xrightarrow{\beta} \hat{H}^0(G, C), \tag{6.4}$$

where α is not necessarily injective (as we saw when the group action was trivial in the previous lecture), and β is not necessarily surjective. This is because Tate cohomology involves two operations: one, taking fixed points, is left-exact, but not right-exact, and the other, taking a quotient, is right-exact but not left-exact.

Now, assume $G = \mathbb{Z}/n\mathbb{Z}$, and let $\sigma \in G$ be a generator (i.e. 1).

DEFINITION 6.14. The *second Tate cohomology group* is

$$\hat{H}^1(G, A) := \mathrm{Ker}(\mathrm{N}\colon A \to A)/(1 - \sigma)A.$$

Note that the reason we take the quotient is because, for any $x := y - \sigma y$ for $y \in A$, we get

$$\mathrm{N}(x) = x + \sigma x + \cdots + \sigma^{n-1}x = y - \sigma y + \sigma y - \sigma^2 y + \cdots + \sigma^{n-1}y - \underbrace{\sigma^n y}_{y} = 0,$$

and we'd like to omit these trivial cases for the kernel.

Now, we claim that for an exact sequence

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

there is an exact sequence

$$\hat{H}^0(A) \to \hat{H}^0(B) \to \hat{H}^0(C) \xrightarrow{\delta} \hat{H}^1(A) \to \hat{H}^1(B) \to \hat{H}^1(C) \tag{6.5}$$

via the boundary map δ, which lifts any $x \in C^G/\mathrm{N}(C)$ to $\tilde{x} \in B$, and then takes $(1-\sigma)\tilde{x}$. Since $x \in C^G$, we have $(1-\sigma)x = 0$ in C, and therefore $(1-\sigma)\tilde{x} \in A$. Moreover, $(1-\sigma)\tilde{x}$ is clearly killed by the norm in A, hence it gives a class in $\hat{H}^1(G, A)$. Again, we check the following:

Claim 6.15. *The boundary map δ is well-defined, i.e., it doesn't depend on the choice of $\tilde{x}$.*

Proof. If $\tilde{\tilde{x}}$ is another lift, then $\tilde{x} - \tilde{\tilde{x}} \in A$ since $C \simeq B/A$, so $(1-\sigma)(\tilde{x} - \tilde{\tilde{x}})$ is zero in $\hat{H}^1(G, A)$. □

Claim 6.16. *The sequence (6.5) extends to be exact.*

Proof. As before, we verify this only at the boundary map. Letting $x \in B^G/\mathrm{N}(B)$, its image in $\hat{H}^1(A)$ is $(1-\sigma)x = 0$. If $x \in \mathrm{Ker}(\delta)$, then $\tilde{x} \in B^G$ and hence in $\hat{H}^0(B)$ for some lift $\tilde{x}$ of x.

Letting $x \in C^G/\mathrm{N}(C)$, its image in $\hat{H}^1(A)$ is $(1-\sigma)\tilde{x}$, where $\tilde{x}$ is a lift of x to B, hence it is killed in $\hat{H}^1(B)$ by definition. If $x \in \hat{H}^1(A)$ is 0 in $\hat{H}^1(B)$, then $x \in (1-\sigma)B$, hence $x \in \mathrm{Im}(\delta)$. □

LECTURE 7

Chain Complexes and Herbrand Quotients

Last time, we defined the Tate cohomology groups $\hat{H}^0(G,M)$ and $\hat{H}^1(G,M)$ for cyclic groups. Recall that if $G = \mathbb{Z}/n\mathbb{Z}$ with generator σ, then a G-module is an abelian group M with an automorphism $\sigma\colon M \xrightarrow{\sim} M$ such that $\sigma^n = \mathrm{id}_M$. Our main example is when L/K is an extension of fields with $\mathrm{Gal}(L/K) = G$, so that both L and $L^\times$ are G-modules. Then

$$\hat{H}^0(G,M) := M^G/\mathrm{N}(M) = \mathrm{Ker}(1-\sigma)\Big/\Big\{\sum_{i=0}^{n-1}\sigma^i m : m \in M\Big\}$$

$$\hat{H}^1(G,M) := \mathrm{Ker}(\mathrm{N})/(1-\sigma),$$

since an element of $\mathrm{Ker}(1-\sigma)$ is fixed under the action of σ, hence under the action of G. Our goal was to compute, in the example given above, that $\#\hat{H}^0 = n$, using long exact sequences.

We saw that if

$$0 \to M \to E \to N \to 0$$

was a short exact sequence of G-modules (that is, M, E, and N are abelian groups equipped with an order-n automorphism compatible with these maps, and $N = E/M$, so that M is fixed under the automorphism of N), then we had a long exact sequence

$$\hat{H}^0(G,M) \to \hat{H}^0(G,E) \to \hat{H}^0(G,N) \xrightarrow{\delta} \hat{H}^1(G,M) \to \hat{H}^1(G,E) \to \hat{H}^1(G,N),$$

where the boundary map δ lifts $x \in \hat{H}^0(N) = N^G/\mathrm{N}(N)$ to $\tilde{x} \in E$, so that $(1-\sigma)\tilde{x} \in \mathrm{Ker}(\mathrm{N}) \subseteq M$, giving a class in $\hat{H}^1(G,M)$.

Now, define a second boundary map

(7.1)

$$\hat{H}^1(G,M) \to \hat{H}^1(G,E) \to \hat{H}^1(G,N) \xrightarrow{\partial} \hat{H}^0(G,M) \to \hat{H}^0(G,E) \to \hat{H}^0(G,N),$$

which lifts $x \in \hat{H}^1(G,N)$ to an element $\tilde{x} \in E$. Then $\mathrm{N}(\tilde{x}) = \sum_{i=0}^{n-1}\sigma^i\tilde{x} \in M^G$, since it is killed by $1-\sigma$, and so it defines a class in $\hat{H}^0(G,M)$. We check the following:

Claim 7.1. *The boundary map ∂ is well-defined.*

Proof. If $\tilde{\tilde{x}}$ is another lift of x, then $\tilde{x} - \tilde{\tilde{x}} \in M$ since $N = E/M$, and therefore $\sum_{i=0}^{n-1}\sigma^i(\tilde{x}-\tilde{\tilde{x}}) \in \mathrm{N}(M)$ is killed in $\hat{H}^0(G,M)$. □

Claim 7.2. *The sequence in (7.1) is exact.*

Proof. If $x \in \hat{H}^1(G,E)$, then $\mathrm{N}(x) = 0$, so $\partial(x) = 0$ in $\hat{H}^0(G,M)$. If $x \in \mathrm{Ker}(\partial)$, then $N(\tilde{x}) = 0$ for some lift $\tilde{x} \in E$ of x, and x is the image of $\tilde{x}$.

If $x \in \hat{H}^1(G,N)$ with lift $\tilde{x} \in E$, then $\partial(x) = \mathrm{N}(\tilde{x})$ is zero in $\hat{H}^0(G,E)$ by definition. If $x \in \hat{H}^0(G,M)$ is 0 in $\hat{H}^0(G,E)$, then $x \in \mathrm{N}(E)$, hence $x \in \mathrm{Im}(\partial)$. □

Thus, we obtain a "2-periodic" exact sequence for Tate cohomology of cyclic groups, motivating the following definition:

Definition 7.3. For each $i \in \mathbb{Z}$ (both positive and negative), define

$$\hat{H}^i(G,M) := \begin{cases} \hat{H}^0(G,M) & \text{if } i \equiv 0 \bmod 2, \\ \hat{H}^1(G,M) & \text{if } i \equiv 1 \bmod 2. \end{cases}$$

This nice property does not hold for non-cyclic groups, so we will often attempt to reduce cohomology to the case of cyclic groups.

As a reformulation, write

$$\cdots \xrightarrow{\sum_{i=0}^{n-1} \sigma^i} M \xrightarrow{1-\sigma} M \xrightarrow{\sum_{i=0}^{n-1} \sigma^i} M \xrightarrow{1-\sigma} \cdots, \tag{7.2}$$

and observe that this forms what we will call a chain complex:

Definition 7.4. A *chain complex* $X^\bullet$ is a sequence

$$\cdots \xrightarrow{d^{-2}} X^{-1} \xrightarrow{d^{-1}} X^0 \xrightarrow{d^0} X^1 \xrightarrow{d^1} X^2 \xrightarrow{d^2} \cdots,$$

such that $d^{i+1}d^i = 0$ for all $i \in \mathbb{Z}$ (that is, $\mathrm{Ker}(d^{i+1}) \supset \mathrm{Ker}(d^i)$, but we need not have equality as for an exact sequence). Then define the *ith cohomology* of $X^\bullet$ as

$$H^i(X^\bullet) := \mathrm{Ker}(d^i)/\,\mathrm{Im}(d^{i-1}).$$

Thus, a long exact sequence is a type of chain complex. We note that (7.2) satisfies this definition as

$$(1-\sigma)\sum_{i=0}^{n-1} \sigma^i x = \sum_{i=0}^{n-1} \sigma^i x - \sum_{i=0}^{n-1} \sigma^{i+1} x = \mathrm{N}x - \mathrm{N}x = 0$$

and the two maps clearly commute. The Tate cohomology groups are then the cohomologies of this chain complex, which makes it clear that they are 2-periodic.

Definition 7.5. The *Herbrand quotient* or *Euler characteristic* of a G-module M is

$$\chi(M) := \frac{\#\hat{H}^0(G,M)}{\#\hat{H}^1(G,M)},$$

which is only defined when both are finite.

This definition generalizes our previous discussion of the trivial G-module, as $\hat{H}^0(G,M) = M/n$ and $\hat{H}^1(G,M) = M[n]$, though note that the boundary maps from even to odd cohomologies will be zero.

Lemma 7.6. *Let*

$$0 \to M \to E \to N \to 0$$

be a short exact sequence of G-modules. If χ is defined for two of the three G-modules, then it is defined for all three, in which case $\chi(M) \cdot \chi(N) = \chi(E)$.

Proof. Construct a long exact sequence

$$0 \to \mathrm{Ker}(\alpha) \to \hat{H}^0(M) \xrightarrow{\alpha} \hat{H}^0(E) \to \hat{H}^0(N) \to$$
$$\xrightarrow{\delta} \hat{H}^1(M) \to \hat{H}^1(E) \xrightarrow{\beta} \hat{H}^1(N) \to \mathrm{Coker}(\beta) \to 0.$$

Since the second boundary map yields an exact sequence

$$\hat{H}^1(E) \xrightarrow{\beta} \hat{H}^1(N) \xrightarrow{\partial} \hat{H}^0(M) \xrightarrow{\alpha} \hat{H}^0(E),$$

we have

$$\mathrm{Ker}(\alpha) = \mathrm{Im}(\partial) = \hat{H}^1(N)/\mathrm{Ker}(\partial) = \hat{H}^1(N)/\mathrm{Im}(\beta) = \mathrm{Coker}(\beta).$$

Applying Lemma 6.4 and canceling $\#\mathrm{Ker}(\alpha)$ and $\#\mathrm{Coker}(\beta)$ then yields the desired result (as for Lemma 6.7). □

A quick digression about finiteness:

Claim 7.7. *The groups $\hat{H}^0(G,M)$ and $\hat{H}^1(G,M)$ are n-torsion.*

Proof. Let $x \in M^G$. Then $\mathrm{N}(x) = \sum_{i=0}^{n-1} \sigma^i x = \sum_{i=0}^{n-1} x = nx$. Thus, $nx \in N(M)$, and $\hat{H}^0(G,M)$ is n-torsion. Now let $x \in \mathrm{Ker}(\mathrm{N})$. Then

$$nx = nx - \mathrm{N}x = \sum_{i=1}^{n}(1-\sigma^i)x = (1-\sigma)\sum_{i=1}^{n}(1+\cdots+\sigma^{i-1})x,$$

hence $nx \in (1-\sigma)M$, and $\hat{H}^1(G,M)$ is n-torsion as well. □

Thus, finite generation of $\hat{H}^0(G,M)$ and $\hat{H}^1(G,M)$ implies finiteness. Now, we recall that our goal was to show that $\#\hat{H}^0(L^\times) = n$ for a cyclic degree-n extension of local fields L/K. We have the following refined claims:

Claim 7.8. *Preserving the setup above,*

(1) $\hat{H}^1(L^\times) = 0$ *(implying* $\chi(L^\times) = \#\hat{H}^0(L^\times)$*);*
(2) $\chi(\mathcal{O}_L^\times) = 1$*;*
(3) $\chi(L^\times) = n$.

Proof. We first show that (2) implies (3). We have an exact sequence

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

where v denotes the valuation. Then by Lemma 7.6, we have

$$\chi(L^\times) = \chi(\mathcal{O}_L^\times) \cdot \chi(\mathbb{Z}) = 1 \cdot n = n$$

by (2), where we note that

$$\hat{H}^0(\mathbb{Z}) = \mathbb{Z}^G/\mathrm{N}\mathbb{Z} = \mathbb{Z}/n\mathbb{Z} \quad \text{and} \quad \hat{H}^1(\mathbb{Z}) = \mathrm{Ker}(\mathrm{N})/(1-\sigma) = 0.$$

We now show (2).

Lemma 7.9. *If M is a finite G-module, then $\chi(M) = 1$.*

Proof. We have exact sequences

$$0 \to M^G \to M \xrightarrow{1-\sigma} \mathrm{Ker}(\mathrm{N}) \to \hat{H}^1(G,M) \to 0,$$

$$0 \to \mathrm{Ker}(\mathrm{N}) \to M \xrightarrow{\sum_{i=0}^{n-1}\sigma^i} M^G \to \hat{H}^0(G,M) \to 0,$$

hence by Lemma 7.6,

$$\#\mathrm{Ker}(\mathrm{N}) \cdot \#M^G = \#M \cdot \#\hat{H}^0(G,M),$$
$$\#M^G \cdot \#\mathrm{Ker}(\mathrm{N}) = \#M \cdot \#\hat{H}^1(G,M),$$

and so $\#\hat{H}^0(G,M) = \#\hat{H}^1(G,M)$ and $\chi(M) = 1$ as desired. □

The analogous statement is $\chi(\mathcal{O}_L) = 1$, where we regard $\mathcal{O}_L$ as an additive group. In fact, an even easier statement to establish is $\chi(L) = 1$. Intuitively, this is because since we are working over the p-adic numbers, everything must be a $\mathbb{Q}$-vector space, hence n is invertible; but our cohomology groups are all n-torsion by Claim 7.7, hence our cohomology groups must both vanish and $\chi(L) = 1$.

By the normal basis theorem, if L/K is a finite Galois extension, we have

$$L \simeq \prod_{g \in G} K = K[G]$$

as a $K[G]$-module, where G acts by permuting coordinates. This is because the action of K (by homothety, as L is a K-vector space) commutes with the action of G (which acts on L as a K-vector space), hence we have a $K[G]$-action on L.

Claim 7.10. *Let A be any abelian group, and $A[G] := \prod_{g \in G} A$ be a G-module where G acts by permuting coordinates. If G is cyclic, then*

$$\hat{H}^0(G, A[G]) = \hat{H}^1(G, A[G]) = 0.$$

Proof. We reformulate the claim as follows: let R be a commutative ring, so that $R[G]$ is an (possibly non-commutative) R-algebra via the multiplicative operation

$$\left(\sum_{g \in G} x_g [g] \right) \left(\sum_{h \in G} y_h [h] \right) := \sum_{g,h \in G} x_g y_h [gh],$$

where we have let $[h] \in \prod_{g \in G} R$ denote the element that is 1 in the h-coordinate, and 0 otherwise. Thus, $R[G]$-modules are equivalent to R-modules equipped with a homomorphism $G \to \mathrm{Aut}_R(M)$. In particular, $\mathbb{Z}[G]$-modules are equivalent to G-modules.

Now, we have $\hat{H}^0(G, A[G]) = A[G]^G/\mathrm{N}$, where $A[G]^G$ is equivalent to a diagonally embedded $A \subset \prod_{g \in G} A$, and $\mathrm{N}((a, 0, \ldots, 0)) = \sum_{g \in G} a[g]$ which is equal to the diagonal embedding of A, hence $\hat{H}^0(G, A[G]) = 0$.

Similarly, $\hat{H}^1(G, A[G]) = \mathrm{Ker}(\mathrm{N})/(1 = \sigma)$, and

$$A[G] \supseteq \mathrm{Ker}(\mathrm{N}) = \left\{ \sum_{g \in G} a_g [g] \in A[G] : \sum_{g \in G} a_g = 0 \right\}.$$

Now, we may write a general element as $\sum_{i=0}^{n-1} a_i [\sigma^i]$, and choose b_i such that $(1 - \sigma^{n-i}) a_i = (1 - \sigma) b_i$ for each i. Then

$$(1 - \sigma) \sum_{i=0}^{n-1} b_i [\sigma^i] = \sum_{i=0}^{n-1} (1 - \sigma^{n-i}) a_i [\sigma^i] = \sum_{i=0}^{n-1} a_i [\sigma^i] - \sum_{i=0}^{n-1} a_i [1] = \sum_{i=0}^{n-1} a_i [\sigma^i],$$

hence $\mathrm{Ker}(\mathrm{N}) \subset (1 - \sigma) A[G]$, and therefore $\hat{H}^1(G, A[G]) = 0$ as desired. □

Thus, we see that we cannot obtain interesting Tate cohomology in this manner. Now we return to showing $\chi(\mathcal{O}_L) = 1$. The problem is that the normal basis theorem does not apply as for L, that is, whereas $L = K[G]$, we do not necessarily have $\mathcal{O}_L \simeq \mathcal{O}_K[G]$.

However, there does exist an open subgroup of $\mathcal{O}_L$ with a normal basis. Choose a normal basis $\{e_1, \ldots, e_n\}$ of L/K. For large enough N, we have $\pi^N e_1, \ldots, \pi^N e_n \in$

$\mathcal{O}_L$, where π is a uniformizer of L, hence they freely span some open subgroup of $\mathcal{O}_L$. Because this subgroup, call it Γ, is finite index, we have

$$\chi(\mathcal{O}_K) = \chi(\Gamma) = \chi(\mathcal{O}_K[G]) = 1$$

by (6.2).

To show that $\chi(\mathcal{O}_L^\times) = 1$ (a more complete proof will be provided in the following lecture), observe that $\mathcal{O}_L^\times \supseteq \Gamma \simeq \mathcal{O}_L^+$ via G-equivalence, where Γ is an open subgroup (the proof of this fact uses the p-adic exponential). Then $\chi(\mathcal{O}_L^\times) = \chi(\Gamma) = 1$, as desired. □

Remark 7.11. In this course, all rings and modules are assumed to be unital.

LECTURE 8

Tate Cohomology and Inverse Limits

Recall that, for an extension L/K of local fields with Galois group $G := \mathbb{Z}/n\mathbb{Z}$, we were trying to show that $\#\hat{H}^0(G, L^\times) = n$. We claimed that $\chi(L^\times) = n$ if and only if $\chi(\mathcal{O}_L^\times) = 1$, where χ denotes the Herbrand quotient $\#\hat{H}^0/\#\hat{H}^1$ and we recall that a finite group has Herbrand quotient equal to 1 and that χ is multiplicative for short exact sequences.

Last time, we proved $\chi(\mathcal{O}_L) = 1$, using the normal basis theorem to show that $L \simeq K[G]$, that $\mathcal{O}_L$ contains a finite-index open subgroup Γ such that $\mathcal{O}_L^\times \supset \Gamma \simeq \mathcal{O}_L^+$ via G-equivalence (so that Γ is closed under the G-action), and that $\mathcal{O}_K[G] \simeq \Gamma \subseteq \mathcal{O}_L$. We then used Claim 7.10 to show that $\hat{H}^i(G, \Gamma) = 0$ for each i, hence $\chi(\mathcal{O}_L) = \chi(\Gamma) = 1$.

Now we'd like to give a better, i.e., more algebraic (without p-adic exponentials!), proof that $\chi(\mathcal{O}_L^\times) = 1$. So fix some open subgroup $\Gamma \subseteq \mathcal{O}_L$ isomorphic to $\mathcal{O}_K[G]$ (as $\mathcal{O}_K[G]$-modules).

Claim 8.1. *For sufficiently large N, $1 + \mathfrak{p}_K^N\Gamma$ is a subgroup of $\mathcal{O}_L^\times$, where $\mathfrak{p}_K$ is the maximal ideal of $\mathcal{O}_K$.*

Proof. For $x, y \in \Gamma \subseteq \mathcal{O}_L$, we have

$$(1 + \pi^N x)(1 + \pi^N y) = 1 + \underbrace{\pi^N(x + y)}_{\in \mathfrak{p}_K^N\Gamma} + \underbrace{\pi^{2N}(xy)}_{\in \mathfrak{p}_K^{2N}\mathcal{O}_L}, \tag{8.1}$$

where π is a uniformizer of $\mathfrak{p}_K$. Thus, if we choose N large enough that $\mathfrak{p}_K^N\mathcal{O}_L \subseteq \Gamma$, which is possible because Γ is an open subgroup of $\mathcal{O}_L$, this product will be in $1 + \pi^N\Gamma$ and therefore $1 + \mathfrak{p}_K^N\Gamma$ will be a subgroup of $\mathcal{O}_L^\times$. □

Claim 8.2. *The cohomologies of Γ all vanish.*

Choose N such that $\mathfrak{p}_K^N\mathcal{O}_L \subseteq \mathfrak{p}_K\Gamma$. Then the last term in (8.1) is in $\mathfrak{p}_K^{2N}\mathcal{O}_L \subseteq \mathfrak{p}_K^{N+1}\Gamma$. This suggests that we ought to filter $1 + \mathfrak{p}_K^N\Gamma$ with additive subquotients, that is, by $1 + \mathfrak{p}_K^{N+i}\Gamma$, so that

$$(1 + \mathfrak{p}_K^{N+i}\Gamma)/(1 + \mathfrak{p}_K^{N+i+1}\Gamma) \simeq \Gamma/\mathfrak{p}_K\Gamma \simeq k_K[G]$$

for all $i \geq 0$ as additive groups by the above calculation, where k_K denotes the residue field of K. Moreover, these isomorphisms are *Galois-equivariant*, or *G-equivariant*, as the G-action preserves all terms (Γ is preserved by assumption), hence acts on both sides, and is preserved by the isomorphism. Thus, by Claim 7.10,

$$\hat{H}^j(G, (1 + \mathfrak{p}_K^{N+i}\Gamma)/(1 + \mathfrak{p}_K^{N+i+1}\Gamma)) = \hat{H}^j(G, k_K[G]) = 0,$$

for each $i \geq 0$ and j. As a corollary, for which we need the following lemma,

$$\hat{H}^j(G, (1 + \mathfrak{p}_K^N\Gamma)/(1 + \mathfrak{p}_K^{N+i}\Gamma)) = 0 \tag{8.2}$$

for all $i \geq 0$ and j.

LEMMA 8.3. *For any short exact sequence*

$$0 \to M \to E \to N \to 0$$

of G-modules, $\hat{H}^i(G, M) = \hat{H}^i(G, N) = 0$ implies $\hat{H}^i(G, E) = 0$ for each i.

PROOF. By (6.4), we have an exact sequence

$$\underbrace{\hat{H}^i(G, M)}_{0} \xrightarrow{\alpha} \hat{H}^i(G, E) \xrightarrow{\beta} \underbrace{\hat{H}^i(G, N)}_{0},$$

hence $\hat{H}^i(E) = \mathrm{Ker}(\beta) = \mathrm{Im}(\alpha) = 0$, as desired. □

Now, we have an exact sequence

$$0 \to \frac{1 + \mathfrak{p}_K^{N+i}\Gamma}{1 + \mathfrak{p}_K^{N+i+1}\Gamma} \to \frac{1 + \mathfrak{p}_K^{N}\Gamma}{1 + \mathfrak{p}_K^{N+i+1}\Gamma} \to \frac{1 + \mathfrak{p}_K^{N}\Gamma}{1 + \mathfrak{p}_K^{N+i}\Gamma} \to 0,$$

so (8.2) follows by induction on i and Lemma 8.3.

It remains to show that $\hat{H}^j(1 + \mathfrak{p}^N\Gamma) = 0$. In a perfect world, we would have

$$\hat{H}^j(G, \varprojlim_n M_n) = \varprojlim_n \hat{H}^j(G, M_n)$$

for any sequence of modules with a G-action and G-equivariant structure maps. Thus would then imply

$$\begin{aligned}
\hat{H}^j(1 + \mathfrak{p}_K^N\Gamma) &= \hat{H}^j\big(\varprojlim_{i \geq 0}(1 + \mathfrak{p}_K^N\Gamma)/(1 + \mathfrak{p}_K^{N+i}\Gamma)\big) \\
&= \varprojlim_{i \geq 0} \hat{H}^j((1 + \mathfrak{p}_k^N\Gamma)/(1 + \mathfrak{p}_K^{N+i}\Gamma)) \\
&= \varprojlim_{i \geq 0} 0 \\
&= 0
\end{aligned}$$

by (8.2), as our filtration is complete. Thus, we need to find some way to justify commuting Tate cohomologies and inverse limits.

LEMMA 8.4. *Suppose we have a sequence of modules*

(8.3)

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_{n+1} & \longrightarrow & E_{n+1} & \longrightarrow & N_{n+1} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & M_n & \longrightarrow & E_n & \longrightarrow & N_n & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

with exact rows. Then we have an exact sequence

$$0 \to \varprojlim_n M_n \xrightarrow{\varphi} \varprojlim_n E_n \xrightarrow{\psi} \varprojlim_n N_n.$$

Moreover, if $M_n \to M_{n+1}$ is surjective for each n, then ψ is as well (otherwise, it may not be!).

PROOF. Evidently, φ is injective, as if $x \in \mathrm{Ker}(\varphi)$, then each coordinate of its image is 0, so by compatibility and injectivity of $M_n \to E_n$ for each n, each coordinate of x is 0, hence $x = 0$. Similarly, $\mathrm{Ker}(\psi) = \mathrm{Im}(\varphi)$ by exactness of each row in (8.3).

To see (intuitively) how surjectivity of ψ can fail, consider a compatible system $(x_n) \in \varprojlim_n N_n$. We can lift each x_n to some $y_n \in E_n$, but it is unclear how to do it compatibly, so that $(y_n) \in \varprojlim_n E_n$.

Now assume that that each of the maps $M_n \to M_{n+1}$ is surjective. Let $(x_n) \in \varprojlim_n N_n$, and suppose we have constructed $y_n \in E_n$ for some n. Choose any $\tilde{y}_{n+1} \mapsto x_{n+1}$ via the map $E_{n+1} \to N_{n+1}$, and let α_{n+1} be the image of $\tilde{y}_{n+1}$ in E_n. Then $y_n - \alpha_{n+1} \in M_n$ as it vanishes in N_n, and it lifts to $\beta_{n+1} \in M_{n+1}$ by assumption. If we now define $y_{n+1} := \tilde{y}_{n+1} + \beta_{n+1}$, then this maps to $\alpha_{n+1} + y_n - \alpha_{n+1} = y_n$ in E_n and to x_{n+1} in N_{n+1} as β_{n+1} maps to 0 in N_{n+1}, hence by induction there exists a compatible system $(y_n) \in \varprojlim_n E_n$ mapping to (x_n) via ψ, as desired (note that we may express this result as a surjection $E_{n+1} \twoheadrightarrow E_n \times_{N_n} N_{n+1}$, i.e., to the fibre product).. □

PROPOSITION 8.5. *If*

$$\cdots \twoheadrightarrow M_{n+1} \twoheadrightarrow M_n \twoheadrightarrow \cdots \twoheadrightarrow M_0 \tag{8.4}$$

is a sequence of G-modules, and $\hat{H}^i(M_{n+1}) \twoheadrightarrow \hat{H}^i(M_n)$ for all n and i, then

$$\hat{H}^i(\varprojlim_n M_n) = \varprojlim_n \hat{H}^i(M_n)$$

for all i.

PROOF. We provide a proof for $\hat{H}^0$. Let $M := \varprojlim_n M_n$, so that we are comparing $\hat{H}^0(M) = M^G/\mathrm{N}(M)$ and $\varprojlim_n \hat{H}^0(M_n) = \varprojlim_n M_n^G/\mathrm{N}(M_n)$. This amounts to showing that the natural map

$$(\varprojlim_n M_n^G)/(\varprojlim_n \mathrm{N}(M_n)) \xrightarrow{\sim} \varprojlim_n (M_n^G/\mathrm{N}(M_n))$$

is an isomorphism. We have a commutative diagram

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{N}(M_{n+1}) & \longrightarrow & M_{n+1}^G & \longrightarrow & \hat{H}^0(G, M_{n+1}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \alpha_n} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{N}(M_n) & \longrightarrow & M_n^G & \longrightarrow & \hat{H}^0(G, M_n) & \longrightarrow & 0, \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

and we claim that α_n is surjective for each n. Indeed, let $x \in \mathrm{N}(M_n)$, so that $x = \mathrm{N}(y)$ for some $y \in M_n$. Lifting y to an element $z \in M_{n+1}$, we have $\alpha_n(\mathrm{N}(z)) = x$,

as desired. Thus, by Lemma 8.4, we have

$$\varprojlim_n \hat{H}^0(M_n) = (\varprojlim_n M_n^G)/(\varprojlim_n \mathrm{N}(M_n)).$$

Now, we have

$$\hat{H}^0(\varprojlim_n M_n) = (\varprojlim_n M_n)^G/\mathrm{N}(\varprojlim_n M_n) = M^G/\mathrm{N}(M).$$

It is clear that $(\varprojlim_n M_n)^G = \varprojlim_n M_n^G$, since G acts on each of the coordinates of $\varprojlim_n M_n$, so it remains to show that $\mathrm{N}(\varprojlim_n M_n) \xrightarrow{\sim} \varprojlim_n \mathrm{N}(M_n)$. Letting $K_n := \mathrm{Ker}(\mathrm{N}\colon M_n \to M_n)$ for each n, we have a commutative diagram

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K_{n+1} & \longrightarrow & M_{n+1} & \longrightarrow & \mathrm{N}(M_{n+1}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \beta_n} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K_n & \longrightarrow & M_n & \longrightarrow & \mathrm{N}(M_n) & \longrightarrow & 0. \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

We'd like to show that β_n is surjective. Recall that $\hat{H}^1(G, M_n) = K_n/(1-\sigma)M_n$, and thus we have a commutative diagram

$$\begin{array}{ccccccccc}
 & & \vdots & & \vdots & & \vdots & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (1-\sigma)M_{n+1} & \longrightarrow & K_{n+1} & \longrightarrow & \hat{H}^1(G, M_{n+1}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \gamma_n} & & \downarrow{\scriptstyle \beta_n} & & \downarrow{\scriptstyle \delta_n} & & \\
0 & \longrightarrow & (1-\sigma)M_n & \longrightarrow & K_n & \longrightarrow & \hat{H}^1(G, M_n) & \longrightarrow & 0. \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & \vdots & & \vdots & & \vdots & &
\end{array}$$

Now, γ_n is surjective (the proof is similar to that for α_n), and δ_n is surjective by hypothesis. Thus, β_n is surjective by the Snake Lemma, and so Lemma 8.4 implies

$$\varprojlim_n \mathrm{N}(M_n) = (\varprojlim_n M_n)/(\varprojlim_n K_n) = \mathrm{N}(\varprojlim_n M_n).$$

It follows that $\hat{H}^0(\varprojlim_n M_n) = \varprojlim_n \hat{H}^0(M_n)$, as desired. □

Corollary 8.6. *For a sequence (8.4), if $\hat{H}^i(M_n) = 0$ for all n and i, then $\hat{H}^i(\varprojlim_n M_n) = 0$. In particular, $\hat{H}^i(1+\mathfrak{p}_K^N\Gamma) = 0$, where we have set $M_i := (1+\mathfrak{p}_K^N\Gamma)/(1+\mathfrak{p}_K^{N+i}\Gamma)$ for each i.*

It follows that, since $1+\mathfrak{p}_K^N\Gamma \subseteq \mathcal{O}_L^\times$ is a (additive, with a normal basis) finite-index subgroup, we have $\chi(\mathcal{O}_L^\times) = \chi(1+\mathfrak{p}_K^N) = 1$, which establishes (2) of Claim 7.8.

LECTURE 9

Hilbert's Theorem 90 and Cochain Complexes

As always, $G = \mathbb{Z}/n\mathbb{Z}$ and L/K is a Galois extension of local fields with $\mathrm{Gal}(L/K) = G$ and generator $\sigma \in G$. In the last lecture, we showed:

THEOREM 9.1. *$\chi(L^\times) = n$, where χ denotes the Herbrand quotient.*

Note that our methods actually generalize easily to the non-archimedean case. In this lecture, we will show:

THEOREM 9.2 (Hilbert's Theorem 90). *$\hat{H}^1(G, K^\times) = 0$.*

Together, these imply that $\hat{H}^0(G, L^\times) = K^\times/\mathrm{N}(L^\times)$ has cardinality n. Another corollary of Hilbert's Theorem 90 is that if L and K are finite fields, then $\hat{H}^i(G, L^\times) = 0$ for all i, because $\chi(L^\times) = 1$ as L is finite (so all cohomologies vanish by periodicity). This is similar to the first result in [Wei74]. Explicitly, we have

$$\hat{H}^1(G, L^\times) = \mathrm{Ker}(\mathrm{N}\colon L^\times \to K^\times)/\{y/\sigma y : y \in L^\times\},$$

where each element $y/\sigma y$ has norm 1 as $y/\sigma y \cdot \sigma y/\sigma^2 y \cdots \sigma^{n-1} y/\sigma^n y = 1$. Then Hilbert's Theorem 90 implies the following:

COROLLARY 9.3. *If L/K is a cyclic extension, and $x \in L^\times$ with $\mathrm{N}(x) = 1$, then $x = y/\sigma y$ for some $y \in L^\times$.*

EXAMPLE 9.4. Let $L := \mathbb{Q}(i)$ and $K := \mathbb{Q}$. Choose $x \in \mathbb{Q}(i)$ with $\mathrm{N}(x) = 1$. Then $x = a/c + (b/c)i$ for some $a, b, c \in \mathbb{Z}$ satisfying $a^2 + b^2 = c^2$. Then Hilbert's Theorem 90 yields the usual parametrization of Pythagorean triples, $(r-s)^2 + (2rs)^2 = (r+s)^2$.

For $n = 2$, the proof is simple. We have $\mathrm{N}(x) = x \cdot \sigma x = 1$, so if we let $y := x + 1$ when $x \neq -1$, then $x \cdot \sigma y = x(\sigma x + 1) = \mathrm{N}(x) + x = 1 + x = y$, hence $x = y/\sigma y$ as desired. If $x = -1$, then let $y := \sqrt{d}$, where $L = K(\sqrt{d})$, then again we have $y/\sigma y = \sqrt{d}/(-\sqrt{d}) = -1 = x$. Note that this completes the proof that $\#(K^\times/\mathrm{N}L^\times) = 2$ for a quadratic extension L/K of local fields, and thus of the good properties of Hilbert symbols! Indeed, recall that, for a field $L := K(\sqrt{a})$ with $a \in K^\times$ but not a square, then $(a, b) = 1$ if and only if $b \in \mathrm{N}(L^\times)$.

We now move on to the general case of Hilbert's Theorem 90. Here's the main lemma:

LEMMA 9.5. *For each $x \in L$, let*

$$H_x\colon L \to L, \quad y \mapsto x \cdot \sigma(y),$$

which is a linear map of K-vector spaces. Then the characteristic polynomial of H_x is $t^n - \mathrm{N}(x) \in K[t]$, where we have normalized the definition of the characteristic polynomial to be monic.

Note that this characteristic polynomial is simpler than that of $y \mapsto xy$, which will have a nonzero multiple of t^{n-1} as long as the $\mathrm{T}(x) \neq 0$, which will occur when the trace is nondegenerate (which is true of any separable extension).

Proof (9.5 $\Longrightarrow$ 9.2). Let $x \in L$, and assume $\mathrm{N}(x) = 1$. Then the characteristic polynomial of $\hat{H}_x$ is $t^n - 1$, implying 1 is a root and hence an eigenvalue of H_x. Thus, $\mathrm{Ker}((H_x - 1) \otimes_K \overline{K}) \neq 0$, so since for fields tensor products commute with taking kernels, we have $\mathrm{Ker}(H_x - 1) \neq 0$. Thus, there exists some $y \in L^\times$ such that $H_x(y) = x \cdot \sigma(y) = y$, that is, $x = y/\sigma y$, as desired. □

Proof (of Lemma). First observe that H_x^n corresponds to multiplication by $\mathrm{N}(x)$, since

$$H_x^n(y) = x \cdot \sigma(x \cdot \sigma(x \cdots \sigma(y))) = x \cdot \sigma(x) \cdot \sigma^2(x) \cdots \sigma^{n-1}(x) \cdot \sigma^n(y) = \mathrm{N}(x)y$$

for any $y \in L$. It follows that the minimal polynomial of H_x divides $t^n - \mathrm{N}(x)$. Now, recall that the minimal polynomial of a linear operator T always divides its characteristic polynomial, which has degree n, so showing that they are equal suffices. Thus is true if and only if there are no blocks with shared eigenvalues in the Jordan decomposition of T, which is true if and only if $\dim_K(\mathrm{Ker}(T - \lambda I)) \leq 1$, for all $\lambda \in \overline{K}$.

Here's a proof that doesn't quite work. Suppose that $H_x(y_1) = \lambda y_1$, $H_x(y_2) = \lambda y_2$, and $y_1, y_2 \neq 0$ (so that the two are "honest eigenvalues"). We'd like to show that y_2 is a multiple of y_1, that is, $y_2/y_1 \in K$, i.e., is fixed by $\mathrm{Gal}(L/K)$. Indeed, we have

$$\frac{\sigma y_2}{\sigma y_1} = \frac{\frac{1}{x}\lambda y_2}{\frac{1}{x}\lambda y_1} = \frac{y_2}{y_1},$$

since $\sigma y_2 = H_x(y_2)/x$, and similarly for y_1. However, the issue is that this proof occurred in L, and not $\overline{K}$, which is where our eigenvalues actually live! Thus, we need to work in $L \otimes_K \overline{K} \simeq \prod_{g \in G} \overline{K}$, which is not necessarily a field.

We can compute the characteristic polynomial after extension of scalars. Recall that

$$L \otimes_K \overline{K} \xrightarrow{\sim} \prod_{i=0}^{n-1} \overline{K}, \quad a \otimes b \mapsto ((\sigma^i a) \cdot b)_{i=0}^{n-1}.$$

This extends non-canonically to an automorphism of $\overline{K}$, but otherwise everything is canonical, with the group acting on the set of coordinates by left multiplication. The map

$$\sigma \otimes \mathrm{id} \colon L \otimes_K \overline{K} \to L \otimes_K \overline{K}$$

corresponds to permuting the coordinates, and we have a map

$$\mu_x \otimes \mathrm{id} \colon L \otimes_K \overline{K} \to L \otimes_K \overline{K}, \quad (y_0, \ldots, y_{n-1}) \mapsto (xy_0, (\sigma x)y_1, \ldots, (\sigma^{n-1}x)y_{n-1}),$$

where μ_x denotes multiplication by x. Now, say $\lambda \in \overline{K}$ is an eigenvalue of H_x with corresponding eigenvector $(y_0, \ldots, y_{n-1})$. Then

$$H_x(y) = (xy_1, (\sigma x)y_2, (\sigma^2 x)y_3, \ldots, (\sigma^{n-1}x)y_0) = (\lambda y_0, \lambda y_1, \lambda y_2, \ldots, \lambda y_{n-1}),$$

and so $xy_1 = \lambda y_0$, implying $y_1 = (\lambda/x)y_0$, and similarly $y_2 = (\lambda/\sigma x)y_1 = (\lambda^2/(x \cdot \sigma x))y_0$. In general, we have

$$y_i = \frac{\lambda^i}{x \cdots \sigma^{i-1}x} y_0,$$

so all coordinates are uniquely determined by y_0, i.e.,

$$(y_0, \dots, y_{n-1}) = y_0 \left(1, \frac{\lambda}{x}, \frac{\lambda^2}{x \cdot \sigma x}, \dots, \frac{\lambda^{n-1}}{\prod_{i=0}^{n-2} \sigma^i x}\right).$$

So indeed, our eigenspaces each only have dimension one, as desired. Note that this only defines an eigenvector if

$$\frac{\lambda^n}{x \cdots \sigma^{n-1} x} = \frac{\lambda^n}{\mathrm{N}(x)} = 1,$$

that is, if $\lambda^n = \mathrm{N}(x)$, which is consistent with what we expected (and all nth roots appear with multiplicity one). □

Now, we recall that our goal was to show that for an abelian extension L/K of local fields,

$$K^\times / \mathrm{N}L^\times \simeq \mathrm{Gal}(L/K)$$

canonically (in a strong sense). We've shown that $K^\times/\mathrm{N}L^\times$ has the right order, but we'll prove this generally for non-cyclic groups using cohomology. We now introduce the language of homological algebra, which will be central to our approach.

Definition 9.6. A (cochain) complex X of abelian groups is a sequence

$$\cdots \to X^{-1} \xrightarrow{d^{-1}} X^0 \xrightarrow{d^0} X^1 \xrightarrow{d^1} \cdots,$$

such that the *differential* satisfies $d^{i+1}d^i = 0$ for each i.

Notation 9.7. We often refer to the entire complex as $X^\bullet$, where the '$\bullet$' is in the location of the indices. We will also often omit indices, e.g. by writing d for d^i and $d \cdot d = d^2 = 0$. Note that some authors write $H_i := H^{-i}$, and similarly for X_i, so that the differential lowers degree. Our convention, however, is that differentials raise degree.

Definition 9.8. The *ith cohomology group* is $H^i(X) := \mathrm{Ker}(d^i)/\mathrm{Im}(d^{i-1})$.

These are, in fact, the invariants we are after, but X is a "richer" object, so it is better to pass to cohomology at the very end of our processes. We now introduce the important idea of a null-homotopy of a map of chain complexes.

Definition 9.9. A map f such that the diagram

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & X^{-1} & \xrightarrow{d^{-1}} & X^0 & \xrightarrow{d^0} & X^1 & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f^{-1}} & & \downarrow{\scriptstyle f^0} & & \downarrow{\scriptstyle f^1} & & \\
\cdots & \longrightarrow & Y^{-1} & \xrightarrow{d^{-1}} & Y^0 & \xrightarrow{d^0} & Y^1 & \longrightarrow & \cdots
\end{array}$$

commutes is a *map of complexes*. Note that f induces a map of cohomologies because both the kernel and image of the differentials in $X^\bullet$ are preserved in $Y^\bullet$ by commutativity. A map h as in the following diagram

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & X^{-1} & \xrightarrow{d^{-1}} & X^0 & \xrightarrow{d^0} & X^1 & \longrightarrow & \cdots \\
 & \swarrow & \downarrow{\scriptstyle f^{-1}} & \overset{h^0}{\swarrow} & \downarrow{\scriptstyle f^0} & \overset{h^1}{\swarrow} & \downarrow{\scriptstyle f^1} & \swarrow & \\
\cdots & \longrightarrow & Y^{-1} & \xrightarrow{d^{-1}} & Y^0 & \xrightarrow{d^0} & Y^1 & \longrightarrow & \cdots
\end{array}$$

such that $dh + hd = f$, or more precisely, $d^i h^{i+1} + h^i d^{i+1} = f^{i+1}$ for each i, is a *null-homotopy of f*.

LEMMA 9.10. *If f is null-homotopic, then the induced map on cohomology $H^i(X) \xrightarrow{H^i(f)} H^i(Y)$ is zero for all i.*

PROOF. Let $x \in X^i$ such that $dx = 0$. Then $f(x) = (dh + hd)(x) = d(h(x))$, so $f(x) \in \mathrm{Im}(d^{i-1})$, and hence $f(x) = 0$ in $H^i(Y)$. □

Now, our guiding principal here is that for algebra, isomorphism is a much better notion than equality, which refers to sets without structure. Thus, if $f \simeq g$, i.e., f is homotopic to g by which we mean that there exists a null-homotopy of $f - g$, then no test of actual mathematics can distinguish f and g anymore.

We'd like to define some notion of "cokernel" for a map of complexes. A bad idea is, for a map $f\colon X \to Y$ of complexes, to form $\mathrm{Coker}(f)$. A better idea is the following:

DEFINITION 9.11. The *homotopy cokernel* or *cone* $\mathrm{hCoker}(f) = \mathrm{Cone}(f)$ has the universal property that maps of chain complexes $\mathrm{hCoker}(f) \to Z$ are equivalent to maps $Y \to Z$ along with the data of a null-homotopy of $X \to Z$, which we note yields the following commutative diagram:

$$\begin{array}{ccc} X & \longrightarrow & Z \\ \downarrow{\scriptstyle f} & \nearrow & \\ Y. & & \end{array}$$

Note the similarity with the universal property of an ordinary cokernel.

LECTURE 10

Homotopy, Quasi-Isomorphism, and Coinvariants

Please note that proofs of many of the claims in this lecture are left to Problem Set 5.

Recall that a sequence of abelian groups with differential d is a complex if $d^2 = 0$, $f\colon X \to Y$ is a morphism of chain complexes if $df = fd$, and h is a null-homotopy (of f) if $dh + hd = f$, which we illustrate in the following diagram:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & X^{-1} & \xrightarrow{d} & X^0 & \xrightarrow{d} & X^1 & \longrightarrow & \cdots \\ & \swarrow & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle h} & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle h} & \downarrow{\scriptstyle f} & \swarrow & \\ \cdots & \longrightarrow & Y^{-1} & \xrightarrow{d} & Y^0 & \xrightarrow{d} & Y^1 & \longrightarrow & \cdots . \end{array}$$

The invariants of a chain complex are the homology groups

$$H^i(X) := \operatorname{Ker}(d\colon X^i \to X^{i+1}) / \operatorname{Im}(d\colon X^{i-1} \to X^i),$$

and for $f, g\colon X \rightrightarrows Y$, we say that $f \simeq g$, that is, f and g are homotopic, if and only if there exists a null-homotopy of $f - g$, which by Lemma 9.10, forces f and g to give the same map on cohomology.

For a finite group G and extension L/K of local fields with $G = \operatorname{Gal}(L/K)$, we have $\hat{H}^0(G, L^\times) = K^\times / \mathrm{N}L^\times$ by definition. Our goal is to show that $\hat{H}^0(G, L^\times) \simeq G^{\mathrm{ab}}$ canonically, i.e., the abelianization of G. Our plan for this lecture will be to define the Tate cohomology groups $\hat{H}^i$ for each $i \in \mathbb{Z}$ (which is more complicated for non-cyclic groups), and then use them to begin working towards a proof of this fact.

Recall that out basic principle was that, given a homotopy $h\colon f \simeq g$, f and g are now indistinguishable for all practical purposes (which we will take on faith). An application of this principle is the construction of cones or homotopy cokernels:

Claim 10.1. *If $f\colon X \to Y$ is a map of complexes, then* $\operatorname{hCoker}(f)$ *(a.k.a.* $\operatorname{Cone}(f)$*), characterized by the universal property that maps* $\operatorname{hCoker}(f) \to Z$ *of chain complexes are equivalent to maps $g\colon Y \to Z$ plus a null-homotopy h of $g \circ f\colon X \to Z$, exists.*

Proof. We claim that the following chain complex is $\operatorname{hCoker}(f)$:

$$\cdots \to X^0 \oplus Y^{-1} \to X^1 \oplus Y^0 \to X^2 \oplus Y^1 \to \cdots \tag{10.1}$$

with differential

$$X^{i+1} \oplus Y^i \ni \begin{pmatrix} x \\ y \end{pmatrix} \xmapsto{d} \begin{pmatrix} -dx \\ f(x) + dy \end{pmatrix} \in X^{i+2} \oplus Y^{i+1},$$

which we note increases the degree appropriately. We may summarize this differential as a matrix $\left(\begin{smallmatrix} -d & 0 \\ f & d \end{smallmatrix}\right)$, and we note that it squares to zero as

$$\begin{pmatrix} -d & 0 \\ f & d \end{pmatrix}\begin{pmatrix} -d & 0 \\ f & d \end{pmatrix} = \begin{pmatrix} d^2 & 0 \\ -fd+df & d^2 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

by the definition of a morphism of chain complexes and because both X and Y are complexes.

We now check that this chain complex satisfies the universal property of $\mathrm{hCoker}(f)$. So suppose we have a map $\mathrm{hCoker}(f) \to Z$, so that the diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & X^{i+1} \oplus Y^i & \longrightarrow & X^{i+2} \oplus Y^{i+1} & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & Z^i & \longrightarrow & Z^{i+1} & \longrightarrow & \cdots \end{array}$$

commutes. If we write such a map as $(x, y) \mapsto h(x) + g(y)$, then this means

$$dh(x) + dg(y) = d(h(x) + g(y)) = h(-dx) + g(f(x) + dy) = -h(dx) + gf(x) + g(dy).$$

Taking $x = 0$ implies $dg = gd$, so we must have $dh + hd = g \circ f$, hence h is a null-homotopy of $g \circ f$, as desired. □

Corollary 10.2. *The composition*

$$X \to Y \to \mathrm{hCoker}(f)$$

is canonically null-homotopic (as an exercise, construct this null-homotopy explicitly!).

Example 10.3. Let

$$X := (\cdots \to 0 \to A \to 0 \to \cdots) \quad \text{and} \quad Y := (\cdots \to 0 \to B \to 0 \to \cdots)$$

for finite abelian groups A and B in degree 0, and let $f\colon A \to B$. Then

$$\mathrm{hCoker}(f) = (\cdots \to 0 \to A \xrightarrow{f} B \to 0 \to \cdots),$$

with B in degree 0. Then we have

$$H^0\mathrm{hCoker}(f) = \mathrm{Coker}(f) \quad \text{and} \quad H^{-1}\mathrm{hCoker}(f) = \mathrm{Ker}(f),$$

so we see that the language of chain complexes generalizes prior concepts.

Notation 10.4. For a chain complex X, let $X[n]$ denote the *shift* of X by n places, that is, the chain complex with X^{i+n} in degree i, with the differential $(-1)^n d$ (where d denotes the differential for X). So for instance, $X[1] = \mathrm{hCoker}(X \to 0)$. The content of this is that giving a null-homotopy of $0\colon X \to Y$ is equivalent to giving a map $X[1] \to Y$.

Lemma 10.5. *For all maps $f\colon X \to Y$, the sequence*

$$H^iX \to H^iY \to H^i\mathrm{hCoker}(f)$$

is exact for all i.

Proof. The composition is zero by Lemma 9.10 because $X \to Y \to \mathrm{hCoker}(f)$ is null-homotopic. To show exactness, let $y \in Y^i$ such that $dy = 0$, and suppose that its image in $H^i\mathrm{hCoker}(f)$ is zero, so that

$$\begin{pmatrix} 0 \\ y \end{pmatrix} = \begin{pmatrix} -d & 0 \\ f & d \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -d\alpha \\ f(\alpha) + d\beta \end{pmatrix}$$

for some $\alpha \in X^i$ with $d\alpha = 0$ and $\beta \in Y^{i-1}$. Then $f(\alpha) + d\beta = y$ implies $f(\alpha) = y$ in H^iY, as desired. □

CLAIM 10.6. *There is also a notion of the* homotopy kernel $\mathrm{hKer}(f)$*, defined by the universal property that maps $Z \to \mathrm{hKer}(f)$ are equivalent to maps $Z \to X$ plus the data of a null-homotopy of the composition $Z \to X \to Y$. In particular,* $\mathrm{hKer}(f) = \mathrm{hCoker}(f)[-1]$.

EXAMPLE 10.7. Let $f\colon A \to B$ be a map of abelian groups (in degree 0 as before). Then

$$\mathrm{hCoker}(f) = (\cdots \to 0 \to A \xrightarrow{f} B \to 0 \to 0 \to \cdots)$$
$$\mathrm{hKer}(f) = (\cdots \to 0 \to 0 \to A \xrightarrow{f} B \to 0 \to \cdots),$$

where $\mathrm{hKer}(f)^0 = A$. The homotopy cokernel also recovers the kernel and cokernel in its cohomology.

CLAIM 10.8. *The composition*

$$X \xrightarrow{f} Y \to \mathrm{hCoker}(f)$$

is null-homotopic, so there exists a canonical map

$$X \to \mathrm{hKer}(Y \to \mathrm{hCoker}(f)),$$

where we refer to the latter term as "the mapping cylinder." This map is a homotopy equivalence.

DEFINITION 10.9. A map $f\colon X \to Y$ is a *homotopy equivalence* if there exist a map $g\colon Y \to X$ and homotopies $gf \simeq \mathrm{id}_X$ and $fg \simeq \mathrm{id}_Y$, in which case we write $X \simeq Y$.

It is a *quasi-isomorphism* if $H^i(f)\colon H^i(X) \xrightarrow{\sim} H^i(Y)$ is an isomorphism for each i (i.e., X and Y are equal at the level of cohomology).

CLAIM 10.10. *If $f\colon X \to Y$ is a homotopy equivalence, then it is a quasi-isomorphism.*

PROOF. This is an immediate consequence of Lemma 9.10, which ensures that f and g are inverses at the level of cohomology. □

COROLLARY 10.11. *Given $f\colon X \to Y$, there is a long exact sequence*

$$\cdots \to H^{i-1}\mathrm{hCoker}(f) \to H^iX \to H^iY \to H^i\mathrm{hCoker}(f) \to H^{i+1}X \to \cdots.$$

PROOF. Letting g denote the map $Y \to \mathrm{hCoker}(f)$, the composition

$$Y \xrightarrow{g} \mathrm{hCoker}(f) \to \mathrm{hCoker}(g) = \mathrm{hKer}(g)[1] \simeq X[1]$$

is null-homotopic by Corollary 10.2, and the homotopy equivalence is by Claim 10.8. So by Lemma 10.5, the sequence

$$H^iY \to H^i\mathrm{hCoker}(f) \to H^iX[1] = H^{i+1}X$$

is exact; a further application of Lemma 10.5 shows the claim. □

CLAIM 10.12. *Suppose $f^i\colon X^i \hookrightarrow Y^i$ is injective for all i. Then* $\mathrm{hCoker}(f) \to Y/X$ *(i.e., the complex with Y^i/X^i in degree i) is a quasi-isomorphism.*

EXAMPLE 10.13. If $f\colon A \hookrightarrow B$ is a map of abelian groups in degree 0, then the map $\mathrm{hCoker}(f) \to B/A$ looks like

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & A & \hookrightarrow & B & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & B/A & \longrightarrow & 0 & \longrightarrow & \cdots . \end{array}$$

It's easy to see that this is indeed a quasi-isomorphism. Note that there is a dual statement, that if f^i is surjective in each degree, then the homotopy kernel is quasi-isomorphic to the naive kernel.

REMARK 10.14. If A is an associative algebra (e.g. $\mathbb{Z}$ or $\mathbb{Z}[G]$), then we can have chain complexes of A-modules

$$\cdots \to X^{-1} \xrightarrow{d} X^0 \xrightarrow{d} X^1 \to \cdots ,$$

where the X^i are A-modules and d is a map of A-modules. Here the cohomologies will also be A-modules.

Now, our original problem was to define Tate cohomology for a finite group G acting on some A. Note that

$$\hat{H}^0(G, A) = A^G/\mathrm{N}(A) = \mathrm{Coker}(\mathrm{N}\colon A \to A^G).$$

In fact, we can do better than $\mathrm{N}\colon A \to A^G$; the norm map factors through what we will call the coinvariants.

DEFINITION 10.15. The *coinvariants* of A are $A_G := A\big/\sum_{g\in G}(g-1)A$, which satisfies the universal property that it is the maximal quotient of A with $gx = x$ holding for all $x \in A$ and $g \in G$.

Note that we can think of the invariants A^G as being the intersection of the kernels of each $(g-1)A$, so it is the maximal submodule of A for which $gx = x$ holds similarly. Then the norm map factors as

$$\begin{array}{ccc} A & \xrightarrow{\mathrm{N}} & A^G \\ \downarrow{\scriptstyle \mathrm{N}} & \nearrow & \\ A_G. & & \end{array}$$

Our plan is now to define derived (complex) versions of A_G and A^G called $A_{\mathrm{h}G} \xrightarrow{\mathrm{N}} A^{\mathrm{h}G}$, and Tate cohomology will be the homotopy cokernel of this map. The basic observation is that $\mathbb{Z}$ is a G-module (i.e. $\mathbb{Z}[G]$ acts on $\mathbb{Z}$) in a trivial way, with every $g \in G$ as the identity automorphism. If M is a G-module, then $M^G = \mathrm{Hom}_G(\mathbb{Z}, M)$ (because the image of 1 in M must be G-invariant and corresponds to the element of M^G) and $M_G = M \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. Indeed, let $I \subseteq A$ be an ideal acting on M. Then $A/I \otimes_A M = M/IM$ by the right-exactness of tensor products. Here, $\mathbb{Z} = \mathbb{Z}[G]/I$, where I is the "augmentation ideal" generated by elements $g - 1$ and therefore $M_G = M/I$ as desired.

Now we have the general problem where A is an associative algebra and M an associative A-module, and we would like the "derive" the functors $- \otimes_A M$ and $\mathrm{Hom}_A(M, -)$. These should take chain complexes of A-modules and produce complexes of abelian groups, preserving cones and quasi-isomorphisms. We'll begin working on this in the next lecture.

LECTURE 11

The Mapping Complex and Projective Resolutions

Throughout, A will be an associative algebra (which might not be commutative), e.g. $A = \mathbb{Z}, \mathbb{Z}[G]$, where G is a (usually finite) group. Recall that we wanted rules by which $X \mapsto X^{\mathrm{h}G}, X_{\mathrm{h}G}$, where X is a complex of G-modules and $X^{\mathrm{h}G}$ and $X_{\mathrm{h}G}$ are complexes of abelian groups. Our guiding "axioms" for this construction will be:

(1) If X is *acyclic*, i.e., $H^i(X) = 0$ for all $i \in \mathbb{Z}$, then we'd like $X_{\mathrm{h}G}$ and $X^{\mathrm{h}G}$ to be acyclic also.
(2) Both $X^{\mathrm{h}G}$ and $X_{\mathrm{h}G}$ should commute with cones, i.e., if $f\colon X \to Y$ is a map of complexes of G-modules, then $\mathrm{hCoker}(f)^{\mathrm{h}G} \simeq \mathrm{hCoker}(X^{\mathrm{h}G} \to Y^{\mathrm{h}G})$. This condition is relatively simple to satisfy, as it merely amounts to commuting with finite direct sums and shifts by the proof of Claim 10.1.
(3) The construction should have something to do with invariants and coinvariants. Namely, if $X = (\cdots \to 0 \to M \to 0 \to \cdots)$ is in degree 0 only, then $H^0(X^{\mathrm{h}G}) = M^G$ and

$$H^0(X_{\mathrm{h}G}) = M_G = \mathbb{Z} \otimes_{\mathbb{Z}[G]} M = M \Big/ \sum_{g \in G} (g-1)M.$$

A naive and incorrect attempt would be to define

$$X^{\mathrm{h}G} := (\cdots \to (X^{-1})^G \xrightarrow{d} (X^0)^G \xrightarrow{d} (X^1)^G \to \cdots),$$

for a chain complex

$$X := (\cdots \to X^{-1} \xrightarrow{d} X^0 \xrightarrow{d} X^1 \to \cdots).$$

This trivially satisfies (2) and (3), and note that it is well-defined as the differentials commute with the group automorphisms. A weak version of (1) is satisfied: if $X \simeq 0$, i.e., the zero complex, then $X^{\mathrm{h}G}$ and $X_{\mathrm{h}G}$ are also homotopy equivalent to 0. However, this construction doesn't preserve acyclic complexes. Explicitly, if $G := \mathbb{Z}/2\mathbb{Z}$ acts on $\mathbb{Z}$ via multiplication by 1 and -1, then we have

$$(\cdots \to 0 \to \mathbb{Z} \xrightarrow{\times 2} \mathbb{Z} \to \mathbb{Z}/2 \to 0 \to \cdots)^{\mathrm{h}G} = (\cdots \to 0 \to 0 \to 0 \to \mathbb{Z}/2 \to 0 \to \cdots)$$

which is not acyclic!

A more hands-off approach is to note that if this construction preserved acyclic complexes, then since the cone of any map of acyclic complexes must be acyclic by the construction in (10.1), and since it commutes with cones by assumption, it would also preserve quasi-isomorphisms by Corollary 10.11. But we saw in Claim 10.12 that for an injection $M \xhookrightarrow{i} N$ of G-modules, we have $\mathrm{hCoker}(i) \xrightarrow{\mathrm{qis}} \mathrm{Coker}(i) = N/M$ (where henceforth "qis" denotes a quasi-isomorphism). Thus, if the naive invariants preserved acyclic complexes, then it would also preserve cokernels, which we know to be false.

Observe that, for A an associative algebra, if $A = \mathbb{Z}[G]$, then $M \mapsto M^G = \mathrm{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, M)$, where G is given the trivial G-action. Thus, we have a general class of problems for every associative algebra A and A-module M.

DEFINITION 11.1. Let X and Y be complexes of A-modules. Then the *mapping complex* $\underline{\mathrm{Hom}}_A(X, Y)$ is the complex of abelian groups defined by $\underline{\mathrm{Hom}}^i_A(X, Y) := \prod_{j\in\mathbb{Z}} \mathrm{Hom}_A(X^j, Y^{j+i})$, with differential $d^i f := df - (-1)^i fd$ (the signs alternate to ensure that the differential squares to zero). We can visualize this as follows:

$$\begin{array}{ccccccc}
 & \overbrace{\cdots : \cdots \to \cdots} & & \overbrace{\cdots : \cdots \to \cdots} & & \overbrace{\cdots : \cdots \to \cdots} & \\
\to h^{-1} : X^{-1} \to Y^{-2} & \xrightarrow{dh^{-1}+h^0 d} & f^{-1} : X^{-1} \to Y^{-1} & \xrightarrow{df^{-1}-f^0 d} & g^{-1} : X^{-1} \to Y^0 & \to & \\
\to \quad h^0 : X^0 \to Y^{-1} & \xrightarrow{dh^0+h^1 d} & f^0 : X^0 \to Y^0 & \xrightarrow{df^0-f^1 d} & g^0 : X^0 \to Y^1 & \to & \\
\to \quad h^1 : X^1 \to Y^0 & \xrightarrow{dh^1+h^2 d} & f^1 : X^1 \to Y^1 & \xrightarrow{df^1-f^2 d} & g^1 : X^1 \to Y^2 & \to & \\
\underbrace{\cdots : \cdots \to \cdots} & & \underbrace{\cdots : \cdots \to \cdots} & & \underbrace{\cdots : \cdots \to \cdots} & & \\
\cap & & \cap & & \cap & & \\
\to \prod_{i\in\mathbb{Z}} \mathrm{Hom}(X^i, Y^{i-1}) & \xrightarrow{h\mapsto dh+hd} & \prod_{i\in\mathbb{Z}} \mathrm{Hom}(X^i, Y^i) & \xrightarrow{f\mapsto df-fd} & \prod_{i\in\mathbb{Z}} \mathrm{Hom}(X^i, Y^{i+1}) & \to & \\
\| & & \| & & \| & & \\
\underline{\mathrm{Hom}}^{-1}(X, Y) & & \underline{\mathrm{Hom}}^0(X, Y) & & \underline{\mathrm{Hom}}^1(X, Y) & &
\end{array}$$

where d denotes the respective differentials for X and Y.

CLAIM 11.2. *For any complexes X and Y of A-modules, $\underline{\mathrm{Hom}}_A(X, Y)$ is a complex .*

Note that a map of complexes $f : X \to Y$ is equivalent to an element $f = (f^i) \in \underline{\mathrm{Hom}}^0_A(X, Y)$ such that $df = 0$, where d denotes the differential on $\underline{\mathrm{Hom}}(X, Y)$. A null-homotopy of f is likewise equivalent to an element $h \in \underline{\mathrm{Hom}}^{-1}_A(X, Y)$ such that $dh = f$, with d as before. Thus, $H^0\underline{\mathrm{Hom}}(X, Y)$ is equivalent to the equivalence classes of maps $X \to Y$ modulo homotopy. This construction therefore generalizes many important notions in homological algebra.

EXAMPLE 11.3. If $X := (\cdots \to 0 \to A \to 0 \to \cdots)$, with A in degree 0, then $\underline{\mathrm{Hom}}_A(X, Y) = Y$. Thus, X is what we will call projective.

DEFINITION 11.4. A complex P of A-modules is *projective* (or *homotopy projective*, or *K-projective*, etc.; the notion was defined by Spaltenstein) if for every acyclic complex Y of A-modules, $\underline{\mathrm{Hom}}_A(P, Y)$ is also acyclic.

The issue above is that $\mathbb{Z}$ is not projective as a complex of $\mathbb{Z}[G]$-modules. We will show that we can in some sense replace $\mathbb{Z}$ "uniquely" by a projective module.

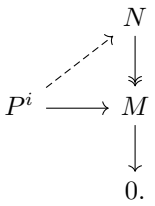
LEMMA 11.5. *If P is a complex of A-modules with $P^i = 0$ for all $i \gg 0$ (i.e., the nonzero elements of P are bounded above in index), and P^i is projective as an A-module for all i, then P is projective (as a complex).*

We recall the following definition:

DEFINITION 11.6. An A-module P^i is *projective* as an A-module if any of the following equivalent conditions hold:

(1) $\mathrm{Hom}_A(P^i, -)$ preserves surjections;
(2) $\mathrm{Hom}_A(P^i, -)$ is an exact functor;

(3) P^i is a direct summand of a free module;
(4) Given any surjection $N \twoheadrightarrow M$, every map $P^i \to M$ of A-modules lifts to a map $P^i \to N$ such that the following diagram commutes:



We briefly justify these equivalences. Evidently (1) and (4) are equivalent, as (4) states that if $N \twoheadrightarrow M$ then $\mathrm{Hom}_A(P^i, N) \twoheadrightarrow \mathrm{Hom}_A(P^i, M)$. Condition (2) is trivially equivalent to (1). To show (3), take $M := P^i$ and N to be some free module surjecting onto P^i (for instance, take all elements of P^i as a basis, and then just send corresponding elements to each other). Then (4) gives a splitting of $N \twoheadrightarrow P^i$, realizing P^i as a direct summand of M. It's easy to see that direct summands of projective modules are projective, so to show the converse, we simply note that free modules are projective.

Claim 11.7. *An A-module P is projective as an A-module if and only if it is projective as a complex in degree* 0.

Proof. If P is projective as a complex in degree 0, then let $f\colon N \twoheadrightarrow M$ be a surjection, and form the acyclic complex

$$X := (\cdots \to 0 \to \mathrm{Ker}(f) \to N \to M \to 0 \to \cdots).$$

Then $\underline{\mathrm{Hom}}_A(P, X)$ is

$$\cdots \to 0 \to \mathrm{Hom}_A(P, \mathrm{Ker}(f)) \to \mathrm{Hom}_A(P, N) \to \mathrm{Hom}_A(P, M) \to 0 \to \cdots,$$

and so $\mathrm{Hom}_A(P^i, -)$ preserves surjections and P is projective as an A-module by definition.

Conversely, if $X := (\cdots \to X^{-1} \xrightarrow{d^{-1}} X^0 \xrightarrow{d^0} X^1 \to \cdots)$ is an acyclic complex and P is projective as an A-module, then

$$\underline{\mathrm{Hom}}_A(P, X) = (\cdots \to \mathrm{Hom}_A(P, X^{-1}) \to \mathrm{Hom}_A(P, X^0) \to \mathrm{Hom}_A(P, X^1) \to \cdots),$$

which is acyclic as if $X^{i-1} \twoheadrightarrow \mathrm{Ker}(X^i \to X^{i+1})$, then

$$\mathrm{Hom}(P, X^{i-1}) \twoheadrightarrow \mathrm{Hom}(P, \mathrm{Ker}(X^i \to X^{i+1})) = \mathrm{Ker}(\mathrm{Hom}(P, X^i) \to \mathrm{Hom}(P, X^{i+1}))$$

as $\mathrm{Hom}(P, -)$ is exact and so preserves kernels by assumption. Thus $\underline{\mathrm{Hom}}_A(P, X)$ is also acyclic and P is projective as a complex in degree 0, as desired. □

Proof (of Lemma). Let Y be an acyclic complex of A-modules. We need the following claim:

Claim 11.8. *Every map $P \to Y$ is null-homotopic.*

Proof. Let $f\colon P \to Y$. We construct a null-homotopy h of f by descending induction. For the base case, note that for all $i \gg 0$ (where this has the meaning in the statement of the lemma), we have $P^i = 0$, so $f^i = 0$, and therefore we may

take $h^i := 0$. Now suppose we have maps $h\colon P^j \to Y^{j-1}$ for all $j > i$, so that the following diagram commutes:

$$\begin{array}{ccccccccccc}
\cdots & \xrightarrow{d} & P^{i-1} & \xrightarrow{d} & P^i & \xrightarrow{d} & P^{i+1} & \xrightarrow{d} & \cdots \\
 & & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle ?} & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle h} & \downarrow{\scriptstyle f} & \swarrow{\scriptstyle h} & \\
\cdots & \xrightarrow{d} & Y^{i-1} & \xrightarrow{d} & Y^i & \xrightarrow{d} & Y^{i+1} & \xrightarrow{d} & \cdots .
\end{array}$$

We'd like to construct a map $h\colon P^i \to Y^{i-1}$ such that $dh + hd = f$. Observe that, for all $x \in P^i$, we have

$$(d(f - hd))(x) = ((df - (f - hd)d)(x) = (df - fd)(x) = 0$$

by the inductive hypothesis. Since $(f - hd)\colon P^i \to \mathrm{Ker}(d\colon Y^i \to Y^{i+1})$ by the previous assertion and there is a surjection $d\colon Y^{i-1} \to \mathrm{Ker}(d\colon Y^i \to Y^{i+1})$, the map $f - hd$ lifts to a map $h\colon P^i \to Y^{i-1}$ such that $dh = f - hd$ as P^i is projective by assumption. Thus, $dh + hd = f$ and h defines a null-homotopy of f, as desired. □

By the claim, $H^0(\underline{\mathrm{Hom}}_A(P, Y)) = \{P \to Y\} = 0$ and $H^i(\underline{\mathrm{Hom}}_A(P, Y)) = H^0(\underline{\mathrm{Hom}}_A(P, Y[i])) = 0$ as $Y[i]$ is also acyclic for each i. Thus,the cohomologies vanish for each i and $\underline{\mathrm{Hom}}_A(P, Y)$ is therefore acyclic, so Y is projective as desired. □

Our plan, approximately, will be to show that every X is quasi-isomorphic to a projective complex P, that is, $P \xrightarrow{\mathrm{qis}} X$, called a *projective resolution* of X. Moreover, P will be "unique" or "derived" in a sense to be defined later on. Then we get some "corrected" version called $\underline{\mathrm{Hom}}_A^{\mathrm{der}}(X, Y) := \underline{\mathrm{Hom}}_A(P, Y)$. Letting $A := \mathbb{Z}[G]$ and choosing some projective resolution $P \xrightarrow{\mathrm{qis}} \mathbb{Z}$ (which will be very canonical, and even simpler for finite groups, though not exactly unique, although it will not matter for cohomology), we can define $X^{\mathrm{h}G} := \underline{\mathrm{Hom}}_G(P, X)$. This will satisfy all of our axioms, as it has something to do with invariants since P is akin to $\mathbb{Z}$ and preserves acyclic complexes as P is projective!

The following proposition is sufficient to show the first point, as the complex we are interested in is $\mathbb{Z}$ in degree 0, which is trivially bounded above.

Proposition 11.9. *Let X be a complex of A-modules, and suppose X is bounded above, that is, $X^i = 0$ for all $i \gg 0$ as before. Then there exists a projective resolution $P \xrightarrow{\mathrm{qis}} X$.*

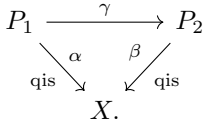
Proof. Without loss of generality, we may assume that X is bounded above at index 0. Let P^0 be a free module surjecting onto X^0 via a map α^0 (one exists as before; simply take generators, so that the kernel consists of the relations among the generators). Then take P^{-1} to be a free module surjecting onto $P^0 \times_{X^0} X^{-1}$ as before (i.e., the fibre product over X^0):

$$\begin{array}{ccccccc}
P^{-1} & \longrightarrow & P^0 & \longrightarrow & 0 & \longrightarrow & \cdots \\
\vdots & & \downarrow{\scriptstyle \alpha^0} & & \downarrow & & \\
X^{-1} & \longrightarrow & X^0 & \longrightarrow & 0 & \longrightarrow & \cdots .
\end{array}$$

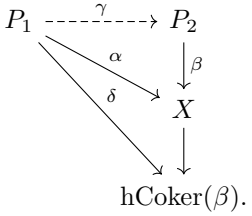
This construction preserves cohomology, as $H^0X = X^0/\mathrm{Im}(X^{-1}) = P^0/P^{-1} = H^0P$, since P^{-1} surjects onto $\mathrm{Ker}(\alpha^0)$ and has image in $P^0/\mathrm{Ker}(\alpha^0) \simeq X^0$ equal to X^{-1} (as $P^0 \twoheadrightarrow X^0$). Since $P^{-1} \twoheadrightarrow X^{-1}$, we may iterate this process to construct a projective resolution P of X, as desired. □

The second claim was about uniqueness of the projective resolution, which is given by the following lemma:

LEMMA 11.10. *Suppose that P_1 and P_2 are projective resolutions of a complex X of A-modules. Then there exists a homotopy equivalence γ such that the following diagram commutes up to homotopy, that is, $\beta\gamma \simeq \alpha$:*



PROOF. Consider the following diagram:



Since β is a quasi-isomorphism by assumption, hCoker(β) is acyclic by Corollary 10.11. By Claim 11.8, the composition δ is null-homotopic, hence by Claim 10.8, there is a canonical map

$$P_1 \xrightarrow{\gamma} \mathrm{hKer}(X \to \mathrm{hCoker}(\beta)) \simeq P_2$$

via homotopy equivalence, as desired. By symmetry, such a map exists in the opposite direction, hence γ is a homotopy equivalence and the diagram trivially commutes up to homotopy. □

We can now ask how unique γ is here. The answer is given by the following:

CLAIM 11.11. *All such γ are homotopic.*

PROOF. We imitate the proof of Lemma 11.10 with individual morphisms replaced by $\underline{\mathrm{Hom}}$-complexes. We have maps

$$\underline{\mathrm{Hom}}(P_1, P_2) \xrightarrow[\text{qis}]{\beta_*} \underline{\mathrm{Hom}}(P_1, X) \to \underline{\mathrm{Hom}}(P_1, \mathrm{hCoker}(\beta)) = \mathrm{hCoker}(\beta_*),$$

where β_* is given by composition with β, and the final identification is for formal reasons. Since P_2 is projective, the last complex is acyclic (by definition), so ψ is a quasi-isomorphism by Corollary 10.11, hence an isomorphism on homotopy classes of maps. In particular,

$$H^0\underline{\mathrm{Hom}}(P_1, P_2) = H^0\underline{\mathrm{Hom}}(P_2, X),$$

so since we have a given map in $H^0\underline{\mathrm{Hom}}(P_2, X)$, the induced map in $H^0\underline{\mathrm{Hom}}(P_1, P_2)$ is well-defined up to homotopy (as noted in the discussion following Definition 11.1). □

In fact, we can show that all such homotopies between homotopies are homotopic, and so on, so this is the best outcome we could possibly hope for in establishing uniqueness.

DEFINITION 11.12. The *ith* Ext-*group* of two chain complexes of A-modules M and N is defined as $\mathrm{Ext}_A^i(M,N) := H^i\underline{\mathrm{Hom}}(P,N)$, where P is some projective resolution of M.

As we just showed, this definition is independent of which P we choose.

LECTURE 12

Derived Functors and Explicit Projective Resolutions

Let X and Y be complexes of A-modules. Recall that in the last lecture we defined $\underline{\mathrm{Hom}}_A(X,Y)$, as well as $\underline{\mathrm{Hom}}_A^{\mathrm{der}}(X,Y) := \underline{\mathrm{Hom}}_A(P,Y)$ for a projective complex $P \xrightarrow{\mathrm{qis}} X$, i.e., a *projective resolution* of X. We also defined the Ext-*groups* $\mathrm{Ext}_A^i(X,Y) := H^i\underline{\mathrm{Hom}}_A^{\mathrm{der}}(X,Y)$. The most important example in this case is $A := \mathbb{Z}[G]$, where $X^{\mathrm{h}G} := \underline{\mathrm{Hom}}_A^{\mathrm{der}}(\mathbb{Z},X)$ are the *homotopy invariants* of X. This construction has the basic properties that $\underline{\mathrm{Hom}}_A^{\mathrm{der}}(X,-)$ preserves quasi-isomorphisms, and $P \xrightarrow{\mathrm{qis}} X$ is unique up to homotopy, and such homotopies are unique up to homotopy, which are unique up to homotopy, and so on.

As an aside, note that we can actually define the derived functor $\underline{\mathrm{Hom}}^{\mathrm{der}}(X,-)$ more canonically, without choosing a particular projective resolution, via

$$\underline{\mathrm{Hom}}^{\mathrm{der}}(X,Y) := \varinjlim_{\substack{P \xrightarrow{\mathrm{qis}} X \\ \text{projective}}} \underline{\mathrm{Hom}}(P,Y),$$

where the P are ordered by maps of chain complexes

$$P' \longrightarrow P \xrightarrow{\mathrm{qis}} X, \qquad P' \xrightarrow[\mathrm{qis}]{} X$$

which forcibly removes the choice of P.

Claim 12.1. *Suppose we have a map of chain complexes $f\colon X_1 \to X_2$, which have projective resolutions P_1 and P_2, respectively. Then we have a map $\varphi\colon P_1 \to P_2$ such that the following diagram commutes up to homotopy:*

$$\begin{array}{ccc} X_1 & \xrightarrow{f} & X_2 \\ {\scriptstyle\mathrm{qis}}\uparrow & & \uparrow{\scriptstyle\mathrm{qis}} \\ P_1 & \xrightarrow{\varphi} & P_2. \end{array}$$

Moreover, such a map is unique up to homotopy.

Proof. Because the derived functor preserves quasi-isomorphisms, the induced map of complexes of maps

$$\underline{\mathrm{Hom}}(P_1,P_2) \xrightarrow{\mathrm{qis}} \underline{\mathrm{Hom}}(P_1,X_2)$$

is a quasi-isomorphism. We are given a map, namely the composition $P_1 \to X_1 \to X_2$, which is killed by the differential since it is a map of chain complexes, and therefore defines a cohomology class in $H^0\underline{\mathrm{Hom}}(P_1,X_2)$. So there is some cohomology class in $H^0\underline{\mathrm{Hom}}(P_1,P_2)$ which is a lift of that map through P_2, which is well-defined and unique up to homotopy. □

The upshot is that, for every chain complex Y, we get a map

$$\underline{\mathrm{Hom}}_A^{\mathrm{der}}(X_2, Y) \to \underline{\mathrm{Hom}}_A^{\mathrm{der}}(X_1, Y)$$

by pulling back along φ. A quick "application" is the following:

Claim 12.2. *If $H \subseteq G$ is a subgroup and X is a complex of G-modules, then we get a* restriction map $X^{\mathrm{h}G} \to X^{\mathrm{h}H}$ *(which is well-defined up to homotopy).*

Intuitively, something which is G-invariant is also H-invariant.

Proof. Consider

$$\mathbb{Z}[G/H] = \{f \colon G/H \to \mathbb{Z} \mid f \text{ nonzero at finitely many points}\},$$

which has a G-action via translations and is equivalent to the induced module from H to G by the trivial module, $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} \mathbb{Z}$.

Claim 12.3. $\underline{\mathrm{Hom}}_G^{\mathrm{der}}(\mathbb{Z}[G/H], X) \simeq X^{\mathrm{h}H}$ *is a quasi-isomorphism.*

Proof. Let $P_H \xrightarrow{\mathrm{qis}} \mathbb{Z}$, where P_H is a projective complex of H-modules. Then we have an induced G-module $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} P_H$. Note that $\mathbb{Z}[G]$ is free as a $\mathbb{Z}[H]$ module, as choosing coset representatives for G/H yields a basis. Therefore, $\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} -$ preserves quasi-isomorphisms (we know this for $\mathbb{Z}[H]$, and then we may regard $\mathbb{Z}[G]$ as a direct sum of copies of $\mathbb{Z}[H]$). This implies that

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} P_H \xrightarrow{\mathrm{qis}} \mathbb{Z}[G/H],$$

which is projective as a complex of $\mathbb{Z}[G]$-modules. This is because both $\mathbb{Z}[G]$ and P_H are bounded, so it will be bounded, and inducing up to $\mathbb{Z}[G]$ preserves projective modules as we will still obtain a direct summand of a free module. Alternatively, we could use the universal property that every map to an acyclic complex is null-homotopic, as a G-equivariant map out of the induced complex is the same as an H-equivariant map out of P_H. This gives the claim, as

$$\underline{\mathrm{Hom}}_G^{\mathrm{der}}(\mathbb{Z}[G/H], X) := \underline{\mathrm{Hom}}_G(\mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} P_H, X) = \underline{\mathrm{Hom}}_H(P_H, X) =: X^{\mathrm{h}H},$$

by definition. □

The upshot is that we get a map $X^{\mathrm{h}G} \to X^{\mathrm{h}H}$ via

$$\epsilon \colon \mathbb{Z}[G/H] \to \mathbb{Z}$$
$$\sum_{g_i \in G/H} n_i g_i \mapsto \sum_i n_i,$$

which is clearly a G-equivariant map when we equip $\mathbb{Z}$ with the trivial action. By the previous discussion, we have a restriction map of derived functors

$$X^{\mathrm{h}G} = \underline{\mathrm{Hom}}_G^{\mathrm{der}}(\mathbb{Z}, X) \to \underline{\mathrm{Hom}}_G^{\mathrm{der}}(\mathbb{Z}[G/H], X) = X^{\mathrm{h}H},$$

which is well-defined up to homotopy (defined up to homotopy, etc., our "usual error"). □

Recall that everything here is a complex of abelian groups, so there is no "type incompatibility". In fact, if $H \leq G$ is finite index, then we have a G-equivariant map

$$\mathbb{Z} \xrightarrow{\kappa} \mathbb{Z}[G/H] \xrightarrow{\epsilon} \mathbb{Z}$$

$$1 \mapsto \sum_{g \in G/H} g,$$

such that the composition corresponds to multiplication by the index $[G : H]$. This gives an *inflation map* $X^{\mathrm{h}H} \to X^{\mathrm{h}G}$ such that the composition $X^{hG} \to X^{\mathrm{h}H} \to X^{\mathrm{h}G}$ is homotopic to multiplication by $[G : H]$.

More concretely, suppose we had an H-invariant object and a G-invariant object. Taking coset representatives of G/H, we could take the "relative norm" of any H-invariant element, which would yield a G-invariant element. This is precisely what our maps are doing above, and explains why the composition multiplies by $[G : H]$.

DEFINITION 12.4. $H^i(G, X) := H^i(X^{\mathrm{h}G})$ is the *(hyper-)cohomology* of G with coefficients in X.

The prefix "hyper" used to refer to an operation on complexes; if the complex was only in degree 0, it would be called "group cohomology."

CLAIM 12.5. *If X is only in non-negative degrees, that is, $X^i = 0$ for all $i < 0$, then $H^0(G, X) = H^0(X)^G$ and $H^i(G, X) = 0$ for $i < 0$.*

PROOF. Choose some projective resolution P of $\mathbb{Z}$ as a G-module, which by the construction in Proposition 11.9 can be taken to be in non-positive degrees only. By definition, $H^0(G, X)$ is equivalent to the homotopy classes of maps $f \colon P \to X$, all of which look like

$$\begin{array}{ccccccccccccc}
\cdots & \longrightarrow & P^{-2} & \longrightarrow & P^{-1} & \xrightarrow{d} & P^0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle f} & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & X^0 & \xrightarrow{d} & X^1 & \longrightarrow & X^2 & \longrightarrow & \cdots .
\end{array}$$

Thus, any homotopy of f is 0, and $H^i(G, X) = 0$ for $i < 0$ similarly. By commutativity, we must have $df = fd = 0$. It follows that such maps f are equivalent to G-equivariant maps

$$\mathbb{Z} = P^0/dP^{-1} = \mathrm{Coker}(P^{-1} \to P^0) \to \mathrm{Ker}(X^0 \to X^1) = H^0(X)$$

by quasi-isomorphism, which is equivalent to a G-invariant vector in the cohomology $H^0(X)$ (i.e., via the image of 1). □

We now turn to the problem of constructing explicit projective resolutions of $\mathbb{Z}$ as a G-Module.

EXAMPLE 12.6. Let $G := \mathbb{Z}/n\mathbb{Z}$ with generator σ. We claim that the following is a quasi-isomorphism:

$$\begin{array}{ccccccccccccc}
\cdots & \xrightarrow{\sum_i \sigma^i} & \mathbb{Z}[G] & \xrightarrow{1-\sigma} & \mathbb{Z}[G] & \xrightarrow{\sum_i \sigma^i} & \mathbb{Z}[G] & \xrightarrow{1-\sigma} & \mathbb{Z}[G] & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \epsilon} & & \downarrow & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots .
\end{array}$$

The vanishing of the negative cohomologies follows from our earlier results on Tate cohomology, and the kernel of ϵ, i.e., elements whose coordinates sum to zero, is the image of $1 - \sigma$.

COROLLARY 12.7. *If M is a G-module (thought of as a complex in degree 0, then M^{hG} is quasi-isomorphic to the complex*

$$\cdots \to 0 \to 0 \to M \xrightarrow{1-\sigma} M \xrightarrow{\sum_i \sigma^i} M \xrightarrow{1-\sigma} \cdots,$$

where the first M is in degree 0.

Note that a G-equivariant map from $\mathbb{Z}[G]$ to any object is that object. Indeed, the invariants are the zeroth cohomology group, as desired. Thus, this construction gives "half of" what we learned earlier with Tate cohomology.

Now we'd like to construct an explicit resolution for every G. Throughout, our "motto" will be that "all such things come from the bar construction." Let A be a commmutative ring, and B an A-algebra; the most important case will be $A := \mathbb{Z}$ and $B := \mathbb{Z}[G]$.

DEFINITION 12.8. For all such A and B, the *bar complex* $\mathrm{Bar}_A(B)$ is

$$\cdots \to B \otimes_A B \otimes_A B \xrightarrow{b_1 \otimes b_2 \otimes b_2 \mapsto b_1 b_2 \otimes b_3 - b_1 \otimes b_2 b_3} B \otimes_A B \xrightarrow{b_1 \otimes b_2 \mapsto b_1 b_2} B \to 0 \to \cdots$$

with B in degree 0. In general, $\mathrm{Bar}_A^{-n}(B) := B^{\otimes_A n+1}$, with differential

$$\begin{aligned} b_1 \otimes \cdots \otimes b_{n+1} \mapsto \quad & b_1 b_2 \otimes b_3 \otimes \cdots \otimes b_{n+1} \\ & - b_1 \otimes b_2 b_3 \otimes \cdots \otimes b_{n+1} \\ & + b_1 \otimes b_2 \otimes b_3 b_4 \otimes \cdots \otimes b_{n+1} \\ & - \cdots. \end{aligned}$$

It's easy enough to see that this differential squares to zero by selectively removing tensors and checking signs, so this is indeed a chain complex.

CLAIM 12.9. *$\mathrm{Bar}_A(B)$ is homotopy equivalent to zero.*

PROOF. We'd like a null-homotopy of the identity map of $\mathrm{Bar}_A(B)$, that is, a map h such that $hd + dh + \mathrm{id}$:

$$\begin{array}{ccccccccccc} \cdots & \longrightarrow & B \otimes_A B \otimes_A B & \longrightarrow & B \otimes_A B & \longrightarrow & B & \longrightarrow & 0 & \longrightarrow & \cdots \\ & \swarrow^{h^2} & \downarrow \mathrm{id} & \swarrow^{h^1} & \downarrow \mathrm{id} & \swarrow^{h^0} & \downarrow \mathrm{id} & \swarrow & \downarrow & & \\ \cdots & \longrightarrow & B \otimes_A B \otimes_A B & \longrightarrow & B \otimes_A B & \longrightarrow & B & \longrightarrow & 0 & \longrightarrow & \cdots. \end{array}$$

So define $h^0(b) := 1 \otimes b$, and $h^1(b_1 \otimes b_2) := 1 \otimes b_1 \otimes b_2$. Indeed, we then have

$$(dh' + h^0 d)(b_1 \otimes b_2) = d(1 \otimes b_1 \otimes b_2) + 1 \otimes b_1 b_2 = b_1 \otimes b_1 - 1 \otimes b_1 b_2 + 1 \otimes b_1 b_2 = b_1 \otimes b_2,$$

as desired. It's easy to show that defining h^n similarly for all n gives a null-homotopy of the identity. □

As a reformulation, consider the diagram

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & B \otimes_A B \otimes_A B & \longrightarrow & B \otimes_A B & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow d & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & B & \longrightarrow & 0 & \longrightarrow & \cdots, \end{array}$$

where d is the multiplication map in the differential. This is a homotopy equivalence, since its cone is $\mathrm{Bar}_A(B)$.

Consider each term as a bimodule (that is, a module with commuting actions on the left and right), where we multiply in the first term by B on the left, and

multiply in the last term by B on the right. These differentials are then bimodule homomorphisms. Then given a (left) B-module M, we can tensor over B with M, which yields a diagram

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & B \otimes_A B \otimes_A M & \longrightarrow & B \otimes_A M & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow{\scriptstyle b\otimes m \mapsto bm} & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & M & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

that is also a homotopy equivalence (the map $B \otimes_A M \to M$ is the "action map"; also note that these tensor products make sense since B is an A-module). The differentials are the same, except the last term is replaced with an element of m, so for instance we have

$$b_1 \otimes b_2 \otimes m \mapsto b_1 b_2 \otimes m - b_1 \otimes b_2 m.$$

In words, M is canonically homotopy equivalent to a complex where every term is of the form $B \otimes_A N$, where in this case N stands for $B \otimes_A \cdots \otimes_A B \otimes_A M$, that is, a module induced from some A-module.

We now apply this to the case where $A := \mathbb{Z}$, $B := \mathbb{Z}[G]$, and $M := \mathbb{Z}$, i.e., the trivial module. Note that this is only a quasi-isomorphism of complexes *of B-modules*, and not a homotopy equivalence, as the inverse is only A-linear, and not B-linear! Indeed, note that such an inverse would be

$$B \otimes_A M \xrightarrow{b\otimes m \mapsto bm} M \xrightarrow{m \mapsto 1 \otimes m} B \otimes_A M$$
$$b \otimes m \mapsto bm \mapsto 1 \otimes bm \neq b \otimes m = b(1 \otimes m),$$

since the action is on B, not M, and is not an action of B-modules. In general, existence of a quasi-isomorphism in one direction does not imply existence of one in the other direction, whereas by fiat homotopy equivalence includes a map in the other direction and is therefore reflexive. Also, recall that homotopy equivalence implies quasi-isomorphism.

Thus, we obtain a canonical projective resolution of $\mathbb{Z}$ by free G-modules

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & \mathbb{Z}[G^3] & \longrightarrow & \mathbb{Z}[G \times G] & \longrightarrow & \mathbb{Z}[G] & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \epsilon} & & \downarrow & & \\ \cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots, \end{array}$$

with differentials $(g_1, g_2) \mapsto g_1 g_2 - g_1$, and so forth, since G acts trivially on $\mathbb{Z}$. Note that $\mathbb{Z}[G \times G] \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}} \mathbb{Z}[G]$, since both have a basis by the elements of the product group.

This is a great explicit projective resolution of $\mathbb{Z}$ for computing group cohomology! We end up with a complex of the form

$$\cdots \to 0 \to M \to \mathbb{Z}[G] \otimes M \to \mathbb{Z}[G \times G] \otimes M \to \cdots,$$

with M in degree 0 and G finite. Elements in $\mathbb{Z}[G] \otimes M$ in the kernel of the differential are called *group n-cocycles* with coefficients in M; elements in the image of the differential are called *n-coboundaries*.

LECTURE 13

Homotopy Coinvariants, Abelianization, and Tate Cohomology

Recall that last time we explicitly constructed the homotopy invariants $X^{\mathrm{h}G}$ of a complex X of G-modules. To do this, we constructed the *bar resolution* $P_G^{\mathrm{can}} \xrightarrow{\mathrm{qis}} \mathbb{Z}$, where P_G^{can} is a canonical complex of free G-modules in non-positive degrees. Then we have a quasi-isomorphism $X^{\mathrm{h}G} \simeq \underline{\mathrm{Hom}}_G(P_G^{\mathrm{can}}, X)$.

In particular, we have

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & \mathbb{Z}[G^3] & \longrightarrow & \mathbb{Z}[G\times G] & \longrightarrow & \mathbb{Z}[G] & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \epsilon} & & \downarrow & & \\
\cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 & \longrightarrow & \cdots
\end{array}$$

for P_G^{can}, with differential of the form $(g_1, g_2) \mapsto g_1 g_2 - g_1$ (for d^{-1}; the G-action is always on the first term). Note that if G is finite, then these are all finite-rank G-modules.

For every G-module M, we have

$$\cdots \to 0 \to M \xrightarrow{m \mapsto (gm-m)_{g\in G}} \underbrace{\prod_{g\in G} M}_{\{\varphi\colon G\to M\}} \to \prod_{g,h\in G} M \to \cdots$$

via some further differential, for $M^{\mathrm{h}G}$. We can use this expression to explicitly compute the first cohomology of $M^{\mathrm{h}G}$. It turns out that a function $\varphi\colon G \to M$ is killed by this differential if it is a 1-*cocycle* (sometimes called a *twisted homomorphism*), that is, $\varphi(gh) = \varphi(g) + g \cdot \varphi(h)$ for all $g, h \in G$ via the group action. Similarly, φ is a 1-*coboundary* if there exists some $m \in M$ such that $\varphi(g) = g \cdot m - m$ for all $g \in G$. The upshot is that

$$H^1(G, M) := H^1(M^{\mathrm{h}G}) = \{\text{1-cocycles}\}/\{\text{1-coboundaries}\}.$$

As a corollary, if G acts trivially on M, then $H^1(G, M) = \mathrm{Hom}_{\mathsf{Group}}(G, M)$, since the 1-coboundaries are all trivial, and the 1-cocycles are just ordinary group homomorphisms. This also shows that zeroth cohomology is just the invariants, as we showed last lecture.

Now, our objective (from a long time ago) is to define Tate cohomology and the Tate complex for any finite group G. We'd like $\hat{H}^0(G, M) = M^G/\mathrm{N}(M) = \mathrm{Coker}(M_G \xrightarrow{N} M^G)$, because it generalizes the central problem of local class field theory for extensions of local fields. Recall that $M_G = M/(g-1)$ (equivalent to tensoring with the trivial module, and dual to invariants, which we prefer as a submodule), so that this map factors through M and induced the norm map above.

Our plan is, for a complex X of G-modules, to form

$$X_{\mathrm{h}G} \xrightarrow{\mathrm{N}} X^{\mathrm{h}G} \to X^{\mathrm{t}G} := \mathrm{hCoker(N)}.$$

Thus, we first need to define the homotopy coinvariants $X_{\mathrm{h}G}$.

Note that if M is a G-module, then $M_G = M \otimes_{\mathbb{Z}[G]} \mathbb{Z}$. Define $I_G := \mathrm{Ker}(\epsilon)$, so that we have a short exact sequence

$$0 \to I_G \to \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0$$
$$\sum_i n_i g_i \mapsto \sum_i n_i,$$

We claim that I_G is $\mathbb{Z}$-spanned by $\{g - 1 : g \in G\}$ (which we leave as an exercise). A corollary is that

$$\mathbb{Z}[G]^{\oplus G} \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$$

is exact, since $\mathbb{Z}[G]^{\oplus G} \twoheadrightarrow I_G$ via $1 \mapsto g - 1$ on the gth coordinate.

Remark 13.1. The correct algorithm for computing tensor products is as follows: recall that tensor products are right-exact, that is, they preserve surjections, and tensoring with the algebra gives the original module. To tensor with a module, take generators and relations for that module, use it to write a resolution as above, tensor with that resolution, giving a matrix over a direct sum of copies of that module, and then take the cokernel.

It would be very convenient if we could define $M_{\mathrm{h}G}$ via an analogous process for chain complexes.

Definition 13.2. If X and Y are chain complexes, then

$$(X \otimes Y)^i := \bigoplus_{j \in \mathbb{Z}} X^j \otimes Y^{i-j},$$

with differential

$$d(x \otimes y) := dx \otimes y + (-1)^j x \otimes dy$$

If X is a complex of right A-modules, and Y is a complex of left A-modules, then $X \otimes_A Y$ is defined similarly.

Note that the factor of $(-1)^j$ ensures that the differential squares to zero. Also, there is no need to worry about left and right A-modules for algebras, since left and right algebras are isomorphic via changing the order of multiplication; for G-modules, this means replacing every element with its inverse.

Now, a bad guess for $X_{\mathrm{h}G}$ would be $X \otimes_{\mathbb{Z}[G]} \mathbb{Z}$, because it doesn't preserve acyclic complexes, equivalently quasi-isomorphisms. A better guess is to take a projective resolution $P_G \simeq \mathbb{Z}$, e.g. P_G^{can}, and tensor with that instead: $X_{\mathrm{h}G} := X \otimes_{\mathbb{Z}[G]} P_G$.

Definition 13.3. A complex F of left A-modules is *flat* is for every acyclic complex Y of right A-modules, $Y \otimes_A F$ is also acyclic, that is, $- \otimes_A F$ preserves injections.

We now ask if P_G is flat. In fact:

Claim 13.4. *Any projective complex is flat.*

An easier claim is the following:

Claim 13.5. *Any complex F that is bounded above with F^i flat for all i is flat.*

To prove this claim, we will use the fact that projective modules are flat, as they are direct summands of free modules, which are trivially flat (i.e., if $F = F_1 \oplus F_2$, then $F \otimes M = (F_1 \otimes M) \oplus (F_2 \otimes M)$).

PROOF. **Case 1.** Suppose F is in degree 0 only, i.e., $F^i = 0$ for all $i \neq 0$. For every complex $Y = Y^\bullet$, we have

$$\cdots \to Y^i \otimes_A F \xrightarrow{d^i \otimes \mathrm{id}_F} Y^{i+1} \otimes_A F \to \cdots$$

for $Y \otimes_A F$. Since F is flat, we have $H^i(Y \otimes_A F) = H^i(Y) \otimes_A F$ for each i (since F flat means that tensoring with F commutes with forming kernels, cokernels and images), so if Y is acyclic, then $Y \otimes_A F$ is as well.

Case 2. Suppose F is in degrees 0 and -1 only, i.e., F is of the form

$$\cdots \to 0 \to F^{-1} \to F^0 \to 0 \to \cdots,$$

and so $F^\bullet = \mathrm{hCoker}(F^{-1} \to F^0)$. Then since tensor products commute with homotopy cokernels, we obtain

$$Y \otimes_A F = \mathrm{hCoker}(Y \otimes_A F^{-1} \to Y \otimes_A F^0),$$

so by Case 1, if Y is acyclic, then $Y \otimes_A F^0$ and $Y \otimes_A F^{-1}$ are as well, hence $Y \otimes_A F$ is as well by the long exact sequence on cohomology. A similar (inductive) argument gives the case where F is bounded.

Case 3. In the general case, form the diagram

$$\begin{array}{ccccccccccccc}
F_0 & \cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & F^0 & \longrightarrow & 0 & \longrightarrow \cdots \\
\downarrow & & & \downarrow & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & \\
F_1 & \cdots & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & F^1 & \xrightarrow{d} & F^0 & \longrightarrow & 0 & \longrightarrow \cdots \\
\downarrow & & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & \\
F_2 & \cdots & \longrightarrow & 0 & \longrightarrow & F^2 & \xrightarrow{d} & F^1 & \xrightarrow{d} & F^0 & \longrightarrow & 0 & \longrightarrow \cdots \\
\downarrow & & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow & \\
\vdots & & & \vdots & & \vdots & & \vdots & & \vdots & & \vdots &
\end{array}$$

Clearly all squares of this diagram commute, hence these are all morphisms of complexes, and $F = \varinjlim_i F_i$. Since direct limits commute with tensor products (note that is not true for inverse limits because of surjectivity), we have $Y \otimes_A F = \varinjlim_i Y \otimes_A F_i$. By Case 2, $Y \otimes_A F_i$ is acyclic for each i, so since cohomology commutes with direct limits (because they preserve kernels, cokernels, and images), if Y is acyclic, then $Y \otimes_A F$ is too. □

REMARK 13.6. Let Y be a complex of A-modules, choose a quasi-isomorphism $F \xrightarrow{\mathrm{qis}} Y$, where F is flat, and define $Y \otimes_A^{\mathrm{der}} X := F \otimes_A X$. Then this is well-defined up to quasi-isomorphism, which is well-defined up to homotopy, etc. (it's turtles all the way down!).

DEFINITION 13.7. The *ith torsion group (of Y against X)* is $\mathrm{Tor}_i^A(Y, X) := H^{-i}(Y \otimes_A^{\mathrm{der}} X)$.

DEFINITION 13.8. The *homotopy coinvariants* of a chain complex X is the complex $X_{\mathrm{h}G} := X \otimes^{\mathrm{der}}_{\mathbb{Z}[G]} \mathbb{Z} \simeq X \otimes_{\mathbb{Z}[G]} P_G$ (which we note is only well-defined up to quasi-isomorphism).

DEFINITION 13.9. $H_i(G, X) := H^{-i}(X_{\mathrm{h}G})$ (where we note that the subscript notation is preferred as $X_{\mathrm{h}G}$ is generally a complex in non-positive degrees only).

We now perform some basic calculations.

CLAIM 13.10. *If X is bounded from above by 0, then $H_0(G, X) = H^0(X)_G$ (the proof is similar to that of Claim 12.5).*

CLAIM 13.11. *$H_1(G, \mathbb{Z}) = G^{\mathrm{ab}}$, where G^{ab} denotes the abelianization of G.*

Note that this is sort of a dual statement to what we saw at the beginning of lecture; $H^1(G, M)$ had to do with maps $G \to M$, which are the same as maps from $G^{\mathrm{ab}} \to M$, and here $H_1(G, \mathbb{Z})$ is determined by the maps out of G.

PROOF. Recall the short exact sequence

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

The long exact sequence on cohomology gives an exact sequence

$$H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \to H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}).$$

We have

$$H_0(G, \mathbb{Z}[G]) = H^0(\mathbb{Z}[G])_G = \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} \mathbb{Z} = \mathbb{Z}$$

by Claim 13.10. Certainly $H_0(G, \mathbb{Z}) = H^0(\mathbb{Z})_G = \mathbb{Z}$, and $H_1(G, \mathbb{Z}[G]) = 0$ as

$$\mathbb{Z}[G]_{\mathrm{h}G} := \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} P_G = P_G \simeq \mathbb{Z}$$

is a quasi-isomorphism. Thus, our exact sequence is really

$$0 \to H_1(G, \mathbb{Z}) \xrightarrow{\sim} H_0(G, I_G) \to \mathbb{Z} \xrightarrow{\sim} \mathbb{Z},$$

which gives the noted isomorphism. The upshot is that

$$H_1(G, \mathbb{Z}) = (I_G)_G = I_G / I_G^2$$

since $M_G = M / I_G \cdot M$.

CLAIM 13.12. *The map*

$$\mathbb{Z}[G]/I_G^2 \to G^{\mathrm{ab}} \times \mathbb{Z}, \quad g \mapsto (\bar{g}, 1)$$

is an isomorphism.

This would imply that $I_G/I_G^2 = \mathrm{Ker}(\epsilon)/I_G^2 = G^{\mathrm{ab}}$, as desired.

PROOF. First note that the map above is a homomorphism. Indeed, letting $[g] \in \mathbb{Z}[G]$ denote the class of g, we have

$$[g] + [h] \mapsto (\bar{g}\bar{h}, 2)$$
$$[g] \mapsto (\bar{g}, 1)$$
$$[h] \mapsto (\bar{h}, 1)$$

for any $g, h \in G$, and the latter two images add up to the first. We claim that this map has an inverse, induced by the map

$$G \times \mathbb{Z} \to \mathbb{Z}[G]/I_G^2, \quad (g, n) \mapsto [g] + n - 1.$$

This is a homomorphism, as

$$([g] - 1)([h] - 1) = [gh] - [g] - [h] + 1 \in I_G^2,$$

and therefore

$$([g]-1)+([h]-1)\equiv[gh]-1 \bmod I_G^2,$$

as desired. Finally, they are inverses, as

$$(\bar{g},1)\mapsto[g]+1-1=[g] \quad \text{and} \quad [g]+n-1\mapsto(\bar{g},1)(1,n-1)=(\bar{g},n),$$

as desired. □

This proves the claim. □

Finally, we define the norm map $X_{\mathrm{h}G} \xrightarrow{\mathrm{N}} X^{\mathrm{h}G}$ to be the composition

$$X_{\mathrm{h}G} = X \otimes_{\mathbb{Z}[G]} P_G \to X \otimes_{\mathbb{Z}[G]} \mathbb{Z} \to \underline{\mathrm{Hom}}_{\mathbb{Z}[G]}(\mathbb{Z}, X) \to \underline{\mathrm{Hom}}_{\mathbb{Z}[G]}(P_G, X) = X^{\mathrm{h}G},$$

where the second map is via degree-wise norm maps (using tensor-hom adjunction). We then set

$$X^{\mathrm{t}G} := \mathrm{hCoker}(X_{\mathrm{h}G} \xrightarrow{\mathrm{N}} X^{\mathrm{h}G}),$$

which we claim generalizes what we had previously for cyclic groups up to quasi-isomorphism, so that we may define

$$\hat{H}^i(G,X) := H^i(X^{\mathrm{t}G}).$$

Soon we will prove:

Claim 13.13 (lcft). *For a finite group G and extension L/K of local fields,*

$$P_G \to L^\times[2]$$

is an isomorphism on Tate cohomology.

This gives that

$$\hat{H}^{-2}(G,\mathbb{Z}) \simeq \hat{H}^0(G,L^\times) = K^\times/\mathrm{N}(L^\times).$$

We have an exact sequence

$$0 = H^{-2}(\mathbb{Z}^{\mathrm{h}G}) \to \hat{H}^{-2}(G,\mathbb{Z}) \xrightarrow{\sim} \underbrace{H^{-1}(\mathbb{Z}_{\mathrm{h}G})}_{H_1(G,\mathbb{Z})=G^{\mathrm{ab}}} \to H^{-1}(\mathbb{Z}^{\mathrm{h}G}) = 0,$$

since $\mathbb{Z}^{\mathrm{h}G}$ is in non-negative degrees. Thus, for an extension L/K of local fields with Galois group G, we have

$$L^\times/\mathrm{N}(L^\times) \simeq G^{\mathrm{ab}}.$$

LECTURE 14

Tate Cohomology and K^{unr}

Let G be a finite group and X be a complex of G-modules. Let $P \xrightarrow{\mathrm{qis}} \mathbb{Z}$ be a projective complex of G-modules. Then

- $X^{\mathrm{h}G} := \underline{\mathrm{Hom}}_G(P, X)$ are the *homotopy invariants*;
- $X_{\mathrm{h}G} := P \otimes_{\mathbb{Z}[G]} X$ are the *homotopy coinvariants*;
- $X^{\mathrm{t}G} := \mathrm{hCoker}(X_{\mathrm{h}G} \xrightarrow{\mathrm{N}} X^{\mathrm{h}G})$ is the *Tate complex*.

The former two constructions preserve quasi-isomorphisms, sending acyclic complexes to acyclic complexes, as projective complexes are flat. Moreover, recall the notation

- $H^i(G, X) := H^i(X^{\mathrm{h}G})$ is *group cohomology*;
- $H_i(G, X) := H^{-i}(X_{\mathrm{h}G})$ is *group homology*;
- $\hat{H}^i(G, X) := H^i(X^{\mathrm{t}G})$ is *Tate cohomology*.

The final construction generalizes what we had earlier when G was cyclic if X is in degree 0.

Let us now consider Tate cohomology for modules, and not complexes. Suppose G acts on M. Then giving a map $N \xrightarrow{f} M^G$ for an abelian group N is the same as giving a map $f\colon N \to M$ such that $g \cdot f(x) = f(x)$ for all $g \in G$. Dually, giving a map $M_G \xrightarrow{f} N$ is the same as giving a map $f\colon M \to N$ such that $f(g \cdot x) = f(x)$ (this is because the coinvariants are a quotient of M, whereas the invariants are a submodule). Then since $\mathrm{N}(g \cdot x) = \mathrm{N}(x)$ and $g \cdot \mathrm{N}(x) = \mathrm{N}(x)$ for all $g \in G$, these universal properties yield a diagram

$$\begin{array}{ccc} M & \xrightarrow{\mathrm{N}:=\sum g} & M \\ \downarrow & & \uparrow \\ M_G & \xrightarrow{\mathrm{N}} & M^G, \end{array}$$

where the norm map factors through the invariants and coinvariants. Note that the norm map N is an isomorphism if $\#G$ is invertible in M. Mimicking the definition of Tate cohomology, we get $M^G/\mathrm{N}(M_G) = M^G/\mathrm{N}(M) = \hat{H}^0(G, M)$, so homological algebra is in fact better behaved than our "usual" algebra!

Now we ask: what is the norm map N for a complex of G-modules? We have a canonical composition

$$X_{\mathrm{h}G} = P \otimes_{\mathbb{Z}[G]} X \to \underbrace{\mathbb{Z} \otimes_{\mathbb{Z}[G]} X}_{\substack{\text{term-wise} \\ \text{coinvariants}}} \xrightarrow{\mathrm{N}} \underbrace{\underline{\mathrm{Hom}}_G(\mathbb{Z}, X)}_{\substack{\text{term-wise} \\ \text{invariants}}} \to \underline{\mathrm{Hom}}_G(P, X) = X^{\mathrm{h}G}$$

where the last map is via pullback, and the norm map is applied term-wise via the norm on modules, which we know acts as desired by the previous construction

(though it is only defined up to homotopy, etc.). Note that the "term-wise invariants" take the degree-wise "naive" invariants, and don't preserve quasi-isomorphisms; the "term-wise coinvariants" are similar. Altogether, this gives a map which we will call $\mathrm{N}\colon X_{\mathrm{h}G} \to X^{\mathrm{h}G}$.

Taking a complex in degree 0 (and in general, for a complex that is bounded below), the homotopy invariants take that complex further to the right; similarly, coinvariants take that complex leftward. But Tate cohomology does both those things, so the result is unbounded, and tends to be very messy. It can be computed in some simpler cases though, such as the following:

PROPOSITION 14.1. *Let M be a G-module, thought of as a complex in degree 0. Then*

(1) $\hat{H}^i(G,M) = H^i(G,M)$ *if* $i \geq 1$*;*
(2) $\hat{H}^0(G,M) = M^G/\mathrm{N}(M)$*;*
(3) $\hat{H}^{-1}(G,M) = \mathrm{Ker}(\mathrm{N})/(g-1) = \mathrm{Ker}(\mathrm{N}\colon M_G \to M)$*;*
(4) $\hat{H}^{-i}(G,M) = H_{i-1}(G,M)$ *if* $i \geq 2$*.*

PROOF. The composition

$$M_{\mathrm{h}G} \xrightarrow{\mathrm{N}} M^{\mathrm{h}G} \to M^{\mathrm{t}G} = \mathrm{hCoker}(\mathrm{N})$$

yields a long exact sequence on cohomology

$$\cdots \to H_{-i}(M_{\mathrm{h}G}) \to H^i(M^{\mathrm{h}G}) \to \hat{H}^i(G,M) \to H_{-i-1}(M_{\mathrm{h}G}) \to \cdots .$$

If $i \geq 1$, then both $H_{-i}(M_{\mathrm{h}G})$ and $H_{-i-1}(M_{\mathrm{h}G})$ vanish, yielding an isomorphism $H^i(G,M) \simeq \hat{H}^i(G,M)$ by exactness.

Both $H_{-1}(M_{\mathrm{h}G})$ and $H^{-1}(G,M)$ vanish, yielding an exact sequence

$$0 \to \hat{H}^{-1}(G,M) \to M_G \xrightarrow{\mathrm{N}} M^G \to \hat{H}^0(G,M) \to 0,$$

which shows (2) and (3).

If $i \geq 1$, then $H^{-i-1}(G,M)$ and $H^{-i}(G,M)$ vanish, yielding an isomorphism $\hat{H}^{-i-1}(G,M) \simeq H_i(G,M)$ by exactness. □

Thus, cohomology shows up as Tate cohomology in higher degrees, though not in the zeroth degree, and similarly homology shows up except (crucially) in degree 0. Of course, all of this depends on the fact that P is bounded.

THEOREM 14.2 (Main Theorem of Cohomological LCFT). *Let L/K be an extension of nonarchimedean local fields with finite Galois group G. Then*

$$(L^\times)^{\mathrm{t}G} \simeq (\mathbb{Z}[-2])^{\mathrm{t}G}.$$

While it's not immediately clear how to construct this isomorphism, it's actually not too complicated! In the next lecture, we'll reduce it to a (very canonical!) vanishing statement.

Now, what does this theorem actually mean? Taking zeroth cohomology, we obtain

$$\begin{aligned} K^\times/\mathrm{N}(L^\times) = \hat{H}^0(G,L^\times) &= H^0((L^\times)^{\mathrm{t}G}) \\ &\simeq H^0((\mathbb{Z}[-2])^{\mathrm{t}G}) = \hat{H}^{-1}(G,\mathbb{Z}) = H_1(G,\mathbb{Z}) \simeq G^{\mathrm{ab}}, \end{aligned}$$

as proven last lecture. We saw that this was true for degree-2 extensions of local fields, so this provides a huge generalization of the Hilbert symbol for local fields!

We now recall the construction of the isomorphism $H_1(G,\mathbb{Z}) \simeq G^{\mathrm{ab}}$. First, we showed that $H_i(G,\mathbb{Z}[G]) = 0$ for all $i > 0$. Indeed,

$$\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} P \simeq \mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} \mathbb{Z} = \mathbb{Z}$$

is a quasi-isomorphism, since P is quasi-isomorphic to $\mathbb{Z}$. In particular, all of the lower homology groups vanish, since $\mathbb{Z}$ is in degree 0. Then we formed the following short exact sequence:

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

where ϵ is defined by $g \mapsto 1$, and where we have let $I_G := \mathrm{Ker}(\epsilon)$, which is an ideal inside $\mathbb{Z}[G]$ where the sum of all coefficients is zero. Taking the long exact sequence on group homology, we obtain

$$\underbrace{H_1(G,\mathbb{Z}[G])}_{0} \to H_1(G,\mathbb{Z}) \to I_G/I_G^2 \to \mathbb{Z} \xrightarrow{\sim} \mathbb{Z} \to 0,$$

since in general $M_G = M/I_G M$, hence we have an isomorphism $H_1(G,\mathbb{Z}) \simeq I_G/I_G^2$. Finally, we show that $I_G/I_G^2 \simeq G^{\mathrm{ab}}$ by construction maps in both directions. We claim that the following is a homomorphism modulo I_G^2:

$$\begin{array}{ccc} G & \xrightarrow{g \mapsto g-1} & I_G/I_G^2 \\ & \searrow \quad \nearrow & \\ & G^{\mathrm{ab}}. & \end{array}$$

To show this, expand $(g-1)(h-1)$ for $g,h \in G$, and so forth; since I_G/I_G^2 is abelian, this map factors through G^{ab}. For the inverse, we have the composition

$$I_G/I_G^2 \hookrightarrow \mathbb{Z}[G]/I_G^2 \xrightarrow{\sum n_g g \mapsto \prod g^{n_g}} G^{\mathrm{ab}},$$

where we have written G multiplicatively; we can check that this is a homomorphism and an inverse of the previous map.

Example 14.3. Suppose L/K is an unramified extension of local fields, so $G := \mathrm{Gal}(L/K) = \mathbb{Z}/n\mathbb{Z}$ is cyclic, where this isomorphism is canonical with the Frobenius element corresponding to 1. Recall that $\hat{H}^0(G,\mathcal{O}_L^\times) = 0$, i.e., $\mathrm{N}\colon \mathcal{O}_L^\times \twoheadrightarrow \mathcal{O}_K^\times$ is surjective. We proved this via filtering; the first subquotient gives the norm map $k_L^\times \xrightarrow{\mathrm{N}} k_K^\times$ and the rest give the trace map $k_L \xrightarrow{\mathrm{T}} k_K$ both of which are surjective (for instance, the latter is because the extension is separable). We also showed that the Herbrand quotient was $\chi(\mathcal{O}_L^\times) = 1$, which implies that $\hat{H}^1(G,\mathcal{O}_L^\times) = 0$ as well, i.e., $(\mathcal{O}_L^\times)^{\mathrm{t}G} \simeq 0$ is a quasi-isomorphism. Form the short exact sequence

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

where v denotes the normalized valuation on $L^\times$. Taking Tate cohomology then gives a quasi-isomorphism

$$\mathbb{Z}^{\mathrm{t}G}[-2] \simeq (L^\times)^{\mathrm{t}G} \simeq \mathrm{hCoker}\big(0 \to (L^\times)^{\mathrm{t}G}\big) \simeq \mathrm{hCoker}\big((\mathcal{O}_L^\times)^{\mathrm{t}G} \to (L^\times)^{\mathrm{t}G}\big) \simeq \mathbb{Z}^{\mathrm{t}G},$$

by Theorem 14.2, and since Tate cohomology commutes with cones and preserves quasi-isomorphisms. Thus, $(L^\times)^{\mathrm{t}G}$ is 2-periodic. Note that this is canonical, despite requiring a choice of generator, as we may choose the Frobenius element (by which $x \mapsto x^q$).

We now turn to a discussion of general extensions of local fields.

DEFINITION 14.4. K^{unr} is the (p-adic) completion of the maximal unramified extension of $K \subseteq \overline{K}$.

EXAMPLE 14.5. (1) Let $K := \mathbb{F}_q((t))$. The nth unramified extension of K is $K_n = \mathbb{F}_{q^n}((t))$, so the maximal unramified extension of K is

$$\bigcup_{n \geq 1} \mathbb{F}_{q^n}((t)) \subseteq \overline{\mathbb{F}}_q((t)) = K^{\mathrm{unr}}.$$

(2) If $K := \mathbb{Q}_p$, then $K^{\mathrm{unr}} = W(\overline{\mathbb{F}}_p)[1/p]$, where $W(-)$ denotes the ring of Witt vectors.

The basic structure of K^{unr} is thus a "local field" (not in the sense of local compactness, since the residue field is not finite, but in the sense of being a fraction field of a complete DVR) with residue field $\overline{\mathbb{F}}_q$.

Now, letting π be a uniformizer of K, which will continue to be a uniformizer in each K_n (i.e., the degree-n unramified extension of K), $\mathcal{O}_{K^{\mathrm{unr}}}$ is the π-adic completion of $\bigcup_n \mathcal{O}_{K_n}$. Then we have a short exact sequence

$$0 \to \mathcal{O}_{K^{\mathrm{unr}}}^{\times} \to K^{\mathrm{unr},\times} \xrightarrow{v} \mathbb{Z} \to 0,$$

where v is the normalized valuation on K^{unr} (so that $v(\pi) = 1$). We then define

$$\mathrm{Gal}(K^{\mathrm{unr}}/K) := \mathrm{Aut}_{\mathrm{cts}}(K^{\mathrm{unr}}/K),$$

where the latter is the continuous K-automorphisms of K^{unr}. Letting k denote the residue field of K and σ denote the Frobenius element of $\mathrm{Gal}(\bar{k}/k)$, we have

$$\mathrm{Gal}(K^{\mathrm{unr}}/K) \simeq \mathrm{Gal}(\bar{k}/k) \simeq \widehat{\mathbb{Z}},$$
$$\sigma \mapsto 1.$$

Since

$$K = \{x \in K^{\mathrm{unr}} : x = \sigma x\},$$

we have a resolution

$$0 \to K \to K^{\mathrm{unr}} \xrightarrow{1-\sigma} K^{\mathrm{unr}},$$

and further, a sequence

$$0 \to K^{\times} \to K^{\mathrm{unr},\times} \xrightarrow{x \mapsto x/\sigma x} K^{\mathrm{unr},\times} \xrightarrow{v} \mathbb{Z} \to 0. \tag{14.1}$$

Note that π cannot be in the image of central map since $v(x) = v(\sigma x)$ for all x. This gives us an expression for $K^{\times}$ in terms of $K^{\mathrm{unr},\times}$, which will be our main tool in coming lectures.

CLAIM 14.6. *The sequence (14.1) is exact.*

PROOF. This is true if and only if every $x \in \mathcal{O}_{K^{\mathrm{unr}}}^{\times}$ can be written as $y/\sigma y$ for some $y \in \mathcal{O}_{K^{\mathrm{unr}}}^{\times}$. This amounts to showing that the map

$$\mathcal{O}_{K^{\mathrm{unr}}}^{\times} \xrightarrow{x \mapsto x/\sigma x} \mathcal{O}_{K^{\mathrm{unr}}}^{\times}$$

is surjective. By completeness of the filtration by the maximal ideal (since K^{unr} is complete by definition), it suffices to prove that this is true at the associated graded level. This gives the maps

$$\overline{\mathbb{F}}_q^{\times} \xrightarrow{x \mapsto x/x^q} \overline{\mathbb{F}}_q^{\times} \quad \text{and} \quad \overline{\mathbb{F}}_q \xrightarrow{x \mapsto (1-q)x} \overline{\mathbb{F}}_q.$$

The first is surjective as we can solve $x^{q-1} = 1/y$ for any $y \in \overline{\mathbb{F}}_q^{\times}$, since $\overline{\mathbb{F}}_q$ is algebraically closed. The latter is invertible, as the map is just the identity. □

LECTURE 15

The Vanishing Theorem Implies Cohomological LCFT

Last time, we reformulated our problem as showing that, for an extension L/K of nonarchimedean local fields with Galois group G,

$$(L^\times)^{tG} \simeq \mathbb{Z}^{tG}[-2]. \tag{15.1}$$

Thus, our new goal is to compute the Tate cohomology of $L^\times$. Recall that we have let K^{unr} denote the completion of the maximal unramified extension of K; we'd like to use K^{unr} to compute this Tate cohomology.

Claim 15.1. *If $x \in K^{\mathrm{unr}}$ is algebraic over K (which may not be the case due to completion), then $K' := K(x)$ is unramified over K.*

Proof. As a finite algebraic extension of K, K' is a local field, and we have an embedding

$$\mathcal{O}_{K'}/\mathfrak{p}_K\mathcal{O}_{K'} \hookrightarrow \mathcal{O}_{K^{\mathrm{unr}}}/\mathfrak{p}_K\mathcal{O}_{K^{\mathrm{unr}}} = \bar{k},$$

where $k := \mathcal{O}_K/\mathfrak{p}_K$. So $\mathcal{O}_{K'}/\mathfrak{p}_K\mathcal{O}_{K'}$ is a field, hence uniformizers of K and K' are identical. □

Claim 15.2. *$(K^{\mathrm{unr}})^{\sigma=1} = K$, that is, the elements fixed by (i.e., on which it acts as the identity) the Frobenius automorphism $\sigma \in G$ (obtained from the Frobenii of each unramified extension, passed to the completion via continuity).*

Recall that we have a short exact sequence

$$0 \to K \to K^{\mathrm{unr}} \xrightarrow{1-\sigma} K^{\mathrm{unr}},$$

which we may rewrite on multiplicative groups as

$$1 \to K^\times \to K^{\mathrm{unr},\times} \xrightarrow{x \mapsto x/\sigma x} K^{\mathrm{unr},\times} \xrightarrow{v} \mathbb{Z} \to 0.$$

We showed that an element of $K^{\mathrm{unr},\times}$ can only be written as $x/\sigma x$ if it is a unit in the ring of integers $\mathcal{O}^\times_{K^{\mathrm{unr}}}$; this map is an isomorphism on each of the associated graded terms, hence on $\mathcal{O}^\times_{K^{\mathrm{unr}}}$.

Now, we'd like to explicitly construct the isomorphism in (15.1). Our first attempt is as follows: let us assume that L/K is totally ramified (since we discussed the unramified case last time, this is a rather mild assumption), so that $L^{\mathrm{unr}} = L \otimes_K K^{\mathrm{unr}}$. Then we have the following theorem, to be proved later.

Theorem 15.3 (Vanishing Theorem). *If L/K is totally ramified, then the complex $(L^{\mathrm{unr},\times})^{tG}$ is acyclic.*

Claim 15.4. *The vanishing theorem implies cohomological* LCFT.

PROOF. Assume L/K is totally ramified. We have the four-term exact sequence

$$1 \to L^\times \to L^{\mathrm{unr},\times} \xrightarrow{x \mapsto x/\sigma x} L^{\mathrm{unr},\times} \xrightarrow{v} \mathbb{Z} \to 0. \tag{15.2}$$

We may rewrite this as follows:

$$\begin{array}{ccc}
A & \cdots \to 0 \longrightarrow L^\times \longrightarrow 0 \longrightarrow 0 \to \cdots \\
\downarrow & \| \quad \downarrow \quad \downarrow \quad \| \\
B & \cdots \to 0 \to L^{\mathrm{unr},\times} \xrightarrow{1-\sigma} L^{\mathrm{unr},\times} \to 0 \to \cdots \\
\downarrow & \| \quad \downarrow \quad \downarrow v \quad \| \\
\mathrm{Coker}(A \to B) & \cdots \to 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \longrightarrow 0 \to \cdots,
\end{array}$$

where $L^\times$ is in degree -1. The final quasi-isomorphism to the homotopy cokernel obtained from (15.2) follows from Claim 10.12, because $A \hookrightarrow B$ is an injection (note that this holds in general for any four-term exact sequence). The term-wise cokernel yields an injection

$$L^{\mathrm{unr},\times}/L^\times \xhookrightarrow{x \mapsto x/\sigma x} L^{\mathrm{unr},\times}$$

since, omitting the quotient, $L^\times$ is precisely the kernel of this map.

Now, we have a quasi-isomorphism

$$B^{\mathrm{t}G} = \mathrm{hCoker}\big(L^{\mathrm{unr},\times} \xrightarrow{1-\sigma} L^{\mathrm{unr},\times}\big)^{\mathrm{t}G} \simeq \mathrm{hCoker}\big((L^{\mathrm{unr},\times})^{\mathrm{t}G} \to (L^{\mathrm{unr},\times})^{\mathrm{t}G}\big),$$

so since $(L^{\mathrm{unr},\times})^{\mathrm{t}G}$ is acyclic by the vanishing theorem, this homotopy cokernel is as well by the long exact sequence on cohomology. Thus,

$$(L^\times[2])^{\mathrm{t}G} = \mathrm{hCoker}\big((L^\times[1])^{\mathrm{t}G} \to 0\big) = \mathrm{hCoker}\big(A^{\mathrm{t}G} \to B^{\mathrm{t}G}\big) \simeq \mathbb{Z}^{\mathrm{t}G},$$

as desired. □

Now suppose L/K is a general finite Galois extension with $G := \mathrm{Gal}(L/K)$ (though we could handle the unramified and totally ramified cases separately, as any extension is canonically a composition of such extensions). If L/K is unramified, then

$$L \otimes_K K^{\mathrm{unr}} = \prod_{L \hookrightarrow K^{\mathrm{unr}}} K^{\mathrm{unr}}$$

canonically, indexed by such embeddings. In fact, the following holds:

THEOREM 15.5 (General Vanishing Theorem). *$[(L \otimes_K K^{\mathrm{unr}})^\times]^{\mathrm{t}G}$ is acyclic.*

To understand the structure of $L \otimes_K K^{\mathrm{unr}}$, note that we have an action of $\widehat{\mathbb{Z}}\sigma$ on the second factor and of G on the first; these two actions (i.e., $x \otimes y \mapsto gx \otimes y$ and $x \otimes y \mapsto x \otimes \sigma y$) clearly commute. Again, the points fixed under σ are

$$L = L \otimes_K K \hookrightarrow L \otimes_K K^{\mathrm{unr}}.$$

CLAIM 15.6. *The following sequence is exact:*

$$1 \to L^\times \to (L \otimes_K K^{\mathrm{unr}})^\times \xrightarrow{x \mapsto x/\sigma x} (L \otimes_K K^{\mathrm{unr}})^\times \to \mathbb{Z} \to 0.$$

PROOF. If $x \in K^{\mathrm{unr}}$ is a unit, then σx is as well, so the map $x \mapsto x/\sigma x$ is well-defined, and moreover, x is in its kernel if and only if x is fixed under the

action of σ, that is, $x \in K$, and since $L \otimes_K K = L$ we obtain a unit of L, which shows exactness of the left half. Now, the map to $\mathbb{Z}$ is defined by

$$\begin{array}{ccc} (L \otimes_K K^{\mathrm{unr}})^\times & \longrightarrow & \mathbb{Z} \\ & {\scriptstyle \mathrm{N}_{L/K}\otimes\mathrm{id}} \searrow \quad \nearrow {\scriptstyle v} & \\ & \underbrace{K \otimes_K K^{\mathrm{unr},\times}}_{K^{\mathrm{unr},\times}}, & \end{array}$$

where

$$\mathrm{N}_{L/K}(x) := \prod_{g \in G} gx.$$

Thus, its kernel is $\mathcal{O}_{K^{\mathrm{unr}}}^\times$, which is precisely the image of $x \mapsto x/\sigma x$. Moreover, the map is surjective as $1 \otimes \pi \mapsto 1$. □

Observe that if L/K is totally ramified, then this is just our extension from before. Indeed, if we write $L^{\mathrm{unr}} = L \otimes_K K^{\mathrm{unr}}$, then the σ's "match up," that is, the induced Frobenius automorphisms of L^{unr} and K^{unr} are identical as L and K have the same residue field. The norm $\mathrm{N}_{L/K} \colon L^{\mathrm{unr},\times} \to K^{\mathrm{unr},\times}$ for this extension satisfies $v_{K^{\mathrm{unr}}} \circ \mathrm{N} = v_{L^{\mathrm{unr}}}$ (such an extension is generated by the nth root of a uniformizer of K, and then $\mathrm{N}(\pi^{1/n}) = \pi$).

Now suppose L/K is unramified of degree n. Fix an embedding $L \hookrightarrow K^{\mathrm{unr}}$, and let $\sigma \in \mathrm{Gal}(L/K)$ also denote the Frobenius element of L/K. Then we have an isomorphism

$$\begin{aligned} L \otimes_K K^{\mathrm{unr}} &\xrightarrow{\sim} \prod_{i=0}^{n-1} K^{\mathrm{unr}} \\ x \otimes y &\mapsto \left((\sigma^i x) \cdot y\right)_{i=0}^{n-1}, \end{aligned}$$

where the product is taken via our fixed embedding (note that this could be done more canonically by taking the product over embeddings as before). We now ask: what does the automorphism $\mathrm{id} \otimes \sigma$ of $L \otimes_K K^{\mathrm{unr}}$ correspond to under this isomorphism? We have

$$x \otimes \sigma y \mapsto (x \cdot \sigma y, \sigma x \cdot \sigma y, \sigma^2 x \cdot \sigma y, \ldots) = \sigma(\sigma^{-1} x \cdot y, x \cdot y, \sigma x \cdot y, \ldots),$$

so it is the action of σ on the rotation to the right of the image of $x \otimes y$ (note that σ doesn't have finite order on K^{unr}, so this should either, which rules our rotation as a possibility for the image of $\mathrm{id} \otimes \sigma$). Similarly, the norm map $\mathrm{N}_{L/K} \colon \prod K^{\mathrm{unr},\times} \to K^{\mathrm{unr},\times}$ takes the product of all entries.

We'd like for some element $(x_0, \ldots, x_{n-1}) \in \prod K^{\mathrm{unr},\times}$ to be in the image of $y/\sigma y$ (i.e., the map in the middle of the exact sequence of Claim 15.6; here σ refers to the automorphism $\mathrm{id} \otimes \sigma$) if and only if $\prod x_i \in \mathcal{O}_{K^{\mathrm{unr}}}^\times$, that is, $\sum v(x_i) = 0$. Recall that the reverse implication is trivial, as we have shown that $\mathcal{O}_{K^{\mathrm{unr}}}^\times \xrightarrow{y/\sigma y} \mathcal{O}_{K^{\mathrm{unr}}}^\times$ is surjective as it is at the associated graded level. For the forward direction, we have

$$(y_0, \ldots, y_{n-1}) \overset{y/\sigma y}{\longmapsto} \left(\frac{y_0}{\sigma y_{n-1}}, \frac{y_1}{\sigma y_0}, \ldots\right) =: (x_0, x_1, \ldots).$$

Thus,

$$y_0 = x_0 \cdot \sigma y_{n-1},$$

$$\begin{aligned} y_1 &= x_1 \cdot \sigma y_0 = x_1 \cdot \sigma x_0 \cdots \sigma^2 y_{n-1}, \\ \cdots &= \cdots \\ y_{n-1} &= x_{n-1} \cdot \sigma x_{n-2} \cdots \sigma^{n-1} x_0 \cdot \sigma^n y_{n-1}, \end{aligned}$$

that is,

$$\frac{y_{n-1}}{\sigma^n y_{n-1}} = x_{n-1} \cdot \sigma x_{n-2} \cdots \sigma^{n-1} x_0.$$

Note that everything here is an element of K^{unr}, so we really do not have $\sigma^n = \mathrm{id}$! Last time, we showed that we can do this if and only if the right-hand side is in $\mathcal{O}_{K^{\mathrm{unr}}}^{\times}$, which is equivalent to saying that $\sum v(x_i) = 0$. The general case of this exact sequence is sort of a mix of the two.

We now compare these results with those from the last lecture. Assume the Vanishing Theorem. For an unramified extension L/K, we have two quasi-isomorphisms between $(L^{\times})^{\mathrm{t}G}$ and $\mathbb{Z}[-2]^{\mathrm{t}G}$, one from what we just did, and the other since $(\mathcal{O}_L^{\times})^{\mathrm{t}G} \simeq 0$ implies $(L^{\times})^{\mathrm{t}G} \simeq \mathbb{Z}^{\mathrm{t}G} \simeq (\mathbb{Z}[-2])^{\mathrm{t}G}$ by cyclicity. We claim that these two quasi-isomorphisms coincide. A sketch of the proof is as follows: we have $G = \mathbb{Z}/n\mathbb{Z}$ (with generator the Frobenius element), and a short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \xrightarrow{1-\sigma} \mathbb{Z}[G] \to \mathbb{Z} \to 0.$$

As shown in Problem 1(e) of Problem Set 7, $\mathbb{Z}[G]^{\mathrm{t}G} \simeq 0$ is a quasi-isomorphism (this is easy to show, and we've already shown it for cyclic groups). Thus, we get $\mathbb{Z}^{\mathrm{t}G}[2] \simeq \mathbb{Z}^{\mathrm{t}G}$, and we claim that this is the same isomorphism that we get from 2-periodicity of the complex. The proof is by a diagram chase. We have $(L \otimes_K K^{\mathrm{unr}})^{\times} = \prod K^{\mathrm{unr},\times}$, which is a finite product. Thus, the diagram

$$\begin{array}{ccccccccccc} 1 & \longrightarrow & L^{\times} & \longrightarrow & (L \otimes_K K^{\mathrm{unr}})^{\times} & \xrightarrow{x \mapsto x/\sigma x} & (L \otimes_K K^{\mathrm{unr}})^{\times} & \xrightarrow{\sum v} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle \prod v} & & \downarrow{\scriptstyle \prod v} & & \| & & \\ 1 & \longrightarrow & \mathbb{Z} & \longrightarrow & \underbrace{\prod_{i=0}^{n} \mathbb{Z}}_{\mathbb{Z}[G]} & \xrightarrow{1-\sigma} & \mathbb{Z}[G] & \xrightarrow{\epsilon} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

commutes, where ϵ denotes the sum over the coordinates of $\mathbb{Z}[G]$. This says precisely that the isomorphisms obtained from both 4-term exact sequences coincide.

The upshot is that under LCFT, we have an isomorphism $K^{\times}/\mathrm{N}L^{\times} \simeq \mathbb{Z}/n\mathbb{Z}$ by which $\pi \mapsto \mathrm{Frob}$. Thus, we have reduced LCFT to the Vanishing Theorem, which we will prove in the next lecture.

LECTURE 16

Vanishing of Tate Cohomology Groups

Recall that we reduced (cohomological) local class field theory to the following statement: for a finite Galois extension L/K of nonarchimedean local fields with Galois group G, we have

$$\left((L \otimes_K K^{\mathrm{unr}})^\times\right)^{\mathrm{t}G} \simeq 0,$$

i.e., this complex is acyclic. To show this vanishing, we will prove a general theorem (due to Tate) about the vanishing of Tate cohomology, which makes the above more tractable. Thus, we ask: given a complex X of G-modules, what conditions guarantee that $X^{\mathrm{t}G}$ is acyclic? The prototypical such result is the following:

THEOREM 16.1. *For a cyclic group G, $X^{\mathrm{t}G}$ is acyclic if and only if*

$$\hat{H}^0(G, X) = 0 = \hat{H}^1(G, X).$$

PROOF. $X^{\mathrm{t}G}$ can be computed be a 2-periodic complex. Note that any two values of distinct parity (such as consecutive values) would suffice. □

Our main results in this lecture are the following:

THEOREM 16.2. *Theorem 16.1 holds also if G is a p-group (i.e., $\#G = p^n$, for some prime p and $n \geq 0$).*

From here, we will deduce the next result:

THEOREM 16.3. *Suppose that for every prime p and every p-Sylow subgroup $G_p \subseteq G$, $\hat{H}^0(G_p, X) = 0 = \hat{H}^1(G_p, X)$. Then $X^{\mathrm{t}G}$ is acyclic.*

REMARK 16.4. In general, it's not true that vanishing in two consecutive degrees is sufficient for any finite group G. Also, in practice, one often verifies the vanishing of Tate cohomology in two consecutive subgroups for every subgroup of G, and not just p-Sylow ones.

In the following lectures, we will deduce local class field theory from here.

We begin by proving Theorem 16.2. Throughout the following, let G be a p-group.

PROPOSITION 16.5. *Let X be a complex of $\mathbb{F}_p[G]$-modules. If $\hat{H}^0(G, X) = 0$, then $X^{\mathrm{t}G}$ is acyclic.*

Note that we only need vanishing in one degree here! For this, we first recall the following fact.

LEMMA 16.6. *Let V be a non-zero $\mathbb{F}_p[G]$-module. Then $V^G \neq 0$.*

PROOF. Without loss of generality, we may assume that V is finite-dimensional over $\mathbb{F}_p$, since V is clearly the union of its finite-dimensional G-submodules. Then

$\#V = p^r$ for some $0 < r < \infty$. Every G-orbit of V either has size 1 or divisible by p (since they must divide $\#G$ as the orbit is isomorphic to the quotient of G by the stabilizer). Since $\{0\}$ is a G-orbit of size 1, there must be another (since the sizes of all the G-orbits must sum to p^r), that is, some $v \in V^G \setminus \{0\}$. □

Proof (of Proposition 16.5). **Step 1.** First, we claim that $\hat{H}^0(G, X \otimes V) = 0$ for every finite-dimensional G-representation V over $\mathbb{F}_p$. Here G acts via the "diagonal action," i.e., on $(X \otimes V)^i = X^i \otimes V$ via $g \cdot (x \otimes v) := gx \otimes gv$. We proceed by induction on $\dim_{\mathbb{F}_p} V$. By the previous lemma, we have a short exact sequence of $\mathbb{F}_p[G]$-modules

$$0 \to V^G \to V \to W \to 0$$

with $\dim W < \dim V$. This gives

$$\mathrm{hCoker}(V^G \otimes X \to V \otimes X) \simeq W \otimes X.$$

Since $\hat{H}^0(G, W \otimes X) = 0$ by the inductive hypothesis, and

$$\hat{H}^0(G, V^G \otimes X) = \hat{H}^0\big(G, \bigoplus_{\dim V^G} X\big) = \bigoplus_{\dim V^G} \hat{H}^0(G, X) = 0$$

by assumption on X, the long exact sequence on Tate cohomology gives $\hat{H}^0(G, V \otimes X)$, as desired.

Step 2. We now show vanishing in negative degrees. Consider the short exact sequence

$$0 \to V_1 \to \mathbb{F}_p[G] \xrightarrow{\epsilon} \mathbb{F}_p \to 0,$$

where V_1 is defined as the kernel of ϵ, analogously to what we called I_G with $\mathbb{F}_p$ replaced by $\mathbb{Z}$. Let $\underline{X}$ be X with the trivial G-action. Then

$$\begin{aligned} \underline{X} \otimes \mathbb{F}_p[G] &\to X \otimes \mathbb{F}_p[G] \\ x \otimes g &\mapsto gx \otimes g \end{aligned}$$

is a G-equivariant map, and a bijection, hence an isomorphism. Indeed,

$$h(x \otimes g) = x \otimes hg \mapsto hgx \otimes hg = h(gx \otimes g).$$

In Problem 1(e) of Problem Set 7, it was proven that $(\underline{X} \otimes \mathbb{F}_p[G])^{\mathrm{t}G}$ is acyclic, hence $(X \otimes \mathbb{F}_p[G])^{\mathrm{t}G}$ is as well. Thus, the long exact sequence on Tate cohomology gives

$$\hat{H}^{i-1}(G, X) \simeq \hat{H}^i(G, X \otimes V_1).$$

We've seen in Step 1 that the right-hand side vanishes for $i = 0$, therefore $\hat{H}^{-1}(G, X) = 0$. Iterating, we get $\hat{H}^i(G, X) = 0$ for all $i \leq 0$.

Step 3. To show vanishing in positive degrees, note that we have an exact sequence

$$0 \to \mathbb{F}_p \xrightarrow{1 \mapsto \sum_{g \in G} g} \mathbb{F}_p[G] \to V_2 \to 0,$$

where V_2 is defined to be the cokernel as before. The same logic gives

$$\hat{H}^i(G, X \otimes V_2) \simeq \hat{H}^{i+1}(G, X),$$

and so Step 1 again shows that $\hat{H}^i(G, X) = 0$ for all $i \geq 0$. □

PROOF (OF THEOREM 16.2). Define $X/p := \mathrm{hCoker}(X \xrightarrow{\times p} X)$; note that this is not the same as modding out all terms by p. Note that, as a complex of $\mathbb{Z}[G]$-modules, X/p is quasi-isomorphic to a complex of $\mathbb{F}_p[G]$-modules. Since X is only defined up to quasi-isomorphism, we may assume it is projective (in particular, flat) as a complex of $\mathbb{Z}[G]$-modules. Thus, we have a quasi-isomorphism

$$X/p = X \otimes_{\mathbb{Z}[G]} \mathrm{hCoker}(\mathbb{Z}[G] \xrightarrow{\times p} \mathbb{Z}[G]) \simeq X \otimes_{\mathbb{Z}[G]} \mathbb{F}_p[G],$$

where the right-hand side computes X modded out by p term-wise. We then have a long exact sequence

$$\to \hat{H}^i(G,X) \xrightarrow{\times p} \hat{H}^i(G,X) \to \hat{H}^i(G,X/p) \to \hat{H}^{i+1}(G,X) \xrightarrow{\times p} \hat{H}^{i+1}(G,X) \to$$

and so setting $i = 0$, we obtain $\hat{H}^0(G, X/p) = 0$ by assumption. Thus, $(X/p)^{\mathrm{t}G}$ is acyclic by Proposition 16.5. It follows that $\hat{H}^i(G, X/p) = 0$ for all i, and therefore, multiplication by p is an isomorphism on $\hat{H}^i(G,X)$ for each i. But as shown in Problem 2(c) of Problem Set 7, multiplication by $\#G$ is zero on $\hat{H}^i(G,X)$. Since G is a p-group, this is only possible if $\hat{H}^i(G,X) = 0$ for all i. □

PROOF (OF THEOREM 16.3). Since as mentioned above, multiplication by $\#G$ is the zero map on $\hat{H}^i(G,X)$, it follows that $\hat{H}^i(G,X)$ is $\#G$-torsion. Thus, it suffices to show that $\hat{H}^i(G,X)[p] = 0$ for all p (i.e., the p-torsion of $\hat{H}^i(G,X)$ vanishes).

Recall that for every subgroup H of G, there are restriction and inflation maps $X^{\mathrm{t}G} \to X^{\mathrm{t}H}$ and $X^{\mathrm{t}H} \to X^{\mathrm{t}G}$ respectively, whose composition as an endomorphism of $X^{\mathrm{t}G}$ is homotopic to multiplication by the index $[G : H]$.

Applying this to a p-Sylow subgroup $H = G_p$ of G and taking cohomology, we obtain maps

$$\hat{H}^i(G,X)[p] \subset \hat{H}^i(G,X) \to \hat{H}^i(G_p,X) \to \hat{H}^i(G,X)$$

whose composition is multiplication by $[G : G_p]$, which is prime to p by definition. Thus, it is an isomorphism when restricted to $\hat{H}^i(G,X)[p]$, and in particular, $\hat{H}^i(G,X)[p] \to \hat{H}^i(G_p,X)$ is injective. But by Theorem 16.2, $\hat{H}^i(G_p,X) = 0$ for all i, which yields the desired result. □

LECTURE 17

Proof of the Vanishing Theorem

In this lecture, our goal is to show that, for an extension of nonarchimedean local fields L/K with Galois group G, we have

$$\left[(L \otimes_K K^{\mathrm{unr}})^\times\right]^{\mathrm{t}G} \simeq 0.$$

Recall that this implies that $(L^\times)^{\mathrm{t}G} \simeq \mathbb{Z}^{\mathrm{t}G}[-2]$ (which is the main theorem of cohomological LCFT), which in turn implies that $G^{\mathrm{ab}} \simeq K^\times/\mathrm{N}L^\times$. For now, we'll assume that L/K is totally ramified (a reduction from the general case will occur later), which implies $L^{\mathrm{unr}} = L \otimes_K K^{\mathrm{unr}}$. Last time, we proved that it suffices to show that

$$\hat{H}^0(G_\ell, L^{\mathrm{unr},\times}) = 0 = \hat{H}^1(G_\ell, L^{\mathrm{unr},\times})$$

for all ℓ-Sylow subgroups $G_\ell \subseteq G$, where ℓ is a prime. Note that, if we let $K' := L^{G_\ell}$, then L/K' is a G_ℓ-Galois extension. Thus, we may replace K by K' and G with G_ℓ, so that we may simply assume that G is an ℓ-group (that is, $\#G = \ell^n$ for some n). Now, the latter equality above is simply Hilbert's Theorem 90 (or the generalization thereof shown in Problem 3 of Problem Set 7) for the extension $L^{\mathrm{unr}}/K^{\mathrm{unr}}$, so it remains to show the former, that is, that the norm map

$$\mathrm{N}\colon L^{\mathrm{unr},\times} \to K^{\mathrm{unr},\times}$$

is surjective.

We recall the structure theory of ℓ-groups:

PROPOSITION 17.1. *Let G be an ℓ-group. Then there is a chain of normal subgroups*

$$1 \lhd G_0 \lhd \cdots \lhd G_m = G,$$

such that G_{i+1}/G_i is cyclic for all i.

PROOF. The main step is to show that $Z(G) \neq 1$ (i.e., the centralizer of G is non-trivial) if $G \neq 1$. Let G act on itself via the adjoint action, that is, $g \cdot x := gxg^{-1}$ for $g, x \in G$. Then the size of every G-orbit is either 1 or divisible by ℓ. Since

$$\sum_{O \in G\text{-orbits}} \#O = \#G = \ell^n > 1,$$

and the G-orbit of 1 has order 1, ℓ must divide the number of G-orbits of size 1, hence $\#Z(G) \neq 0$. Then, choosing a nontrivial element $x \in Z(G)$, we see that $G/\langle x \rangle$ is a normal subgroup of G, and the result follows by induction. □

Thus, by Galois theory, we have a series of corresponding cyclic extensions

$$L = L_m/L_{m-1}/\cdots/L_0 = K.$$

Since it suffices to show that the norm map is surjective on each of these subextensions (since a composition of surjective maps is surjective), we may assume

that G is cyclic, say of order n. Recall that $\mathrm{N}\colon L^\times \to K^\times$ is *not* surjective, as we showed $\#\hat{H}^0(G, L^\times) = n$. Now, for each m, let $K \subseteq K_m \subseteq K^{\mathrm{unr}}$ denote the degree-m unramified extension of K. The main step is the following:

Claim 17.2. *Let $x \in K^\times$. Then x is in the image of $\mathrm{N}\colon L_m^\times \to K_m^\times$.*

Proof. Observe that $K^\times/\mathrm{N}L^\times = \mathcal{O}_K^\times/\mathrm{N}\mathcal{O}_L^\times$. Indeed, we have the usual short exact sequence

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v} \mathbb{Z} \to 0,$$

which yields the exact sequence

$$0 = \hat{H}^{-1}(\mathbb{Z}) \to \hat{H}^0(\mathcal{O}_L^\times) \hookrightarrow \hat{H}^0(L^\times) \to \hat{H}^0(\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z},$$

and the rightmost map is zero since L/K is totally ramified (and therefore $n \mid v(y)$ for all $y \in K^\times$). Thus, we have an isomorphism $\hat{H}^0(L^\times) \simeq \hat{H}^0(\mathcal{O}_L^\times)$, which is precisely our observation.

We have a commutative diagram

$$\begin{array}{ccccccc}
L^\times & \xrightarrow{\mathrm{N}} & K^\times & \longrightarrow & K^\times/\mathrm{N}L^\times & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
L_m^\times & \xrightarrow{\mathrm{N}} & K_m^\times & \longrightarrow & K_m^\times/\mathrm{N}L_m^\times & \longrightarrow & 0 \\
\downarrow{\scriptstyle \mathrm{N}_{L_m/L}} & & \downarrow{\scriptstyle \mathrm{N}_{K_m/K}} & & \downarrow & & \\
L^\times & \longrightarrow & K^\times & \xrightarrow{\mathrm{N}} & K^\times/\mathrm{N}L^\times & \longrightarrow & 0.
\end{array}$$

Now, the composition $K^\times/\mathrm{N}L^\times \to K^\times/\mathrm{N}L^\times$ of induced maps is raising to the nth power, hence 0. We'd like to show that the induced map

$$\mathrm{N}_{K_m/K}\colon K_m^\times/\mathrm{N}L_m^\times \to K^\times/\mathrm{N}L^\times$$

is an isomorphism, which implies that the induced map $K^\times/\mathrm{N}L^\times \to K^\times/\mathrm{N}L^\times$ is 0, proving the claim. By Claim 7.8(3), i.e., our earlier analysis of Herbrand quotients, both groups have order n, hence this map is injective if and only if it is surjective. Moreover, it is equivalent to the map

$$\mathrm{N}_{K_m/K}\colon \mathcal{O}_{K_m}^\times/\mathrm{N}\mathcal{O}_{L_m}^\times \to \mathcal{O}_K^\times/\mathrm{N}\mathcal{O}_L^\times$$

by our observation, and since $\mathrm{N}\colon \mathcal{O}_{K_m}^\times \to \mathcal{O}_K^\times$ is surjective by a proof identical to that of Claim 3.4, this map is surjective too, which completes the proof. □

Again, we have a cyclic group G of order n, and all we need to show is that $\mathrm{N}\colon L^{\mathrm{unr},\times} \to K^{\mathrm{unr},\times}$ is surjective. Applying the claim to $K_m^\times$, we see that every element of $K_m^\times$ is the norm of an element of $L_{m+m'}^\times$, and therefore

$$\mathrm{N}\colon \bigcup_m L_m^\times \to \bigcup_m K_m^\times$$

is surjective. It remains to pass to completions. We know that the image of the map $\mathrm{N}\colon L^{\mathrm{unr},\times} \to K^{\mathrm{unr},\times}$ contains $\bigcup_m K_m^\times$, which is dense, so it is enough to show that the image contains an open neighborhood of 1. Clearly

$$\mathrm{N}(L^{\mathrm{unr},\times}) \supseteq \mathrm{N}(K^{\mathrm{unr},\times}) = (K^{\mathrm{unr},\times})^n,$$

and we saw in Problem 1(a) of Problem Set 1 that every element of $1 + \mathfrak{p}_{K^{\mathrm{unr}}}^{2v(n)+1}$ is an nth power in K^{unr}; this is our desired open neighborhood.

Finally, we prove the general case of the vanishing theorem, where our G-extension L/K of nonarchimedean local fields may not be totally ramified. Let $L/L_0/K$ me the (unique) maximal unramified extension of K inside of L, so that L/L_0 is totally unramified. Let $H := \mathrm{Gal}(L/L_0)$, so that L_0/K is Galois with group G/H.

LEMMA 17.3. *Let X be a complex of G-modules, and suppose we have an exact sequence*

$$1 \to H \to G \to G/H \to 1.$$

If

$$X^{\mathrm{t}H} \simeq 0 \simeq \left(X^{\mathrm{h}H}\right)^{\mathrm{t}G/H},$$

then $X^{\mathrm{t}G} \simeq 0$.

Note that it is not true in general that $\left(X^{\mathrm{t}H}\right)^{\mathrm{t}G/H} = X^{\mathrm{t}G}$! For instance, if H is the trivial group, then

$$X^{\mathrm{t}H} = \mathrm{hCoker}(\mathrm{N}\colon X \to X) = 0,$$

where here $\mathrm{N} = \mathrm{id}_X$.

PROOF. By the first condition, $X_{\mathrm{h}H} \xrightarrow{\mathrm{qis}} X^{\mathrm{h}H}$, so by the second condition and Problem 3 of Problem Set 6,

$$X_{\mathrm{h}G} \simeq \left(X_{\mathrm{h}H}\right)_{\mathrm{h}G/H} \simeq \left(X^{\mathrm{h}H}\right)_{\mathrm{h}G/H} \xrightarrow{\mathrm{qis}} \left(X^{\mathrm{h}H}\right)^{\mathrm{h}G/H} \simeq X^{\mathrm{h}G}.$$

It's easy to check that this quasi-isomorphism is given by the norm map (it is given by the composition of two norm maps), which implies that

$$X^{\mathrm{t}G} = \mathrm{hCoker}\left(X_{\mathrm{h}G} \to X^{\mathrm{h}G}\right)$$

is acyclic, as desired. □

Now, we'd like to show that $\left[(L \otimes_K K^{\mathrm{unr}})^\times\right]^{\mathrm{t}G} \simeq 0$. Recall that we have

$$L \otimes_K K^{\mathrm{unr}} = L \otimes_{L_0} L_0 \otimes_K K^{\mathrm{unr}} = L \otimes_{L_0} \prod_{L_0 \hookrightarrow K^{\mathrm{unr}}} K^{\mathrm{unr}} = \prod_{L_0 \hookrightarrow K^{\mathrm{unr}}} L \otimes_{L_0} K^{\mathrm{unr}}$$

canonically (where the second isomorphism is via the map $\alpha \otimes \beta \mapsto (i(\alpha)\beta)_i$, indexed over embeddings $i\colon L_0 \hookrightarrow K^{\mathrm{unr}}$). We have

$$\left[(L \otimes_K K^{\mathrm{unr}})^\times\right]^{\mathrm{t}H} \simeq \prod_{L_0 \hookrightarrow K^{\mathrm{unr}}} \left[(L \otimes_{L_0} K^{\mathrm{unr}})^\times\right]^{\mathrm{t}H} \simeq \prod_{L_0 \hookrightarrow K^{\mathrm{unr}}} \left[(L \otimes_{L_0} L_0^{\mathrm{unr}})^\times\right]^{\mathrm{t}H} \simeq 0$$

by the totally ramified case (as L_0/K is unramified and L/L_0 is totally ramified), which establishes the first condition of the lemma. To show the second condition, note that

$$\prod_{L_0 \hookrightarrow K^{\mathrm{unr}}} \left[(L \otimes_{L_0} K^{\mathrm{unr}})^\times\right]^{\mathrm{h}H} = \prod_{L_0 \hookrightarrow K^{\mathrm{unr}}} K^{\mathrm{unr},\times} \simeq K^{\mathrm{unr},\times}[G/H]$$

as a G/H-module (once we fix an embedding $L_0 \hookrightarrow K^{\mathrm{unr}}$). But as shown in Problem 1(e) of Problem Set 7, Tate cohomology vanishes for induced modules (thus, the equality above is irrelevant, as we just needed a product over such embeddings to construct an induced G/H-module). Lemma 17.3 then yields the desired result.

LECTURE 18

Norm Groups, Kummer Theory, and Profinite Cohomology

Last time, we proved the vanishing theorem, which we saw implied that for every finite Galois G-extension L/K, we have $(L^\times)^{tG} \simeq \mathbb{Z}^{tG}[-2]$, which, taking zeroth cohomology, implies $K^\times/\mathrm{N}L^\times \simeq G^{\mathrm{ab}}$, which we note cannot be trivial because G must be a solvable group. However, in the first lecture, we formulated a different theorem:

$$\mathrm{Gal}(\overline{K}/K)^{\mathrm{ab}} := \varprojlim_{L/K} \mathrm{Gal}(L/K)^{\mathrm{ab}} \simeq \widehat{K^\times},$$

where the inverse limit is over finite Galois extensions L/K. Recall that

$$\widehat{K^\times} := \varprojlim_{[K^\times:\Gamma]<\infty} K^\times/\Gamma,$$

is the profinite completion of K, where Γ is a finite-index *closed* subgroup of K (this is the only reasonable way to define profinite-completion for topological groups). Thus, we'd like to show that

$$\varprojlim_{L/K} K^\times/\mathrm{N}L^\times \simeq \varprojlim_{[K^\times:\Gamma]<\infty} K^\times/\Gamma,$$

with L and Γ as above.

Definition 18.1. A subgroup Γ of $K^\times$ is a *norm group* (or *norm subgroup*) if $\Gamma = \mathrm{N}L^\times$ for some finite extension L/K.

Theorem 18.2 (Existence Theorem). *A subgroup Γ of $K^\times$ is a norm group if and only if Γ is closed and of finite index.*

This clearly suffices to prove the statement of LCFT above.

Remark 18.3. A corollary of LCFT is that is L/K is G-Galois, and $L/L_0/K$ is the maximal abelian subextension of K inside L, then $\mathrm{N}L^\times = NL_0^\times$. This is because

$$K^\times/\mathrm{N}L^\times \simeq G^{\mathrm{ab}} \simeq K^\times/\mathrm{N}L_0^\times.$$

We'll prove the existence theorem in the case $\mathrm{char}(K) = 0$, though it is true in other cases (but the proof is more complicated).

Lemma 18.4. *If $\Gamma \subseteq K^\times$ is a norm subgroup, then Γ is closed and of finite index.*

Proof. Let L/K be an extension of degree n such that $\Gamma = \mathrm{N}L^\times$. Then $\Gamma \supseteq N_{L/K}K^\times = (K^\times)^n$, which we've seen is a finite-index closed subgroup (because it contains $1 + \mathfrak{p}_K^n$ for all sufficiently large n), hence Γ is as well. Note that if $\mathrm{char}(K) > 0$, then $(K^\times)^n$ actually has infinite index in $K^\times$! $\square$

The content of the existence theorem is thus that $\pi^{n\mathbb{Z}}(1+\mathfrak{p}_K^n)$ is a norm subgroup for all n; we've shown that norm subgroups are "not too small," and now we need to show that we can make them "small enough."

LEMMA 18.5. *If Γ' is a subgroup of $K^\times$ such that $K^\times \supseteq \Gamma' \supseteq \Gamma$ for a norm subgroup Γ, then Γ' is a norm subgroup as well.*

PROOF. Let L/K be a finite extension such that $\Gamma = \mathrm{N}L^\times$. As before, we may assume that L/K is abelian. Then by LCFT,

$$\Gamma'/\Gamma \subseteq K^\times/\mathrm{N}L^\times \simeq \mathrm{Gal}(L/K)$$

is a normal subgroup as $\mathrm{Gal}(L/K)$ is abelian by assumption. Thus, there exists some intermediate extension $L/K'/K'$ with $\Gamma'/\Gamma = \mathrm{Gal}(L/K')$, and

$$\begin{aligned} K^\times/\mathrm{N}(K')^\times = \mathrm{Gal}(K'/K) &= \mathrm{Gal}(L/K)/\mathrm{Gal}(L/K') = (K^\times/\mathrm{N}L^\times)/(\Gamma'/\Gamma) \\ &= K^\times/\Gamma' \end{aligned}$$

canonically. Thus, $\Gamma' = \mathrm{N}(K')^\times$, which is the desired result.

Note that we have implicitly used the fact that following diagram commutes (for abelian extensions L/K) by our explicit setup of LCFT:

$$\begin{array}{ccc} \mathrm{Gal}(L/K) & \simeq & K^\times/\mathrm{N}L^\times \\ \downarrow & & \downarrow{\scriptstyle \alpha} \\ \mathrm{Gal}(K'/K) & \simeq & K^\times/\mathrm{N}(K')^\times. \end{array}$$

Since the inverse image of $\Gamma'/\Gamma = \mathrm{Ker}(\alpha)$ in $K^\times$ is both Γ' and $\mathrm{N}(K')^\times$, we again obtain $\Gamma' = \mathrm{N}(K')^\times$. □

Now, a digression: in the second lecture, we said that

$$K^\times/(K^\times)^2 \simeq \mathrm{Gal}^{\mathrm{ab}}(K)/2 \simeq \mathrm{Hom}\left(K^\times/(K^\times)^2, \mathbb{Z}/2\mathbb{Z}\right),$$

assuming $\mathrm{char}(K) = 0$ (in particular, not 2) and where the first isomorphism is via LCFT. That is, $K^\times/(K^\times)^2$ is self-dual. Now we ask, how do we generalize this beyond $n = 2$? The answer is to use Kummer theory.

Recall that, assuming $n \nmid \mathrm{char}(K)$ and that the group of nth roots of unity $\mu_n \subseteq K^\times$ has order n, we have

$$K^\times/(K^\times)^n \simeq \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(K), \mu_n),$$

where these are group homomorphisms. The upshot is that if K is also local, we'd expect that

$$K^\times/(K^\times)^n \simeq \mathrm{Hom}(K^\times/(K^\times)^n, \mu_n). \tag{18.1}$$

Indeed, we have a map defined by

$$\begin{aligned} K^\times/(K^\times)^n &= \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(K), \mu_n) \\ &= \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}^{\mathrm{ab}}(K), \mu_n) \\ &= \mathrm{Hom}_{\mathrm{cts}}\left(\varprojlim_{L/K} K^\times/\mathrm{N}L^\times, \mu_n\right) \\ &= \varinjlim_{L/K} \mathrm{Hom}(K^\times/\mathrm{N}L^\times, \mu_n) \\ &\hookrightarrow \mathrm{Hom}_{\mathrm{cts}}(K^\times, \mu_n) \end{aligned}$$

$$= \mathrm{Hom}(K^\times/(K^\times)^n, \mu_n),$$

where the second equality is because all such maps must factor through the abelianization of $\mathrm{Gal}(K)$ (since μ_n is abelian), the third is by LCFT, and the fourth is by duality. Note that the inverse limits are over finite extensions L/K, and that "continuous" (which is unnecessary when the domain is finite) here means that a map kills some compact open subgroup, justifying the injection above. We'd like to show that this map is also an isomorphism. Note that $K^\times/(K^\times)^n$ is a finite abelian group and n-torsion; thus, it suffices to show that both sides have the same order.

CLAIM 18.6. *Let A be an n-torsion finite abelian group. Then*

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

PROOF. A is a direct sum of groups $\mathbb{Z}/d\mathbb{Z}$ for $d \mid n$, so we may reduce to the case where $A = \mathbb{Z}/d\mathbb{Z}$ for such a d (for the general case, direct sums and Hom commute). Then

$$\mathrm{Hom}(\mathbb{Z}/d\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})[d]$$

which has order $d = \#A$, as desired. □

This shows that (18.1) is a *canonical* isomorphism (though the general statement of the claim alone shows that it is an isomorphism). In the $n = 2$ case, one can easily see that this is just the Hilbert symbol.

COROLLARY 18.7. *If $\mu_n \subseteq K$, then $(K^\times)^n$ is a norm subgroup.*

PROOF. If we dualize our Kummer theory "picture," we obtain the following commutative diagram:

$$\begin{array}{ccccc} & & \mathrm{Gal}(K) & \xrightarrow{\text{cts}} & \mathrm{Hom}(K^\times/(K^\times)^n, \mu_n) \\ & & \downarrow & \overset{\beta}{\nearrow}_{\text{cts}} & \\ K^\times & \xrightarrow[\text{cts}]{\alpha} \varprojlim_{L/K} K^\times/\mathrm{N}L^\times & = & \mathrm{Gal}^{\mathrm{ab}}(K), & \end{array}$$

where α is continuous as an open subgroup inside the inverse limit is a norm subgroup, hence its inverse image in $K^\times$ is a finite-index and open subgroup. As we just saw, $\mathrm{Ker}(\beta \circ \alpha) = (K^\times)^n$, which is open (i.e., the full inverse image under the canonical projection maps of a subset of $K^\times/\mathrm{N}L^\times$ for some L/K) in the inverse limit as the maps are continuous. Thus, by Lemma 18.5, $(K^\times)^n$ is a norm subgroup. □

Note that the map β above is surjective since it is realized as $\mathrm{Gal}^{\mathrm{ab}}(K)$ modulo nth powers.

REMARK 18.8. "A priori" (i.e., if we forgot about the order of each group), the kernel of this composition could be bigger than $(K^\times)^n$. By arguing that the two were equal, we've produced a "small" norm subgroup.

PROOF (OF EXISTENCE THEOREM). Let K be a general local field of characteristic 0. Let $L := K(\zeta_n)/K$, where ζ_n denotes the set of primitive nth roots of unity. Since $(L^\times)^n$ is a norm subgroup in $L^\times$ by Corollary 18.7, $\mathrm{N}(L^\times)^n = \mathrm{N}((L^\times)^n) \subseteq K^\times$ is a norm subgroup in $K^\times$. But $\mathrm{N}(L^\times)^n \subseteq (K^\times)^n \subseteq K^\times$, so Lemma 18.5 shows that $(K^\times)^n$ is a norm subgroup in $K^\times$.

Now, observe that for all N, there exists some n such that

$$(\mathcal{O}_K^\times)^n = (K^\times)^n \cap \mathcal{O}_K^\times \subseteq 1 + \mathfrak{p}_K^{\mathrm{N}}.$$

Indeed, note that $(\mathcal{O}_K^\times)^{q-1} \subseteq 1 + \mathfrak{p}_K$, where $q = \#\mathcal{O}_K/\mathfrak{p}_K$ (since the reduction mod $\mathfrak{p}_K$ raised to the $(q-1)$st power must be 1). Thus, for sufficiently large $v(n)$ we have $(\mathcal{O}_K^\times)^{(q-1)n} \subseteq 1 + \mathfrak{p}_K^N$, since in general $(1+x)^n = 1 + nx + \cdots$ (where the ellipsis represents higher-order terms), and if $v(n) \gg 0$ then all terms aside from 1 will be in $\mathfrak{p}_K^N$.

As for finite-index subgroups "in the $\mathbb{Z}$-direction," that is, where we restrict to multiples of π^N, it suffices to simply replace n by nN, so that only elements of valuation divisible by N are realized. Thus, every finite-index open subgroup of $K^\times$ contains $(K^\times)^n$ for some n, which is a norm subgroup as shown above, hence is itself a norm subgroup by Lemma 18.5. □

Let us now quickly revisit Kummer theory, which, as we will demonstrate, in fact says something very general about group cohomology. Let G be a profinite group, so that $G = \varprojlim_i G_i$ where the G_i are finite groups.

Definition 18.9. A G-module M is *smooth* if for all $x \in M$, there exists a finite-index open subgroup $K \subseteq G$ such that $K \cdot x = x$.

Example 18.10. If $G := \mathrm{Gal}(\overline{K}/K)$, then G acts on both $\overline{K}$ and $\overline{K}^\times$, both of which are smooth G-modules. This is because every element of either G-module lies in some finite extension L/K, hence fixed by $\mathrm{Gal}(\overline{K}/L)$ which is a finite-index open subgroup by definition.

Smoothness allows to reduce to the case of a finite group, from what is often a very complicated profinite group. We now must define a notion of group cohomology for profinite groups, as our original formulation was only for finite groups.

Definition 18.11. Let X be a complex of smooth G-modules bounded from below. Then

$$X^{\mathrm{h}G} := \varinjlim_i \left(X^{K_i}\right)^{\mathrm{h}G/K_i},$$

where $K_i := \mathrm{Ker}(G \to G_i)$ and X^{K_i} denotes the vectors stabilized (naively) by K_i.

It's easy to see that this forms a directed system. Note that G_i doesn't act on X, as it is only a quotient of G, but it does act on the vectors stabilized by K_i. The K_i are compact open subgroups of G that are decreasing in size. Taking "naive invariants" by K_i is worrisome, as it does not preserve quasi-isomorphism, but in fact we have the following:

Claim 18.12. *If X is acyclic, then $X^{\mathrm{h}G}$ is too.*

The proof is omitted, though we note that it is important that X is bounded from below. We have the following "infinite version" of Hilbert's Theorem 90:

Proposition 18.13. *If L/K is a (possibly infinite) G-Galois extension, then*

$$H^1(G, L^\times) := H^1\left((L^\times)^{\mathrm{h}G}\right) = 0.$$

Proof. We write $L = \bigcup_i L_i$, where each L_i is a finite G_i-Galois extension of K. Then by definition,

$$H^1(G, L^\times) = \varinjlim_n H^1(G_i, K_i^\times) = 0$$

by Hilbert's Theorem 90. □

COROLLARY 18.14. *Let* $G := \mathrm{Gal}(\overline{K}/K)$ *and* n *be prime to* $\mathrm{char}(K)$. *If* $\mu_n \subseteq K$, *then*

$$K^\times/(K^\times)^n \simeq \mathrm{Hom}_{\mathrm{cts}}(G, \mu_n).$$

PROOF. We have a short exact sequence of smooth G-modules

$$0 \to \mu_n \to \overline{K}^\times \xrightarrow{x \mapsto x^n} \overline{K}^\times \to 0.$$

The long exact sequence on cohomology then gives

$$\underbrace{H^0(G, \overline{K}^\times)}_{K^\times} \xrightarrow{x \mapsto x^n} \underbrace{H^0(G, \overline{K}^\times)}_{K^\times} \to H^1(G, \mu_n) \to \underbrace{H^1(G, \overline{K}^\times)}_{0}$$

by Hilbert's Theorem 90 (Proposition 18.13). Thus, $K^\times/(K^\times)^n \simeq H^1(G, \mu_n)$. Since $\mu_n \subseteq K$ as in the setting of Kummer theory, it is fixed by G; as we saw via cocycles, for the trivial group action we have $H^1(G, \mu_n) = \mathrm{Hom}_{\mathrm{cts}}(G, \mu_n)$, which gives the desired result. □

Thus, we can actually derive Kummer theory very simply from abstract group cohomology and Hilbert's Theorem 90.

LECTURE 19

Brauer Groups

In this lecture, we present an overview of Brauer groups. Our presentation will be short on proofs, but we will give precise constructions and formulations of claims. For complete proofs, see [**Mil13**, **Ser79**, **Boy07**]. Our motivating question is: "what was all that stuff about Hamiltonian algebras?" (see Problem 5 of Problem Set 1, Problem 3 of Problem Set 2, and Problem 2 of Problem Set 3). We will see that there are two objects called the "Brauer group," one which has a cohomological definition, and one which has a more general algebraic definition; we'll show that the two coincide.

Recall that, if L/K is a G-Galois extension of nonarchimedean local fields, then $\mathbb{Z}[-2]^{\mathrm{t}G} \simeq (L^\times)^{\mathrm{t}G}$. When we took H^0 (zeroth cohomology), we obtained LCFT, that is, $K^\times/\mathrm{N}L^\times \simeq H_1(G,\mathbb{Z}) = G^{\mathrm{ab}}$. This is natural, as $L^\times$ is in degree 0. But $\mathbb{Z}$ is in degree 2, so what if we take H^2? Well, we obtain an isomorphism

$$\hat{H}^0(G,Z) \simeq \hat{H}^2(G,L^\times),$$

where the left-hand side is very simply isomorphic to

$$\mathbb{Z}/[L:K]\mathbb{Z} = \mathbb{Z}/\#G\mathbb{Z} = \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z},$$

since the invariants are $\mathbb{Z}$ as G acts trivially on $\mathbb{Z}$, and the norms correspond to multiplication by $\#G$. However, the right-hand side is more mysterious, motivating the following definition:

Definition 19.1. The *cohomological Brauer group of* L/K is

$$\mathrm{Br}^{\mathrm{coh}}(K/L) := H^2(G,L^\times).$$

Remark 19.2. What happens if we vary L? Suppose we have Galois extensions $L_2/L_1/K$, with $\mathrm{Gal}(L_i/K) = G_i$ for $i = 1,2$. Then we have a short exact sequence

$$0 \to \mathrm{Gal}(L_2/L_1) \to G_2 \to G_1 \to 0,$$

and maps

$$\mathrm{Br}^{\mathrm{coh}}(L_1/K) = H^2(G_1,L_1^\times) \to H^2(G_2,L_1^\times) \to H^2(G_2,L_2^\times) = \mathrm{Br}^{\mathrm{coh}}(L_2/K)$$

since invariance with respect to G_2 implies impvariance with respect to G_1, and via the embedding $L_1^\times \hookrightarrow L_2^\times$. This motivates the following definition.

Definition 19.3. The *cohomological Brauer group of* K is

$$\mathrm{Br}^{\mathrm{coh}}(K) := \varinjlim_{L/K} \mathrm{Br}^{\mathrm{coh}}(K/L) = H^2(\mathrm{Gal}(K),\overline{K}^\times),$$

where the directed limit is over finite Galois extensions L/K.

Note that the right-most expression above uses our notation from last lecture.

CLAIM 19.4. *Under* LCFT*, the following diagram commutes:*

$$\begin{array}{ccc} H^2(G_2, L_1^\times) & \longrightarrow & H^2(G_1, L_1^\times) \\ \| & & \| \\ \frac{1}{[L_1:K]}\mathbb{Z}/\mathbb{Z} & \hookrightarrow & \frac{1}{[L_2:K]}\mathbb{Z}/\mathbb{Z}. \end{array}$$

COROLLARY 19.5. *For a nonarchimedean local field K, we have*

$$\mathrm{Br}^{\mathrm{coh}}(K) \simeq \mathbb{Q}/\mathbb{Z}.$$

REMARK 19.6. One can also show that the top-most map is injective. For an extension L/K of nonarchimedean local fields, there is an exact sequence

$$0 \to \mathrm{Br}^{\mathrm{coh}}(K/L) \to \underbrace{\mathrm{Br}^{\mathrm{coh}}(K)}_{H^2(\mathrm{Gal}(K),\overline{K}^\times)} \to \underbrace{\mathrm{Br}^{\mathrm{coh}}(L)}_{H^2(\mathrm{Gal}(L),\overline{K}^\times)},$$

which we'll justify next time.

We now turn to the algebraic perspective, which provides the classical definition of the Brauer group.

PROPOSITION 19.7. *Let K be a field, and let A be a finite-dimensional K-algebra with center K. Then the following are equivalent:*

(1) A is simple, that is, it has no non-trivial 2-sided ideals.
(2) $A \otimes_K L \simeq \mathrm{M}_n(L)$ (i.e., an $n \times n$ matrix algebra) for some separable extension L/K.
(3) $A \simeq \mathrm{M}_n(D)$ for some central (i.e., with center K) division (i.e., multiplicative inverses exist, but multiplication is not necessarily commutative) algebra D over K.

If these conditions hold, then A is called a central simple algebra *(*CSA*; alternatively,* Azumaya algebra*)* over K.

COROLLARY 19.8. *Any central simple algebra over K has dimension a square.*

PROOF. The dimension of A is preserved by the tensoring operation in (2), and $\mathrm{M}_n(L)$ has square dimension. □

EXAMPLE 19.9. (1) $\mathrm{M}_n(K)$.
(2) A central division algebra over K.
(3) The Hamiltonians over $R := K$.
(4) For all fields K with $\mathrm{char}(K) \neq 2$ and elements $a, b \in K^\times$, $H_{a,b}$ is a CSA.

However, a general field L/K does not satisfy the centrality property, and indeed, its dimension might not be a square.

DEFINITION 19.10. The CSA *Brauer group of K* is

$$\mathrm{Br}^{\mathrm{csa}}(K) := \{\text{equivalence classes of CSAs over } K\}$$

with respect to the equivalence relation $A \simeq B$ if and only if A and B are matrix algebras over isomorphic division algebras in (3) above (not necessarily of the same dimension).

REMARK 19.11. The isomorphism class of A depends only on the isomorphism class of D.

PROPOSITION 19.12. *If A and B are* CSA*s over K, then $A \otimes_K B$ is also a* CSA *(note that tensor products multiply dimension, so $A \otimes_K B$ also has square dimension). Up to equivalence, this only depends on $[A], [B] \in \mathrm{Br}^{\mathrm{csa}}(K)$, so $\mathrm{Br}^{\mathrm{csa}}(K)$ forms an abelian group.*

The proof is omitted; showing that $A \otimes_K B$ is simple is rather annoying. We note, however, that matrix algebras over K represent the identity element (or "0 equivalence class") of $\mathrm{Br}^{\mathrm{csa}}(K)$. The inverse of A is A, but with opposite multiplication (i.e., $x \cdot y := yx$), which we denote A^{op}. Indeed, we have a canonical algebra homomorphism

$$A \otimes_K A^{\mathrm{op}} \to \mathrm{End}_K(A),$$

with A and A^{op} acting on opposite sides (note that $\mathrm{End}_K(A)$ is in the 0 equivalence class of $\mathrm{Br}^{\mathrm{csa}}(K)$). The kernel of this (nonzero) map must be a 2-sided ideal, so since $A \otimes_K A^{\mathrm{op}}$ is simple, it must be injective. Since both sides have dimension $\dim_K(A)^2$ over K, it is therefore also surjective, hence an isomorphism.

DEFINITION 19.13. The CSA *Brauer group of L/K* is

$$\mathrm{Br}^{\mathrm{csa}}(K/L) := \{\text{equivalence classes of CSAs } A : A \otimes_K L \simeq \mathrm{M}_n(L)\},$$

and we say that such an A *splits* over L.

This notion is equivalent to the underlying division algebra D splitting over L, which likewise means that $D \otimes_K L \simeq \mathrm{M}_n(L)$ is no longer a division algebra. Then clearly

$$\mathrm{Br}^{\mathrm{csa}}(K) = \bigcup_{\substack{L/K \\ \text{seperable}}} \mathrm{Br}^{\mathrm{csa}}(K/L).$$

EXAMPLE 19.14.
(1) If K is algebraically closed, then $\mathrm{Br}^{\mathrm{csa}}(K) = \{0\}$ is clearly trivial.
(2) $\mathrm{Br}^{\mathrm{csa}}(\mathbb{R}) = \{\mathbb{R}, \mathbb{H}\} = \mathbb{Z}/2\mathbb{Z}$, since the only other division algebra over R is $\mathbb{C}$ which is not central. Note that the Hamiltonians $\mathbb{H}$ split over $\mathbb{C}$ and have dimension $4 = 2^2$.
(3) $H_{a,b}$ splits over $K(\sqrt{a})$ and $K(\sqrt{b})$, which are the usual commutative subalgebras of $H_{a,b}$. In fact, we can take $K(\sqrt{c})$ for any $c \in K$, and can also conjugate by units. Thus, in the following claim, L is very non-unique. Note that, unlike in this case, such an L need not be Galois over K; examples are hard to find, but were discovered in the 1970s.

CLAIM 19.15. *An n^2-dimensional central division algebra D/K splits over a degree-n extension L/K if and only if $K \subseteq L \subseteq D$ as a subalgebra. Equivalently, L is a maximal commutative subalgebra in D.*

First, we have the (easy) fact that any commutative subalgebra of a division algebra is a field. This is similar to the fact that every finite-dimensional integral domain over a field is itself a field. This is because multiplication by any element is injective, and given by a matrix, hence surjective. Thus, some element maps to the identity, providing the desired inverse element. Then there is the (non-obvious) fact that $\dim_K(D)$ is the square of the dimension of any maximal commutative subalgebra of D over K. We prove one direction of the claim:

PROOF. Suppose $K \subseteq L \subseteq D$, where $[L : K] = n$ and $\dim_K(D) = n^2$. We claim that D splits over L. We have a map

$$D \otimes_K L \to \mathrm{End}_L(D) = \mathrm{M}_n(L)$$

with L acting on D via right multiplication and D acting on itself via left multiplication; the two actions commute. This map is injective (if $dxl = x$ for some $d \in D$, $l \in L$, and all $x \in D$, then $dl = 1$, hence $dx = xl^{-1} = xd$ for all $x \in D$ and therefore $d \in K$, so $d \otimes l = 1 \otimes 1$), and therefore surjective and an isomorphism, as desired. □

THEOREM 19.16. *For every Galois extension L/K, we have* $\mathrm{Br}^{\mathrm{coh}}(K) \simeq \mathrm{Br}^{\mathrm{csa}}(K)$ *and* $\mathrm{Br}^{\mathrm{coh}}(K/L) \simeq \mathrm{Br}^{\mathrm{csa}}(K/L)$.

Note that the cohomological Brauer group is defined only for Galois extensions L/K, whereas the CSA Brauer group is defined for all extensions L/K. This gives meaning to the cohomological definition of the Brauer group. We provide the following (incomplete) proof sketch:

PROOF. For a G-Galois extension L/K, we define a map

$$H^2(G, L^\times) \to \mathrm{Br}^{\mathrm{csa}}(K/L). \tag{19.1}$$

Every element in H^2 is represented by a 2-cocycle, that is, a map $\varphi\colon G \times G \to L^\times$ satisfying

$$\overset{g_1}{\varphi(g_2,g_3)}\varphi(g_1, g_2g_3) = \varphi(g_1g_2, g_3)\varphi(g_1, g_2)$$

for every $g_1, g_2, g_3 \in G$, and where we have introduced the notation ${}^g x := g \cdot x$. We define a CSA associated to each such φ as follows: form

$$L[G] = \left\{ \textstyle\sum_{g\in G} x_g[g] : x_g \in L \right\}$$

subject to the relations

$$[g]x = {}^g x[g] \quad \text{and} \quad [g][h] = \varphi(g, h)[gh]$$

for each $x \in L$ and $g, h \in G$. We now check that the 2-cocyle identity is equivalent to associativity:

$$\begin{aligned}
[g_1]([g_2][g_3]) &= [g_1]\varphi(g_2, g_3)[g_2g_3] \\
&= {}^{g_1}\varphi(g_2, g_3)[g_1][g_2g_3] \\
&= {}^{g_1}\varphi(g_2, g_3)\varphi(g_1, g_2g_3)[g_1g_2g_3] \\
&= \varphi(g_1g_2, g_3)\varphi(g_1, g_2)[g_1g_2g_3] \\
&= \varphi(g_1, g_2)[g_1g_2][g_3] \\
&= ([g_1][g_2])[g_3],
\end{aligned}$$

for all $g_1, g_2, g_3 \in G$. We claim, but do not prove, that the equivalence class of this CSA only depends on φ, up to coboundaries, and that it splits over L. Moreover, our map (19.1) is a group isomorphism. □

This is not an especially deep theorem, despite being far from obvious; the complete proof uses a lot of structure theory that is not particularly memorable.

We now ask, how many isomorphism classes of central division algebras over K of degree n^2 are there? When $n = 1^2$, there is only 1; when $n = 2^2$, there is again only 1, as shown in Problem 2(d) of Problem Set 3.

CLAIM 19.17. *There are $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$ isomorphism classes of central division algebras over K of degree n^2.*

CLAIM 19.18. *Let L/K be a degree-n extension of nonarchimedean local fields. Then the following diagram commutes:*

$$\begin{array}{ccc} \mathrm{Br}(K) & \longrightarrow & \mathrm{Br}(L) \\ \| \text{LCFT} & & \| \text{LCFT} \\ \mathbb{Q}/\mathbb{Z} & \xrightarrow{\times n} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Note that we have simply denoted the Brauer group by Br in light of Theorem 19.16. Indeed, we've seen that both horizontal maps should have non-trivial kernel; when $L = \overline{K}$, $\mathrm{Br}(L)$ is trivial. Then a central division algebra of degree n^2 has order n in $\mathrm{Br}(K)$, i.e., is n-torsion, since it splits over its degree-n maximal commutative subalgebra. Alternatively, $H^2(G, -)$ is $\#G$-torsion, as proven in Problem 2(c) of Problem Set 7.

COROLLARY 19.19. *Any degree-n^2 division algebra splits over any degree-n extension of K.*

On the other hand, if $A \simeq \mathrm{M}_n(D)$ is a CSA over K of degree n^2, representing some n-torsion class in $\mathrm{Br}(K)$, then A splits over the maximal commutative subalgebra of D. This implies that A is itself a division algebra if it is n-torsion, but not m-torsion for any $m \mid n$. This gives $\varphi(n)$: the division algebras come from classes in $\mathbb{Z}/n\mathbb{Z}$ which do not arise from any smaller $\mathbb{Z}/m\mathbb{Z}$. Another upshot is the following:

COROLLARY 19.20. *Any degree-n^2 central division algebra over K contains every degree-n field extension of L.*

PROOF. Any n-torsion class in $\mathrm{Br}(K)$ maps to zero in the Brauer group $\mathrm{Br}(L)$ over any degree-n extension L of K by Claim 19.18. Thus, it splits over L, hence contains it by Claim 19.15. □

For $n = 2$, this is the result that every $x \in K$ admits a square in $H_{a,b}$, which was shown in Problem 2(c) of Problem Set 3.

LECTURE 20

Proof of the First Inequality

We begin by fulfilling our promise from the last lecture. Let $K^{\text{sep}} = \overline{K}/L/K$ be an extension of nonarchimedean local fields.

CLAIM 20.1. *There is an exact sequence*

$$0 \to \mathrm{Br}^{\mathrm{coh}}(K/L) \to \mathrm{Br}^{\mathrm{coh}}(K) \to \mathrm{Br}^{\mathrm{coh}}(L).$$

Recall that $\mathrm{Br}^{\mathrm{coh}}(K/L)$ essentially encodes division algebras over K that split over L, and $\mathrm{Br}^{\mathrm{coh}}(K)$ and $\mathrm{Br}^{\mathrm{coh}}(L)$ encode division algebras over K and L, respectively. The kernel of the map $\mathrm{Br}^{\mathrm{coh}}(K) \to \mathrm{Br}^{\mathrm{coh}}(L)$ is essentially division algebras over K that split over L, but we'll make this precise from the cohomological side. One can do this with spectral sequences (which are a bit annoying), but our focus on chain complexes will allow for the proofs to come out much more conceptually. We will need the following construction:

DEFINITION 20.2. Let X be a chain complex of A-modules. Then $\tau^{\leq n}X$ is the "truncated" chain complex

$$\cdots \to X^{n-2} \xrightarrow{d^{n-2}} X^{n-1} \xrightarrow{d^{n-1}} \mathrm{Ker}(d^n) \to 0 \to 0 \to \cdots$$

LEMMA 20.3. *The identity map $\tau^{\leq n}X \to X$ is a map of complexes, and this gives an isomorphism $H^i(\tau^{\leq n}X) \xrightarrow{\sim} H^i(X)$ for all $i \leq n$.*

PROOF. It suffices to note that the two central squares below commute by the definition of a chain complex:

$$\begin{array}{ccccccccccccc}
\cdots & \longrightarrow & X^{n-2} & \longrightarrow & X^{n-1} & \longrightarrow & \mathrm{Ker}(d^n) & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \\
 & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
\cdots & \longrightarrow & X^{n-2} & \longrightarrow & X^{n-1} & \longrightarrow & X^n & \longrightarrow & X^{n+1} & \longrightarrow & X^{n+1} & \longrightarrow & \cdots .
\end{array}$$

□

COROLLARY 20.4. *If $X \xrightarrow{\text{qis}} Y$, then the induced map $\tau^{\leq n}X \to \tau^{\leq n}Y$ is also a quasi-isomorphism.*

REMARK 20.5. Truncation, $\tau^{\leq n}$, is the one operation that does *not* commute with cones.

DEFINITION 20.6. $\tau^{\geq n+1}X := \mathrm{hCoker}(\tau^{\leq n}X \to X)$.

LEMMA 20.7. *$H^iX \xrightarrow{\sim} H^i\tau^{\geq n+1}X$ for all $i \geq n+1$.*

PROOF. A simple application of the long exact sequence on cohomology suffices. □

For the application to Brauer groups, we first introduce some notation:

$$\begin{aligned} G_K &:= \mathrm{Gal}(\overline{K}/K) \\ G_L &:= \mathrm{Gal}(\overline{K}/L) \\ H &:= \mathrm{Gal}(L/K), \end{aligned}$$

where we note that L/K must be Galois for $\mathrm{Br}^{\mathrm{coh}}(K/L)$ to be defined. Recall that

$$\begin{aligned} \mathrm{Br}^{\mathrm{coh}}(K) &:= H^2(G_K, \overline{K}^\times) \\ \mathrm{Br}^{\mathrm{coh}}(L) &:= H^2(G_L, \overline{K}^\times) \\ \mathrm{Br}^{\mathrm{coh}}(K/L) &:= H^2(H, \overline{L}^\times). \end{aligned}$$

The main observation is that

$$\left[(\overline{K}^\times)^{\mathrm{h}G_L}\right]^{\mathrm{h}H} = (\overline{K}^\times)^{\mathrm{h}G_K}$$

by Problem 3 on Problem Set 6, since we have a short exact sequence

$$1 \to G_L \to G_K \to H \to 1.$$

Proof (of Claim 20.1). Note that $L^\times = \tau^{\leq 0}(\overline{K}^\times)^{\mathrm{h}G_L}$ as complexes of H-modules. Then by definition,

$$\mathrm{hCoker}\left(L^\times \to (\overline{K}^\times)^{\mathrm{h}G_L}\right) = \tau^{\geq 1}(\overline{K}^\times)^{\mathrm{h}G_L} \simeq \tau^{\geq 2}(\overline{K}^\times)^{\mathrm{h}G_L},$$

since this is equivalent to asserting that $H^1(G_L, \overline{K}^\times) = 0$, which is just Hilbert's Theorem 90. Thus,

$$\mathrm{hCoker}\left((L^\times)^{\mathrm{h}H} \to (\overline{K}^\times)^{\mathrm{h}G_K}\right) = \left(\tau^{\geq 2}(\overline{K}^\times)^{\mathrm{h}G_L}\right)^{\mathrm{h}H}.$$

Finally, the long exact sequence on cohomology gives

$$\underbrace{H^1\left(\tau^{\geq 2}(\overline{K}^\times)^{\mathrm{h}G_L}\right)^{\mathrm{h}H}}_{0} \to \underbrace{H^2(H, L^\times)}_{\mathrm{Br}^{\mathrm{coh}}(K/L)} \to \underbrace{H^2(G_K, \overline{K}^\times)}_{\mathrm{Br}^{\mathrm{coh}}(K)} \to \underbrace{H^2(G_L, \overline{K}^\times)^H}_{\mathrm{Br}^{\mathrm{coh}}(L)^H} \hookrightarrow \mathrm{Br}^{\mathrm{coh}}(L)$$

since for the first term, taking group cohomology can only increase the degrees of a complex, therefore cannot introduce a non-trivial degree-1 cohomology, and for the last, group cohomology is equivalent to taking invariants in the lowest non-zero degree of a complex. □

Now we turn to global class field theory, which is in many ways less beautiful than local class field theory; our treatment will be commensurately less thorough.

Theorem 20.8 (Main Theorems of GCFT). *Let F be a global field. Then*

$$\mathrm{Gal}^{\mathrm{ab}}(G) \simeq \widehat{(\mathbb{A}_F^\times / F^\times)},$$

and moreover, for all finite Galois extensions E/F, we have

$$\mathrm{Gal}(E/F)^{\mathrm{ab}} \simeq \mathrm{N}(\mathbb{A}_E^\times) \backslash \mathbb{A}_F^\times / F^\times.$$

Note that here $\widehat{\cdot}$ denotes profinite completion as usual, and in the second equation we are taking the quotient of $\mathbb{A}_F^\times$ by two separate objects.

The "motto" of GCFT is that $C_F := \mathbb{A}_F^\times / F^\times$, the *idèle class group of F*, plays the role of $K^\times$ in LCFT, and they exhibit very similar behaviors (there's a theory of "class formations" to make this analogy tighter). Thus, we will be importing many of the methods of LCFT for our proofs of GCFT; for instance, we would expect that

some sort of "existence theorem" along with Kummer theory would allow us to prove the former statement of Theorem 20.8 from the latter. We likely won't have time to show this implication in class, so instead we'll focus on showing this second assertion.

Our main "inputs" are the following:

THEOREM 20.9 (Inequalities of GCFT). *(1) Let E/F be a degree-n cyclic extension of global fields. Then $\chi(C_E) = n$ (i.e., the Herbrand quotient of C_E).*
(2) For all finite G-Galois extensions E/F of global fields, $H^1(G, C_E) = 0$.

The second statement is analogous to Hilbert's Theorem 90, but is *much* harder to show. These two statements are variously called the "first inequality" and "second inequality" of GCFT; our (arbitrarily) preferred convention is indicated. Indeed, the first inequality gives

$$\#\hat{H}^0(\mathbb{Z}/n\mathbb{Z}, C_E) = n \cdot \#H^1(\mathbb{Z}/n\mathbb{Z}, C_E) \geq n,$$

and the second inequality gives $\#H^0(\mathbb{Z}/n\mathbb{Z}, C_E) \leq n$, hence it is precisely n.

In this lecture, we will prove the first inequality. Throughout, we let E/F be a degree-n cyclic extension of global fields. To do this, we will compute $\chi(E^\times)$ and $\chi(\mathbb{A}_E^\times)$, or at least their quotient, which will give us $\chi(C_E)$ via the exact sequence

$$0 \to E^\times \to \mathbb{A}_E^\times \to C_E \to 0.$$

A slight problem is that both Herbrand quotients are infinite.

First, a general comment on the structure of the group cohomology of $\mathbb{A}_E^\times$:

CLAIM 20.10. *For a G-Galois extension E/F of global fields, we have*

$$\hat{H}^i(G, \mathbb{A}_E^\times) = \bigoplus_{v \in M_F} \hat{H}^i\big(G, (E \otimes_F F_v)^\times\big)$$

for each i, where M_F denotes the set of places (i.e., equivalence classes of valuations) of F.

To be clear, this claim is entirely local, using the structure of the adèles as amalgamating all local information about a global field; we do not make use of the diagonal embedding of $E^\times$, which allows us to treat a field globally within the adèles. Note that $E \otimes_F F_v$ is like the completion of E at v.

PROOF. Recall that

$$\mathbb{A}_E^\times = \varinjlim_{\substack{S \subset M_F \\ \#S < \infty}} \left(\prod_{v \in S} (E \otimes_F F_v)^\times \times \prod_{v \notin S} (\underbrace{\mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v}}_{\mathcal{O}_{E \otimes_F F_v}})^\times \right),$$

where S contains all ramified primes and infinite places (the set of which we henceforth denote by M_F^∞). Note that usually we take $S \subset M_E$; this alternate formulation instead expresses such places of E in terms of which places of F they lie over. By Problem 6(h) of Problem Set 6, $\hat{H}^i(G, -)$ commutes with direct limits bounded uniformly from below, and also with direct products. This implies that

$$\hat{H}^i(G, \mathbb{A}_E^\times) = \varinjlim_{\substack{S \subset M_F \\ \#S < \infty}} \left(\bigoplus_{v \in S} \hat{H}^i\big(G, (E \otimes_F F_v)^\times\big) \times \prod_{v \notin S} \hat{H}^i\big(G, (\mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v})^\times\big) \right)$$

$$= \varinjlim_{\substack{S \subset M_F \\ \#S < \infty}} \bigoplus_{v \in S} \hat{H}^i\big(G, (E \otimes_F F_v)^\times\big).$$

Indeed, because S was assumed to contain all ramified primes, the extension E_w/F_v of local fields is unramified for any place $w \mid v$ of E with $v \notin S$, hence it has Galois group the decomposition group G_w. Then we have

$$\hat{H}^i\big(G, (\mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_{F_v})^\times\big) = \hat{H}^i(G_w, \mathcal{O}_{E_w}^\times) = 0$$

for any $v \notin S$ and $w \mid v$ by Problem 1(d) on Problem Set 7, since

$$(\mathcal{O}_E \otimes_{\mathcal{O}_F} \mathcal{O}_k)^\times = \prod_{w|v} \mathcal{O}_{E_w}^\times = \mathbb{Z}[G] \otimes_{\mathbb{Z}[G_w]} \mathcal{O}_{E,w}^\times$$

is an induced G-module, and the latter expression vanishes as noted in Example 14.3. □

Now we attempt to circumvent the infinite-ness of the Herbrand quotients.

Definition 20.11. For any finite $M_F^\infty \subseteq S \subset M_F$, let

$$\mathbb{A}_{F,S} := \prod_{v \in S} F_v \times \prod_{v \notin S} \mathcal{O}_{F_v}$$

denote the *ring of S-adèles*, and similarly for the *group of S-idèles* $\mathbb{A}_{F,S}^\times$.

Lemma 20.12. *There exists a finite $S \subset M_F$ with $\mathbb{A}_{F,S}^\times \cdot F^\times = \mathbb{A}_F^\times$.*

Proof. This identity is equivalent to asserting that the map

$$\mathbb{A}_{F,S}^\times \to \mathbb{A}_{F,M_F^\infty}^\times \backslash \mathbb{A}_F^\times / F^\times = \mathrm{Cl}(F)$$

to the class group of F is surjective, where we may also take the quotient by $\mathbb{A}_{F,M_F^\infty}$ since it is contained in $\mathbb{A}_{F,S}$ by assumption, and the final canonical isomorphism is by Problem 1(b) of Problem Set 2. Under this isomorphism, a uniformizer $\mathfrak{p} \subseteq \mathcal{O}_K$ of $F_\mathfrak{p}$ maps to $[\mathfrak{p}] \in \mathrm{Cl}(F)$. Since $\mathrm{Cl}(F)$ is finite, we may simply take S to be M_F^∞ along with a set of places, each associated to a distinct element of $\mathrm{Cl}(F)$. □

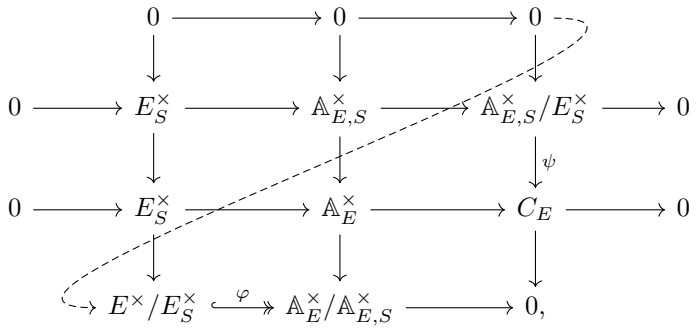
Now let us return to the case where E/F is cyclic, and choose a finite set $S \subset M_F$ containing the infinite and ramified places of S and satisfying $\mathbb{A}_{E,S}^\times \cdot E^\times = \mathbb{A}_E^\times$, which is possible by the lemma (note that $\mathbb{A}_{E,S}^\times := \mathbb{A}_{E,T}^\times$, where T is the set of places of E lying above the places of F in S; thus, we are really applying the lemma to E, and projecting the set of places obtained down to F).

Claim 20.13. *We have a short exact sequence*

$$0 \to E_S^\times \to \mathbb{A}_{E,S}^\times \to C_E \to 0,$$

where $E_S^\times := E^\times \cap \mathbb{A}_{E,S}^\times$.

PROOF. We have the following commutative diagram:



where the map φ is surjective by our choice of S and is also injective by the definition of $E_S^\times$ (i.e., $\varphi(x) \in \mathbb{A}_{E,S}^\times$ implies $x \in E_S^\times$). The snake lemma then implies that the map ψ is an isomorphism, as desired. □

By Claim 20.10, we have

$$\hat{H}^i(E, \mathbb{A}_{E,S}^\times) = \bigoplus_{v \in S} \hat{H}^\times\big(G, (E \otimes_F F_v)^\times\big),$$

so

$$\chi(\mathbb{A}_{E,S}^\times) = \prod_{v \in S} \chi\big((E \otimes_F F_v)^\times\big) = \prod_{v \in S} \chi\Big(\prod_{w \mid v} E_w^\times\Big) = \prod_{v \in S} \chi(E_w^\times) = \prod_{v \in S} [E_w : F_v]$$

for some choice of $w \mid v$ by Claim 7.8 and since

$$\Big(\prod_{w \mid v} E_w^\times\Big)^{\mathrm{t}G} \simeq (E_w^\times)^{\mathrm{t}G_w}$$

as before. Now we'd like to compute $\chi(E_S^\times)$, and we want it to satisfy

$$n \cdot \chi(E_S^\times) = \prod_{v \in S} [E_w : F_v],$$

again for some $w \mid v$. By Dirichlet's unit theorem, $E_S^\times$ is finitely generated, and therefore

$$E_S^\times \simeq (E_S^\times)_{\mathrm{tors}} \times \mathbb{Z}^r,$$

where r is the rank of $E_S^\times$. Thus, up to its torsion, $E_S^\times$ is an r-dimensional lattice.

LEMMA 20.14. *If a cyclic group G acts on an $\mathbb{R}$-vector space V, and $\Lambda_1, \Lambda_2 \subseteq V$ are two lattices fixed under the G-action, then $\chi(\Lambda_1) = \chi(\Lambda_2)$ (where we are regarding both lattices as G-modules).*

We defer the proof to the next lecture for the sake of time. Now, recall the map used in the proof of the unit theorem:

$$\begin{aligned} E_S^\times &\to \prod_{w \in T} \mathbb{R} \\ x &\mapsto (\log |x|_w)_w, \end{aligned}$$

with T the primes of E lying above those in S, as before. The proof of the unit theorem shows that this map has finite kernel, and its image is a lattice in the hyperplane $\{(y_w)_w : \sum_w y_w = 0\}$. Thus,

$$\mathrm{Im}(E_S^\times) \cup \mathbb{Z} \cdot (1, 1, \ldots, 1)$$

is a lattice in $\prod_{w \in T} \mathbb{R}$, and so

$$\chi(E_S^\times) = \chi(\mathrm{Im}(E_S^\times)) = \frac{\chi(\Lambda)}{\chi(\mathbb{Z})} = \frac{\chi(\Lambda)}{n},$$

where Λ is any G-fixed lattice. Now,

$$\Lambda := \prod_{w \in T} \mathbb{Z} \subseteq \prod_{w \in T} \mathbb{R}$$

is one such lattice. The Galois group G acts on $\prod_{w|v} \mathbb{Z}$, hence

$$\chi(\Lambda) = \chi\Big(\prod_{v \in S} \prod_{w|v} \mathbb{Z}\Big) = \prod_{v \in S} \chi\Big(\prod_{w|v} \mathbb{Z}\Big) = \prod_{v \in S} \#G_w = \prod_{v \in S} [E_w : F_v]$$

for a choice of w, as desired. This completes the proof of the first inequality.

LECTURE 21

Artin and Brauer Reciprocity, Part I

Let $F/\mathbb{Q}$ be a global field, so that we have an exact sequence

$$1 \to F^\times \hookrightarrow \mathbb{A}_F^\times \to C_F \to 1,$$

where $C_F := \mathbb{A}_F^\times / F^\times$. Last time, we almost showed that for a cyclic degree-n extension E/F, we have $\chi(C_E) = n$; it remains to prove Lemma 20.14.

LEMMA 21.1. *Let L/K be an extension of infinite fields, A be a K-algebra, and M and N be two A-modules that are finite dimensional over K with M projective over A. If $M \otimes_K L \simeq N \otimes_K L$ as $A \otimes_K L$-modules, then $M \simeq N$.*

PROOF. First note that there is an isomorphism

$$\operatorname{Hom}_A(M, N) \otimes_K L \xrightarrow{\sim} \operatorname{Hom}_{A \otimes_K L}(M \otimes_K L, N \otimes_K L). \tag{21.1}$$

Indeed, because M is a finitely generated projective module, it is a summand of a finite-rank free module, which reduces us to the case $M = A$ (since the Hom functor commutes with direct sums). Then both sides of (21.1) reduce to $N \otimes_K L$. (In fact, a more basic identity holds in greater generality: $\operatorname{Hom}_A(M, N \otimes_A P) = \operatorname{Hom}_A(M, N) \otimes_A P$ for an arbitrary algebra A as long as P is flat and M is finitely presented, i.e., $A^{n_1} \to A^{n_2} \to M \to 0$ is exact for some $n_1, n_2 \in \mathbb{Z}$).

Observe that both $M \otimes_K L$ and $N \otimes_K L$ have the same dimension over L, hence M and N have the same dimension d over K. Let $V := \operatorname{Hom}_A(M, N)$ and $W := \operatorname{Hom}_A(\Lambda^d M, \Lambda^d N)$, where $\Lambda^d(-)$ denotes the dth exterior power. Both of these are finite-dimensional K-vector spaces; in particular, V is d^2-dimensional, and W is 1-dimensional, i.e., isomorphic to K. Functoriality of Λ^d gives the determinant map $\det\colon V \to W$, which is a polynomial map of degree d with coefficients in K, in the sense that after choosing bases of V and W, it is given by a degree-d polynomial in coordinates (as it is computed as the determinant of a $d \times d$ matrix in V). We'd like to show that the map det is non-zero, as a point $\varphi \in V$ with $\det \varphi \neq 0$ is the same as an A-module isomorphism $M \simeq N$. Since K is infinite (and det is polynomial), it suffices to check this after extending scalars to L, which by (21.1) gives a determinant map

$$\operatorname{Hom}_{A \otimes_K L}(M \otimes_K L, N \otimes_K L) \to \operatorname{Hom}_{A \otimes_K L}(\Lambda^d(M \otimes_K L), \Lambda^d(N \otimes_K L)) \simeq L.$$

Since the left-hand side contains an isomorphism $M \otimes_K L \simeq N \otimes_K L$, this map must be non-zero, as desired. □

PROOF (OF LEMMA 20.14). The issue here is that Λ_1 and Λ_2 might not be commensurate (i.e., each is contained in the other up to a finite index and multiplication). However, we claim that $\Lambda_1 \otimes \mathbb{Q} \simeq \Lambda_2 \otimes \mathbb{Q}$ as $\mathbb{Q}[G]$-modules. Indeed, by Lemma 21.1, it suffices to show that $\Lambda_1 \otimes \mathbb{R} \simeq \Lambda_2 \otimes \mathbb{R}$ as $\mathbb{R}[G]$-modules, which is clear as $\Lambda_i \otimes \mathbb{R} \simeq V$ for $i = 1, 2$. Thus, taking the image of Λ_2 under this isomorphism, and

tensoring with $\mathbb{R}$ to obtain inclusion in V, there exists a G-stable lattice $\Lambda_3 \subseteq V$ that is isomorphic to Λ_2 as a $\mathbb{Z}[G]$-modules and commensurate with Λ_1. Thus, $N\Lambda_3 \subseteq \Lambda_1 \subseteq \frac{1}{N}\Lambda_3$ for some sufficiently large N, hence $\chi(\Lambda_1) = \chi(\Lambda_3) = \chi(\Lambda_2)$ as all subquotients are finite, as desired. □

We now turn to a discussion of local Kronecker–Weber theory.

THEOREM 21.2. *For any prime p,*

$$\mathbb{Q}_p^{\mathrm{ab}} = \left[\bigcup_{n\geq 0} \mathbb{Q}_p(\zeta_{p^n})\right] \cdot \mathbb{Q}_p^{\mathrm{unr}},$$

where this is the compositum with the non-completed maximal unramified extension of $\mathbb{Q}_p$.

PROOF. Recall that the extensions $\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p$ are totally ramified, with Galois groups $(\mathbb{Z}/p^n\mathbb{Z})^\times$. Thus, $K \subseteq \mathbb{Q}_p^{\mathrm{ab}}$, where we have denoted the right-hand side by K, and this gives a map

$$\mathbb{Z}_p^\times \times \widehat{\mathbb{Z}} = \widehat{\mathbb{Q}_p^\times} = \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p) \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}_p) = \left[\varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times\right] \times \widehat{\mathbb{Z}},$$

where the left-most equalities are by LCFT, followed by choice of a uniformizer of $\mathbb{Q}_p$; the map is surjective by Galois theory. Since both sides are isomorphic as abstract groups, the following lemma shows that this map is an isomorphism. □

LEMMA 21.3. *Let G be a profinite group, such that for all $n > 0$, the number of open subgroups of index n in G is finite (i.e., G is "topologically finitely generated"). Then every continuous homomorphism $\varphi\colon G \twoheadrightarrow G$ is an isomorphism.*

PROOF. If $H \subseteq G$ is a subgroup of index at most n, then $\varphi^{-1}(H) \subseteq G$ is also a subgroup of index at most n. Thus, we have a map

$$\{H \subseteq G : [G:H] \leq n\} \xrightarrow{\varphi^{-1}} \{H \subseteq G : [G:H] \leq n\},$$

which is injective as φ is surjective. By hypothesis, this set is finite, hence this map is bijective. Since

$$\mathrm{Im}(\varphi^{-1}) = \{H \subseteq G : [G:H] \leq n, \mathrm{Ker}(\varphi) \subseteq H\},$$

it follows that $\mathrm{Ker}(\varphi)$ is contained in every finite-index subgroup of G, hence $\mathrm{Ker}(\varphi)$ is trivial and φ is an isomorphism. □

We now ask: what is the automorphism of $\mathbb{Z}_p^\times \times \widehat{\mathbb{Z}}$ in the proof of Theorem 21.2? The following theorem of "explicit CFT" answers this question, but the proof is involved and not at all obvious (see [**Dwo58**]). An answer to the analogous question for global fields is not known in general, aside from the cases of $\mathbb{Q}$ and imaginary number fields.

THEOREM 21.4 (Dwork, Lubin–Tate). *(1) The element $p \in \mathbb{Q}_p^\times$ acts trivially on $\bigcup_n \mathbb{Q}_p(\zeta_{p^n})$ and acts as the Frobenius element on $\mathbb{Q}_p^{\mathrm{unr}}$.*

(2) An element $x \in \mathbb{Z}_p^\times$ acts trivially on $\mathbb{Q}_p^{\mathrm{unr}}$ and acts by x^{-1} on $\bigcup_n \mathbb{Q}_p(\zeta_{p^n})$, i.e., $\theta_p(x) \cdot \zeta_{p^n} = \zeta_{p^n}^{(x^{-1} \bmod p^n)}$, where

$$\theta_p\colon \mathbb{Q}_p^\times \to \mathrm{Gal}\Big(\bigcup_n \mathbb{Q}_p(\zeta_{p^n}) \cdot \mathbb{Q}_p^{\mathrm{unr}} \Big/ \mathbb{Q}_p\Big)$$

is the homomorphism provided by LCFT.

There are two reciprocity laws which we'd now like to introduce: *Artin reciprocity*, and *Brauer reciprocity*. We'll begin with the former. Let E/F be an abelian G-Galois extension of global fields. Recall that we expect to have

$$F^\times \backslash \mathbb{A}_F^\times / \mathrm{N}(\mathbb{A}_E^\times) = C_F/\mathrm{N}(C_E) \xrightarrow{\sim} G.$$

We'd like to construct this map.

CLAIM 21.5. LCFT *gives us a map* $\theta\colon \mathbb{A}_F^\times \to G$ *with* $\theta(\mathrm{N}(\mathbb{A}_E^\times)) = 1$.

PROOF. Let $x \in \mathbb{A}_F^\times$. For each $v \in M_F$, we have an element $x_v \in F_v^\times$, and LCFT then gives a map

$$\theta_v\colon F_v^\times \to \mathrm{Gal}(E_w/F_v) \subseteq \mathrm{Gal}(E/F) = G$$

for a place $w \mid v$ of E, where the former is the decomposition group of E/F at v. This embedding is induced by the embedding $E \subseteq E_w$. Recall that when E/F is abelian, $\mathrm{Gal}(E_w/F_v)$ is independent of the choice of w.

We now claim that the product

$$\theta(x) := \prod_{v \in M_F} \theta_v(x_v)$$

makes sense, that is, $\theta_v(x_v) = 1$ for all but finitely many v. Indeed, for almost all v, E_w/F_v is unramified and $x_v \in \mathcal{O}_{F_v}^\times$, implying that $\theta_v(x_v) = 1$ (since by LCFT, the map θ_v kills $\mathcal{O}_{F_v}^\times$ and sends a uniformizer of F_v to the Frobenius element of G).

Since $\theta_v(\mathrm{N}(E_w^\times)) = 1$ for all $v \in M_F$, we have $\theta(\mathrm{N}(\mathbb{A}_E^\times)) = 1$, as desired. □

THEOREM 21.6 (Artin Reciprocity). *We have* $\theta(F^\times) = 1$, *hence* θ *gives a map* $C_F/\mathrm{N}(C_E) \to G$.

EXAMPLE 21.7. If $E/\mathbb{Q}$ is a quadratic extension, this reduces to quadratic reciprocity. Indeed, the local Artin maps are simply given by Hilbert symbols, and from here we proved the implication.

We will proof this concurrently with Brauer reciprocity. Let E/F be a finite G-extension of global fields. We have

$$H^2(G, \mathbb{A}_E^\times) = \bigoplus_{v \in M_F} \mathrm{Br}(F_v) = \bigoplus_{v \in M_F \setminus M_F^\infty} \mathbb{Q}/\mathbb{Z} \times \bigoplus_{v \in M_F^\infty} \tfrac{1}{2}\mathbb{Z}/\mathbb{Z},$$

by Claim 20.10 and since $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$. Define the *invariant map* $\iota\colon H^2(G, \mathbb{A}_E^\times) \to \mathbb{Q}/\mathbb{Z}$ via

$$\bigoplus_{v \in M_F/M_F^\infty} \mathbb{Q}/\mathbb{Z} \xrightarrow{(x_v)_v \mapsto \sum_v x_v} \mathbb{Q}/\mathbb{Z},$$

i.e., summing over all local factors (and ignoring all infinite ones).

THEOREM 21.8 (Brauer Reciprocity). *The composition*

$$\mathrm{Br}(F/E) \to H^2(G, \mathbb{A}_E^\times) \xrightarrow{\iota} \mathbb{Q}/\mathbb{Z}$$

is zero for all $E/\mathbb{Q}$.

Note that E is essentially irrelevant here; this theorem is really about $\mathrm{Br}(F)$. The first map is induced by the diagonal embedding $E \hookrightarrow \mathbb{A}_E^\times$, and the cohomological interpretation of the Brauer group then shows that every division algebra over F is a matrix algebra except at finitely many places, which is otherwise not an obvious statement.

EXAMPLE 21.9. Any $a, b \in \mathbb{Q}^\times$ give a Hamiltonian algebra $H_{a,b}$ over $\mathbb{Q}$. At a finite prime p, the invariant is

$$\begin{cases} 0 & \text{if } H_{a,b} \otimes \mathbb{Q}_p \simeq \mathrm{M}_2(\mathbb{Q}_p), \\ 1/2 & \text{otherwise.} \end{cases} \iff \begin{cases} 0 & \text{if } (a,b)_p = 1, \\ 1/2 & \text{if } (a,b)_p = -1. \end{cases}$$

Thus, asserting that the sum of all invariants is zero is again quadratic reciprocity.

CLAIM 21.10. *Artin reciprocity is valid for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, where ζ_n is a primitive nth root of unity.*

PROOF. We proceed via explicit calculation using Dwork's theorem. We may assume that $n = \ell^r$ is a prime power, because $\mathbb{Q}(\zeta_n)$ is the compositum of $\mathbb{Q}(\zeta_{\ell^r})$ over all prime-power factors ℓ^r of n, and $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ then splits as a product over $\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^r})/\mathbb{Q})$. We then have a composition

$$\mathbb{Q}^\times \hookrightarrow \mathbb{A}_\mathbb{Q}^\times \xrightarrow{\theta} \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^r})/\mathbb{Q}) = (\mathbb{Z}/\ell^r\mathbb{Z})^\times,$$

where $\theta = \prod_p \theta_p$ as before. We'd like to show that this map is trivial. To this end, it suffices to show that $\theta(p) = 1$ for all primes p and $\theta(-1) = 1$. Suppose $p \neq \ell$; the case $p = \ell$ will be covered in the next lecture. Then

$$\begin{cases} \theta_p(p) = p, \\ \theta_\ell(p) = p^{-1}, \\ \theta_q(p) = 1, \\ \theta_\infty(p) = 1. \end{cases}$$

Indeed, recall that

$$\begin{aligned} \theta_p \colon \mathbb{Q}_p^\times &\to \mathrm{Gal}(\mathbb{Q}_p(\zeta_{\ell^r})/\mathbb{Q}_p) \\ p &\mapsto \mathrm{Frob}_p, \end{aligned}$$

and $\theta(\mathbb{Z}_p^\times) = 1$. But Frob_p corresponds to $p \in (\mathbb{Z}/\ell^r\mathbb{Z})^\times$. For the second case, $\theta_\ell(p)$ acts as $p^{-1} \in (\mathbb{Z}/\ell^r\mathbb{Z})^\times$ by Dwork's theorem, and for the third case, in which $q \neq p, \ell$, we have $p \in (\mathbb{Z}/q\mathbb{Z})^\times$ and the extension $\mathbb{Q}_q(\zeta_{\ell^r})/\mathbb{Q}_q$ is unramified. Finally, θ_∞ corresponds to taking sign, as it is a map $\mathbb{R}^\times \to \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ which contracts the connected components of $\mathbb{R}^\times$, giving a map from $\mathbb{Z}/2\mathbb{Z}$ sending 1 to complex conjugation. $\square$

LECTURE 22

Artin and Brauer Reciprocity, Part II

In this lecture, our goal is to prove both the Artin and Brauer reciprocity laws, modulo the second inequality. Recall the statement of Artin reciprocity: for a number field F and place v, LCFT gives a map

$$\theta_v \colon F_v^\times \to \mathrm{Gal}^{\mathrm{ab}}(F),$$

and we claim that the induced map

$$\theta \colon \mathbb{A}_F^\times \to \mathrm{Gal}^{\mathrm{ab}}(F)$$

is trivial when restricted to $F^\times$. This is an enormous generalization of quadratic reciprocity: if $F = \mathbb{Q}$, then for any quadratic extension $\mathbb{Q}(\ell)$, we have $\theta_v(\cdot) = (\cdot, \ell)_v$, i.e., the Hilbert symbol over F_v, for v a prime or ∞. However, here we assert that this is true for the entire abelianized Galois group, and not just this particular quotient, which is a copy of $\mathbb{Z}/2\mathbb{Z}$.

Proof (of Artin Reciprocity). First note that for any abelian extension E/F, we obtain a map $\theta \colon \mathbb{A}_F^\times \to \mathrm{Gal}(E/F)$; clearly, it suffices to show vanishing in each such quotient.

Case 1. Let $F := \mathbb{Q}$ and $E := \mathbb{Q}(\zeta_{\ell^r})$ for some prime ℓ. We must show that $\theta(p) = 1$ for every prime p, and $\theta(-1) = 1$, as these elements generate $\mathbb{Q}^\times$ and θ is a group homomorphism. We proceed by explicit calculation using Dwork's theorem.

First suppose $p \neq \ell$. Then

$$\begin{cases} \theta_q(p) = 1, \\ \theta_\infty(p) = 1 \\ \theta_p(p) = p, \\ \theta_\ell(p) = p^{-1}, \end{cases}$$

for $q \neq p, \ell$. For the first equality, note that the cyclotomic extension E/F is unramified at q as long as $q \neq \ell$, and the local Artin map kills every element of $(\mathbb{Z}/q\mathbb{Z})^\times$ for an unramified extension at q (see the proof of Claim 21.5). For the second equality, note that each θ_v factors through the decomposition group at v, which in this case is $\mathbb{Z}/2\mathbb{Z}$, and it is not hard to see explicitly that $\theta_\infty \colon \mathbb{R}^\times \to \mathbb{Z}/2\mathbb{Z}$ corresponds to the sign function. For the third equality, note that E/F is unramified at p because $p \neq \ell$. By Dwork's theorem, the uniformizer p maps to its Frobenius element in $\mathrm{Gal}(E/F) = (\mathbb{Z}/\ell^r\mathbb{Z})^\times$, which is just p. Finally, the extension E/F is totally ramified at ℓ, and $p \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, so Dwork's theorem gives $\theta_\ell(p) = p^{-1}$.

Now suppose $p = \ell$. Then

$$\begin{cases} \theta_q(\ell) = 1, \\ \theta_\infty(\ell) = 1 \\ \theta_\ell(\ell) = 1, \end{cases}$$

for $q \neq \ell$. The final equality is by Dwork's theorem, as ℓ acts trivially on the totally ramified factor of the extension (and as its Frobenius element on the unramified factor).

Finally, we check $\theta(-1)$:

$$\begin{cases} \theta_q(-1) = 1, \\ \theta_\infty(-1) = -1 \\ \theta_\ell(-1) = (-1)^{-1}, \end{cases}$$

for $q \neq \infty, \ell$. Since $-1 \in (\mathbb{Z}/\ell\mathbb{Z})^\times$, Dwork's theorem applies as before in the final case.

Case 2. Let $F := \mathbb{Q}$ as before and $E := \mathbb{Q}(\zeta_n)$, for any integer n. Then

$$n = \prod_{i=1}^{m} p_i^{r_i}$$

for primes p_i, and therefore

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{p_1^{r_1}}) \cdots \mathbb{Q}(\zeta_{p_m^{r_m}})$$

is the compositum over its prime-power factors, hence

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \prod_{i=1}^{m} \mathrm{Gal}(\mathbb{Q}(\zeta_{p_i^{r_i}})/\mathbb{Q}).$$

Then the Artin map

$$\theta \colon \mathbb{A}_\mathbb{Q}^\times \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

is given by the product over the Artin maps for $\mathbb{Q}(\zeta_{p_i^{r_i}})/\mathbb{Q}$ by LCFT, so it suffices to note the general claim that Artin reciprocity for linearly disjoint extensions implies Artin reciprocity for their compositum. That is, $\mathbb{Q}^\times$ is killed as each of its coordinates are killed by the previous case.

Case 3. Let F be a general number field, and $E := F(\zeta_n)$ for some integer n. By LCFT (at the level of multiplicative groups os local fields), we have the following commutative diagram:

$$\begin{array}{ccccc} F^\times & \hookrightarrow & \mathbb{A}_F^\times & \xrightarrow{\theta} & \mathrm{Gal}(F(\zeta_n)/F) \\ \downarrow{\scriptstyle \mathrm{N}} & & \downarrow{\scriptstyle \mathrm{N}} & & \downarrow \\ \mathbb{Q}^\times & \hookrightarrow & \mathbb{A}_\mathbb{Q}^\times & \xrightarrow{\theta} & \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}), \end{array}$$

where θ denotes the Artin map. Since the rightmost map is an injection, it suffices to show that $\mathrm{N}(F^\times) \subseteq \mathbb{Q}^\times$ vanishes in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, but this is just the previous case.

Case 4. Let E/F be a cyclotomic extension of number fields, i.e., $E \subseteq F(\zeta_n)$, for some n. Then by LCFT, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{A}_F & \xrightarrow{\theta} & \mathrm{Gal}(F(\zeta_n)/F) \\ & \searrow^{\theta} & \downarrow \\ & & \mathrm{Gal}(E/F), \end{array}$$

and since θ kills $F^\times$ in the upper Galois group, it also does so in the lower one.

We have established that Artin reciprocity holds for all cyclotomic extensions of number fields; for the general case, we'll use Brauer reciprocity, to which we now turn. □

As a note, Sam is likely the only person in the world to call it "Brauer reciprocity"; usually, it is referred to as "calculation of Brauer groups from GCFT" or the like.

Let E/F be a G-Galois extension of global fields. We have a short exact sequence of G-modules

$$1 \to E^\times \to \mathbb{A}_E^\times \to C_E \to 1,$$

giving a composition

$$\underbrace{\mathrm{Br}(F/E)}_{H^2(G,E^\times)} \to \underbrace{\bigoplus_v \mathrm{Br}(F_v/E_w)}_{H^2(G,\mathbb{A}_E^\times)} \hookrightarrow \bigoplus_v \mathrm{Br}(F_v) \xrightarrow{(x_v)_{v\in M_F} \mapsto \sum_{v\in M_F\setminus M_F^\infty} x_v} \mathbb{Q}/\mathbb{Z},$$

where we recall that $\mathrm{Br}(F/E)$ denotes the group of division algebras over F that become matrix algebras when tensored with E; w is some choice of place lying over v; we recall that

$$\mathrm{Br}(F_v) = \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } v \text{ is finite,} \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{if } v \text{ is real,} \\ 0 & \text{if } v \text{ is complex;} \end{cases}$$

and the rightmost map is referred to as the "invariants" map, as it is a sum over the "local invariants," which classify local division algebras. This composition corresponds to tensoring central simple algebras over division algebras over local places, taking the invariants at each such place, and adding them up. The direct sum tells us (automatically) that we obtain a matrix algebra over a field at all but finitely many places. Brauer reciprocity states that this composition is zero. So for instance, there is no central simple algebra over $\mathbb{Q}$, or any number field, with the property that it is a matrix algebra (splits) over a field at all places but one. Note that in the case when this composition is applied to a Hamiltonian algebra (associated to two rational numbers), then this simply records the Hilbert reciprocity law.

CLAIM 22.1. *Let E/F be a cyclic extension of global fields. Then Artin reciprocity is equivalent to Brauer reciprocity.*

PROOF. Choosing some generator, we have $\mathrm{Gal}(E/F) = G \simeq \mathbb{Z}/n\mathbb{Z}$. Since G is cyclic, it is its own abelianization and Tate cohomology is 2-periodic, so we have the following commutative diagram:

$$\begin{array}{ccccc} \hat{H}^0(G,E^\times) = F^\times/\mathrm{N}(E^\times) & \longrightarrow & \hat{H}^0(G,\mathbb{A}_E^\times) = \mathbb{A}_F^\times/\mathrm{N}(\mathbb{A}_E^\times) & \xrightarrow{\theta} & G = \frac{1}{n}\mathbb{Z}/\mathbb{Z} \\ \| & & \| & & \downarrow \\ \mathrm{Br}(F/E) = \hat{H}^2(G,E^\times) & \longrightarrow & \hat{H}^2(G,\mathbb{A}_E^\times) & \xrightarrow{\iota} & \mathbb{Q}/\mathbb{Z}, \end{array}$$

where ι denotes the invariants map. Now, the left-hand square commutes trivially, and the right-hand square commutes by LCFT for cyclic extensions. The claim then follows by an easy diagram chase. □

CLAIM 22.2. *For any global field F and every $\beta \in \mathrm{Br}(F)$, there exists a cyclic cyclotomic extension E/F such that $\beta \in \mathrm{Br}(F/E)$, that is, β also lies in the relative Brauer group.*

Let us assume this claim for the moment. Then we can deduce the Brauer reciprocity law in general: since the extension E/F is cyclic, we know that Brauer reciprocity is equivalent to Brauer reciprocity, and moreover, we know Artin reciprocity holds as it is cyclotomic.

This claim is easy to check for local fields: given a division algebra over a local field K, then it is split over a field L/K if the square root of its degree divides $[L : K]$. Indeed, recall that if $\beta \subseteq \frac{1}{n}\mathbb{Z}/\mathbb{Z} \subseteq \mathrm{Br}(K)$, i.e., β is a degree-n^2 division algebra, then $\beta \in \mathrm{Br}(K/L)$ if and only if $n \mid [L : K]$ because

$$\mathbb{Q}/\mathbb{Z} = \mathrm{Br}(K) \xrightarrow{\times[L:K]} \mathrm{Br}(L) = \mathbb{Q}/\mathbb{Z}.$$

Recall now the following theorem, which we will prove in the next lecture:

THEOREM 22.3. *For all extensions E/F of global fields, $H^1(G, C_E) = 0$.*

This is a sort of analog of Hilbert's Theorem 90, and proving this is the hardest part of GCFT; we'll assume it for now. The short exact sequence

$$1 \to E^\times \to \mathbb{A}_E^\times \to C_E \to 1$$

then gives an exact sequence

$$\underbrace{H^1(\mathbb{A}_E^\times)}_{0} \to \underbrace{H^1(C_E)}_{0} \to H^2(E) = \mathrm{Br}(F/E) \to H^2(\mathbb{A}_E^\times) = \bigoplus_v \mathrm{Br}(F_v/E_w)$$

where the vanishing is by the previous theorem and Hilbert's Theorem 90 (as the cohomology of the adèles is simply a direct sum over local cohomologies). Passing to direct limits, we obtain the following corollary:

COROLLARY 22.4. *For any global field F, there is a canonical injection*

$$\mathrm{Br}(F) \hookrightarrow \bigoplus_{v \in M_F} \mathrm{Br}(F_v).$$

In other words, any central simple algebra over a number field F is a matrix algebra if and only if it is a matrix algebra at each completion of F. This is definitely not an obvious statement!

The upshot is that, to prove Claim 22.2, it suffices to show the following:

CLAIM 22.5. *Given a finite set of places S of a global field F, and positive integers m_v for all $v \in S$ (such that $m_v = 1$ is v is complex, $m_v = 1, 2$ if v is real, and m_v is arbitrary if v is finite), then there exists a cyclic cyclotomic extension E/F such that E_w/F_v has degree divisible by m_v (for any choice of $w \mid v$).*

PROOF (CLAIM 22.5 $\implies$ CLAIM 22.2). By Corollary 22.4, a central simple algebra over F splits if and only if it splits at every local field F_v, which is true if and only if the square root of its degree divides $[E_w : F_v]$ for some extension E/F and place $w \mid v$. Thus, choosing m_v to be the square root of its degree over F_v for each place v (alternatively, the denominator of its local invariant at v), which will necessarily be 1 or 2 if v is real and 1 if v is complex, this claim implies that our CSA splits over the extension E that it provides. Moreover, as noted previously, such a CSA will split over F_v for all but finitely many places v, which implies that we may take S to be the set of only those places at which our CSA does not split. □

Before beginning the proof, let us take a moment to note that there certainly exist cyclotomic extensions which are not cyclic! Indeed, we have $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, where ζ_n is a primitive nth root of unity, so for instance, if $n = 15$, then

$$(\mathbb{Z}/15\mathbb{Z})^\times \simeq (\mathbb{Z}/3\mathbb{Z})^\times \times (\mathbb{Z}/5\mathbb{Z})^\times \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

is not cyclic!

Proof (of Claim 22.5). First note that we may assume $F = \mathbb{Q}$, as we may replace each local factor m_v by $[F_v : \mathbb{Q}_p] \cdot m_v$ (where p is the place of $\mathbb{Q}$ lying below v), apply the claim over $\mathbb{Q}$, and then replace E by the compositum $E \cdot F$, which is also a cyclic cyclotomic extension of F (as subgroups of cyclic groups are cyclic).

Case 1. Suppose that, for every local place $v \in S$, we have $m_v = p^{r_v}$ for some odd prime p (independent of v). For any r, we have a cyclotomic extension $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ with Galois group $(\mathbb{Z}/p^r\mathbb{Z})^\times$. Note that $\#(\mathbb{Z}/p^r\mathbb{Z})^\times = (p-1)p^{r-1}$, so we may let $\mathbb{Q}(\zeta_{p^r})/E_r/\mathbb{Q}$ be a cyclic subextension with $\mathrm{Gal}(E_r/\mathbb{Q}) \simeq \mathbb{Z}/p^{r-1}\mathbb{Z}$. Then for each $v \in S$ and any choice of $w \mid v$, we claim that $[E_{r,w} : \mathbb{Q}_v] \to \infty$ as $r \to \infty$. Indeed, any local field aside from $\mathbb{C}$ only contains finitely many roots of unity, so these extensions must be increasing in degree. Now, $[E_{r,w} : \mathbb{Q}_v] = [\mathbb{Q}_v(\zeta_{p^r}/\mathbb{Q}_v] \mid (p-1)p^\infty$, hence the p-power factor of this degree diverges, proving the claim in this case as S is finite. Let us note that these extensions are totally complex (i.e., every infinite place is complex), so we need not worry about real places v for which $m_v = 2$.

Case 2. Now suppose that $m_v = 2^{r_v}$ for each $v \in S$. This case is similar, aside from the fact that $(\mathbb{Z}/2^r\mathbb{Z})^\times \simeq \mathbb{Z}/2^{r-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, where this isomorphism may be obtained by checking the easy identity

$$\mathbb{Z}/2^{r-2}\mathbb{Z} \simeq \{x \in (\mathbb{Z}/2^r\mathbb{Z})^\times : x \equiv 1 \bmod 4\}$$

(so show that it is cyclic by computing its 2-torsion and then verifying that it contains only 2 elements, etc.) and noting that $\mathbb{Z}/2\mathbb{Z} \simeq \{1, 2^{r-1} - 1\}$. Then we may let $\mathbb{Q}(\zeta_{2^r})/E_r/\mathbb{Q}$ be a cyclotomic degree-2^{r-2} extension whose Galois group is $(\mathbb{Z}/2^{r-2}\mathbb{Z})^\times$, realized as a quotient of $(\mathbb{Z}/2^r\mathbb{Z})^\times$.

We claim that $E_r/\mathbb{Q}$ is a totally complex extension. Since it is an abelian extension, it suffices to show that complex conjugation, which corresponds to $-1 \in (\mathbb{Z}/2^r\mathbb{Z})^\times$, acts on it non-trivially. For sufficiently large r, $-1 \not\equiv 1 \bmod 4$, hence its projection to $(\mathbb{Z}/2^{r-2}\mathbb{Z})^\times$ is given by $1 - 2^{r-1} \neq 1$ via the explicit isomorphism above (note $2^{r-1} - 1 \equiv 3 \bmod 4$ is the only nontrivial element of either factor with this property). Thus, the extension $E_r/\mathbb{Q}$ suffices by an argument similar to that in the previous case.

Case 3. Finally, for the general case, take the compositum over all prime factors of the m_v's of the extensions we constructed in the previous two cases. Moreover, no "interference" can occur (causing the compositum not to be cyclic) as the Galois group of each extension has distinct prime-power order. □

Thus, assuming our analog of Hilbert's Theorem 90, every element of the Brauer group of a global field F is split by a cyclic cyclotomic extension, which implies Brauer reciprocity for all elements of $\mathrm{Br}(F)$. This implies Artin reciprocity for cyclic extensions, because the two reciprocity laws are equivalent for cyclic extensions. Finally, since any abelian group is a product of cyclic groups, every abelian extension E/F is the compositum of cyclic extensions, implying Artin reciprocity in general (we've already seen that Artin reciprocity for a set of linearly disjoint extensions implies that it holds for their compositum).

LECTURE 23

Proof of the Second Inequality

Our goal for this lecture is to prove the "second inequality": that for all extensions E/F of global fields, we have $H^1(G, C_E) = 0$, where $C_E := \mathbb{A}_E^\times / E^\times$ is the "idèle class group" of E. Our main case is when E/F is cyclic of order p, and $\zeta_p \in F$ for some primitive pth root of unity ζ_p, and we will reduce to this case at the end of the lecture (note that $\mathrm{char}(F) = 0$ as we are assuming that F is a number field). In this case, it suffices to show that

$$\#\hat{H}^0(C_E) = \#(C_F/\mathrm{N}C_E) = \#(\mathbb{A}_F^\times / F^\times \cdot \mathrm{N}(\mathbb{A}_E^\times)) \leq p.$$

Indeed, by the "first inequality," we know that

$$\frac{\#\hat{H}^0(C_E)}{\#\hat{H}^1(C_E)} = p,$$

hence $p \cdot \#\hat{H}^1(C_E) = \#\hat{H}^0(C_E) \leq p$ implies $\#H^1(C_E) = 1$, as desired. Our approach will be one of "trial and error"—that is, we'll try something, which won't quite be good enough, and then we'll correct it.

Fix, once and for all, a finite set S of places of F such that

(1) if $v \mid \infty$, then $v \in S$;
(2) if $v \mid p$, then $v \in S$;
(3) $\mathbb{A}_F^\times = F^\times \cdot \mathbb{A}_{F,S}^\times$, where we recall that
$$\mathbb{A}_{F,S}^\times := \prod_{v \in S} F_v^\times \times \prod_{v \notin S} \mathcal{O}_{F_v}^\times$$
and that this is possible by Lemma 20.12;
(4) $E = F(\sqrt[p]{u})$, for some $u \in \mathcal{O}_{F,S}^\times := F^\times \cap \mathbb{A}_{F,S}^\times$ are the "S-units" of F. This is possible by Kummer Theory.

Note that this last condition implies that E is unramified outside of S, as u is an integral element in any place $v \notin S$, and since p is prime to the order of the residue field of F_v as all places dividing p are in S by assumption, $F_v(\sqrt[p]{u})/F_v$ is an unramified extension.

An important claim, to be proved later in a slightly more refined form, is the following:

Claim 23.1. *$u \in \mathcal{O}_{F,S}^\times$ is a pth power if and only if its image in $F_v^\times$ is a pth power for each $v \in S$.*

Let

$$\Gamma := \prod_{v \in S} (F_v^\times)^p \times \prod_{v \notin S} \mathcal{O}_{F_v}^\times \subseteq \mathbb{A}_{F,S}^\times.$$

Then we have the following claims:

Claim 23.2. $\mathcal{O}_{F,S}^\times \cap \Gamma = (\mathcal{O}_{F,S}^\times)^p$.

PROOF. This follows trivially from the previous claim. □

CLAIM 23.3. $\Gamma \subseteq \mathrm{N}(\mathbb{A}_E^\times)$.

PROOF. The extension E/F is unramified at each $v \notin S$, hence the factor $\prod_{v \notin S} \mathcal{O}_{F_v}^\times \subseteq \mathrm{N}(\mathbb{A}_E^\times)$. Since p kills $\hat{H}^0(E_w^\times)$, for a choice of $w \mid v$, it follows that the factor $\prod_{v \in S}(F_v^\times)^p \subseteq \mathrm{N}(\mathbb{A}_E^\times)$ as well. □

Thus,

$$\#(\mathbb{A}_F^\times/F^\times \cdot \mathrm{N}(\mathbb{A}_E^\times)) \leq \#(\mathbb{A}_F^\times/F^\times \cdot \Gamma),$$

and we have a short exact sequence

$$1 \to \mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times \cap \Gamma) \to \mathbb{A}_{F,S}^\times/\Gamma \to \mathbb{A}_F^\times/(F^\times \cdot \Gamma) \to 1.$$

Indeed, the third map is surjective by property (3) of S above, the second map is injective as $\mathcal{O}_{F,S}^\times \subseteq F^\times$, and exactness at $\mathbb{A}_{F,S}^\times/\Gamma$ holds by definition. Thus,

$$\#(\mathbb{A}_F^\times/F^\times \cdot \Gamma) = \frac{\#(\mathbb{A}_{F,S}^\times/\Gamma)}{\#(\mathcal{O}_{F,S}^\times/\mathcal{O}_{F,S}^\times \cap \Gamma)},$$

and it remains to compute both the numerator and denominator of this expression. We have

$$\mathbb{A}_{F,S}^\times/\Gamma = \prod_{p \in S} F_v^\times/(F_v^\times)^p,$$

and we recall from (6.3) that

$$\#(F_v^\times/(F_v^\times)^p) = \frac{p \cdot \#\mu_p(F_v)}{|p|_v} = \frac{p^2}{|p|_v}$$

as $\zeta_p \in F$ by assumption. Thus,

$$\prod_{v \in S} \frac{p^2}{|p|_v} = p^{2 \cdot \#S}$$

by the product rule, as $|p|_v = 1$ for $v \notin S$ by assumption. Now we'd like to compute

$$\#(\mathcal{O}_{F,S}^\times/\mathcal{O}_{F,S}^\times \cap \Gamma) = \#(\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^p).$$

Recall that, by the S-unit theorem,

$$\mathcal{O}_{F,S}^\times \simeq \mathbb{Z}^{\#S-1} \times (\mathcal{O}_{F,S}^\times)_{\mathrm{tors}}.$$

The latter is cyclic, and has order divisible by p, hence

$$\#(\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^p) = p^{\#S-1} \cdot p = p^{\#S}.$$

Combining these two results, we obtain

$$\#\hat{H}^0(C_E) \leq \frac{p^{2 \cdot \#S}}{p^{\#S}} = p^{\#S},$$

which is unfortunately not good enough.

Here is how we will improve on this result:

CLAIM 23.4. *Given such a set $S \subseteq M_F$, there exists a set $T \subseteq M_F$ such that*

(1) $\#T = \#S - 1$;
(2) $S \cap T = \varnothing$;
(3) every $v \in T$ is split in E, i.e., $E_w = F_v$ for all $w \mid v$;

(4) *any* $u \in \mathcal{O}_{F,S\cup T}^\times$ *is a pth power if and only if* $u \in F_v^\times$ *is a pth power for all* $v \in S$.

Note the key difference here from earlier: in property (4), we do not require that $u \in (F_v^\times)^p$ for all $v \in S \cup T$, merely for all $v \in S$. Given such a T, we redefine Γ by

$$\Gamma := \prod_{v\in S}(F_v^\times)^p \times \prod_{v\in T} F_v^\times \times \prod_{v\notin S\cup T} \mathcal{O}_{F_v^\times}.$$

Claim 23.5. $\Gamma \subseteq \mathrm{N}(\mathbb{A}_E^\times)$.

Proof. Property (3) implies the claim for the second factor; the first and third follow as before. □

Redoing our calculations with $\mathbb{A}_{F,S\cup T}^\times$ instead of $\mathbb{A}_{F,S}^\times$, we obtain

$$\#(\mathbb{A}_{F,S\cup T}^\times/\Gamma) = p^{2\cdot\#S}$$

as before by property (4), and

$$\#(\mathcal{O}_{F,S\cup T}^\times/(\mathcal{O}_{F,S\cup T}^\times \cap \Gamma)) = p^{\#(S\cup T)} = p^{2\cdot\#S-1},$$

again as before, hence their quotient is p, as desired! Thus, it suffices to prove the claim above.

Claim 23.6. *For any abelian extension* F'/F *of global fields, the Frobenius elements for* $v \notin S$ *generate* $\mathrm{Gal}(F'/F)$.

We'd like to prove this purely algebraically, without the Chebotarev density theorem (which, anyhow, gives a slightly different statement).

Proof. Let H be the subgroup generated by all Frobenii for $v \notin S$, and let $F'' := (F')^H$ be the fixed field. We'd like to show that $F'' = F$. Note that Frob_v is trivial in $\mathrm{Gal}(F'/F)/H = \mathrm{Gal}(F''/F)$ for all $v \notin S$, hence every $v \notin S$ splits in F''/F (as they are unramified by assumption). Thus, $F_w'' = F_v$ for all $w \mid v$ and $v \notin S$, and we claim that this is impossible.

We may assume that F''/F is a degree-n cyclic extension (replacing it by a smaller extension if necessary). By the first inequality, $\chi(C_{F''}) = n$, which gives

$$\#(\mathbb{A}_F^\times/\mathrm{N}(\mathbb{A}_{F''}^\times)\cdot F^\times) = \#\hat{H}^0(C_{F''}) \geq n.$$

But because this extension is split for all $v \notin S$, we have $\mathrm{N}((F_v'')^\times) = F_v^\times$ trivially, and therefore $\prod_{v\notin S} F_v^\times \subseteq \mathrm{N}(\mathbb{A}_{F''}^\times)$, where this is the restricted direct product. Strong approximation then gives that $F^\times \cdot \prod_{v\notin S} F_v^\times$ is dense in $\mathbb{A}_F^\times$, and since it is also open, this is a contradiction unless $n = 1$, as desired. □

We'd like to apply this claim for $F' := F(\{\sqrt[p]{u} : u \in \mathcal{O}_{F,S}^\times\})$. First, a claim:

Claim 23.7. $\mathrm{Gal}(F'/F) = (\mathbb{Z}/p\mathbb{Z})^{\#S}$, *for* F' *as above.*

Proof. This is, in essence, Kummer theory, as $\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^p \subseteq F^\times/(F^\times)^p$. We know that all exponent-p extensions of F are given by adjoining pth roots of elements of $F^\times$. The Galois group must be a product of copies of $\mathbb{Z}/p\mathbb{Z}$, but some of these subgroups may coincide—iterated application of Kummer theory gives the statement. □

Now, we have $F'/E/F$, as E/F was assumed to be obtained by adjoining the pth root of some S-unit. Choose places $w_1, \dots, w_{\#S-1}$ of E that do not divide any places of S, whose Frobenii give a basis for $\mathrm{Gal}(F'/E) \simeq (\mathbb{Z}/p\mathbb{Z})^{\#S-1}$, which is possible by the argument of Claim 23.6. Then let $T := \{v_1, \dots, v_{\#S-1}\}$ be the restrictions of the w_i to F.

Claim 23.8. *Each $v \in T$ is split in E.*

Proof. Since $\mathrm{Frob}_v \in \mathrm{Gal}(F'/E)$, it acts trivially on E, so $\mathrm{Gal}(E_w/F_v)$ is trivial for any $w \mid v$, as desired. □

This establishes condition (3) for T; it remains to show condition (4), as conditions (1) and (2) are implicit in the construction of T.

Claim 23.9. *An element $x \in \mathcal{O}_{F,S\cup T}^\times$ is a pth power if and only if $x \in (F_v^\times)^p$ for every $v \in S$.*

Proof. **Step 1.** We claim that

$$\mathcal{O}_{F,S}^\times \cap (E^\times)^p = \{x \in \mathcal{O}_{F,S}^\times : x \in (F_v^\times)^p \text{ for all } v \in T\}.$$

The forward inclusion is trivial as $(F_v^\times)^p = (E_w^\times)^p$ by the previous claim. For the converse, note that for any $x \in \mathcal{O}_{F,S}^\times$, we have an extension $F'/E(\sqrt[p]{x})/E$. If $x \in (E_w^\times)^p$ for each $w \mid v$ and $v \in T$, then this extension is split at w, so Frob_w acts trivially on $E(\sqrt[p]{x})$, hence $\mathrm{Gal}(F'/E)$ acts trivially on $E(\sqrt[p]{x})$ as it is generated by these Frobenii, hence $E(\sqrt[p]{x}) = E$ and $x \in (E^\times)^p$ as desired.

Step 2. Now we claim that the canonical map

$$\mathcal{O}_{F,S}^\times \xrightarrow{\varphi} \prod_{v\in T} \mathcal{O}_{F_v}^\times/(\mathcal{O}_{F_v}^\times)^p$$

is surjective. This is the step that really establishes the limit on the size of T from which the second inequality falls out perfectly. We will proceed by computing the orders of both sides. By Step 1, we have

$$\mathrm{Ker}(\varphi) = \{x \in \mathcal{O}_{F,S}^\times : x \in (E^\times)^p\}.$$

Then $\mathcal{O}_{F,S}^\times/\mathrm{Ker}(\varphi)$ has order $p^{\#S-1}$. Indeed, we computed earlier that $\mathcal{O}_{F,S}^\times/(\mathcal{O}_{F,S}^\times)^p$ has order $p^{\#S}$, and since

$$(\mathcal{O}_{F,S}^\times)^p = \{x \in \mathcal{O}_{F,S}^\times : x \in (F^\times)^p\}$$

and E/F is a degree-p extension obtained by adjoining the pth root of some S-unit, it follows that $[\mathrm{Ker}(\varphi) : (\mathcal{O}_{F,S}^\times)^p] = p$. Now, using the version of our earlier formula for $\mathcal{O}_{F_v}^\times$ (rather than $F_v^\times$), the right-hand side has order

$$\prod_{v\in T} \frac{\#\mu_p(F_v)}{|p|_v} = p^{\#T} = p^{\#S-1},$$

so the map is indeed surjective.

Step 3. We'd now like to establish the claim: that if $x \in (F_v^\times)^p$ for all $v \in S$, then $x \in (\mathcal{O}_{F,S\cup T}^\times)^p$ (the converse is trivial). We'd like to show that $F(\sqrt[p]{x}) = F$. Set

$$\Gamma := \prod_{v\in S} F_v^\times \times \prod_{v\in T} (\mathcal{O}_{F_v}^\times)^p \times \prod_{v\notin S\cup T} \mathcal{O}_{F_v}^\times \subseteq \mathbb{A}_{F,S}^\times,$$

where this is again a different Γ from earlier. Then in fact,

$$\Gamma \subseteq \mathrm{N}(\mathbb{A}^\times_{F(\sqrt[p]{x})}) \subseteq \mathbb{A}^\times_F,$$

where the third term is because $F(\sqrt[p]{x})/F$ is unramified outside of $S \cup T$, the second because $[F(\sqrt[p]{x}) : F] \leq p$, and the first because the extension is split at all places of S by assumption. Now, we want to show that $F^\times \cdot \Gamma = \mathbb{A}^\times_F$, because the first inequality then implies the result as in Claim 23.6. By Step 2, we have

$$\mathcal{O}^\times_{F,S} \twoheadrightarrow \prod_{v \in T} \mathcal{O}^\times_{F_v}/(\mathcal{O}^\times_{F_v})^p = \mathbb{A}^\times_{F,S}/\Gamma,$$

hence $\mathcal{O}^\times_{F,S} \cdot \Gamma = \mathbb{A}^\times_{F,S}$. This implies that

$$F^\times \cdot \Gamma = F^\times \cdot \mathbb{A}^\times_{F,S} = \mathbb{A}^\times_F$$

by assumption on S. □

Now we'd like to infer the general case of the second inequality from the specific case proven above. The first step is as follows:

Claim 23.10. *If the second inequality holds for any cyclic order-p extension for which the base field contains a pth root of unity, then it holds for any cyclic order-p extension.*

Proof. Let E/F be a degree-p cyclic extension of global fields. Recall that the second inequality for E/F is equivalent to the existence of a canonical injection

$$\mathrm{Br}(F/E) \hookrightarrow \bigoplus_{v \in M_F} \mathrm{Br}(F_v).$$

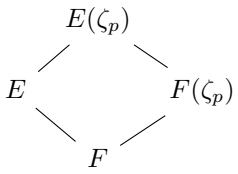
Indeed, we have an short exact sequence

$$0 \to E^\times \to \mathbb{A}^\times_E \to C_E \to 0,$$

and the long exact sequence on cohomology then gives

$$\underbrace{H^1(G, \mathbb{A}^\times_E)}_{\bigoplus H^1(E^\times_w)=0} \to H^1(G, C_E) \to \mathrm{Br}(F/E) \to \bigoplus_v \mathrm{Br}(F_v/E_w) \subseteq \bigoplus_v \mathrm{Br}(F_v)$$

for some choice of $w \mid v$, where the first equality is by Hilbert's Theorem 90. In order to show the vanishing of $H^1(G, C_E)$, it suffices to show that the final map is injective. Now, the field extensions



induce a commutative diagram

$$\begin{array}{ccc} \mathrm{Br}(F/E) & \xrightarrow{\alpha} & \bigoplus_v \mathrm{Br}(F_v/E_w) \\ \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} \\ \mathrm{Br}(F(\zeta_p)/E(\zeta_p)) & \xrightarrow{\beta} & \bigoplus_v \mathrm{Br}(F(\zeta_p)_w) \\ \downarrow & & \\ \mathrm{Br}(F/E), & & \end{array} \qquad \times[F(\zeta_p):F]$$

where the left-most maps are the restriction and inflation maps on cohomology, respectively, using the cohomological interpretation of the Brauer group (see Problem 2 of Problem Set 7). Moreover, the composition is injective on $\mathrm{Br}(F/E)$, as it is p-torsion (by Problem 2(c)), and $[F(\zeta_p) : F] \mid (p-1)$. Thus, γ is injective as well. Since the second equality holds for $E(\zeta_p)/F(\zeta_p)$ by assumption, β is injective, hence α is injective as well. □

Claim 23.11. *If the second inequality holds for any cyclic order-p extension of number fields, then it holds for any extension.*

Proof. We'd like to show that $H^1(G, C_E) = 0$. As for any Tate cohomology group of a finite group, we have an injection

$$H^1(G, C_E) \hookrightarrow \bigoplus_p H^1(G_p, C_E),$$

where G_p is the p-Sylow subgroup of G. Thus, we may assume that G is a p-group. Since every p-group G contains a normal subgroup H isomorphic to $\mathbb{Z}/p\mathbb{Z}$, we may assume that we have field extensions $E_2/E_1/F$, where $\mathrm{Gal}(E_2/E_1) \simeq H$ and $\mathrm{Gal}(E_1/F) \simeq G/H$. We may assume that the theorem holds for H acting on E_2 and G/H acting on E_1, so we may simply repeat the sort of argument showing injectivity on Brauer groups in the proof of the previous claim.

First, we claim that $C_{E_2}^H = C_{E_1}$. Indeed, we have a short exact sequence

$$0 \to E_2^\times \to \mathbb{A}_{E_2}^\times \to C_{E_2} \to 0,$$

and the long exact sequence on cohomology then gives

$$0 \to \underbrace{H^0(H, E_2^\times)}_{E_1^\times} \to \underbrace{H^0(H, \mathbb{A}_{E_2}^\times)}_{\mathbb{A}_{E_1}^\times} \to \underbrace{H^0(H, C_{E_2})}_{C_{E_2}^H} \to \underbrace{H^1(H, E_2^\times)}_{0}$$

by Hilbert's theorem 90. Note that $\mathbb{A}_{E_2}^{\times,H} = \mathbb{A}_{E_1}^\times$ as taking invariants by a finite group commutes with direct limits and products in the definition of the adéles.

Then we have

$$\mathrm{hKer}\left(C_{E_2}^{\mathrm{h}G} = (C_{E_2}^{\mathrm{h}H})^{\mathrm{h}G/H} \to (\tau^{\geq 2} C_{E_2}^{\mathrm{h}H})^{\mathrm{h}G/H}\right) \simeq \left(\tau^{\leq 0} C_{E_2}^{\mathrm{h}H}\right)^{\mathrm{h}G/H} = (C_{E_1})^{\mathrm{h}G/H},$$

where the first equality is by Problem 3 of Problem Set 6, the map follows by definition of truncation, the quasi-isomorphism is because $H^1(H, C_{E_2})$ vanishes by assumption, and finally, the second expression is simply the naive H-invariants of C_{E_2}, as the truncation kills all cohomologies in degrees greater than 0, so the

previous claim gives the equality. The long exact sequence on cohomology then gives

$$\underbrace{H^1\big((C_{E_1})^{\mathrm{h}G/H}\big)}_{H^1(G/H,C_{E_1})=0} \to \underbrace{H^1\big((C_{E_2})^{\mathrm{h}G}\big)}_{H^1(G,C_{E_2})} \to \underbrace{H^1\big((\tau^{\geq 2}C_{E_2}^{\mathrm{h}H})^{\mathrm{h}G/H}\big)}_{0}$$

as the rightmost complex is in degrees at least 2. Thus, $H^1(G, C_{E_2}) = 0$, as desired. □

Index

[1]Note that for brevity's sake we have abbreviated "(Problem m of) Problem Set n" to "PS-n($.m$)" in this index.

Index of Notation

(a, b)	the Hilbert symbol, page 6
$(a, b)_p$	the p-adic Hilbert symbol, page 15
$A \xrightarrow{\sim} B$	indicates an isomorphism between two objects
$\mathbb{A}_F$	the ring of adèles of a number field, page 3
$\mathbb{A}_F^\times$	the group of idèles of a number field, page 3
$\mathbb{A}_{F,S}$	the ring of S-adèles of a number field F for a set of places S, page 89
$\mathbb{A}_{F,S}^\times$	the group of S-idèles of a number field F for a set of places S, page 89
A^G	the invariants of a G-module, page 29
A_G	the coinvariants of a G-module, page 45
A^{op}	the opposite of a central simple algebra, page 83
$\mathrm{Aut}(A)$	the automorphism group of an object
$\mathrm{Aut}_{\mathrm{cts}}(A)$	the continuous automorphisms of a topological object
$\mathrm{Bar}_A(B)$	the bar complex associated to an A-algebra B, page 55
$\mathrm{Br}^{\mathrm{coh}}(K)$	the cohomological Brauer group of a field, page 81
$\mathrm{Br}^{\mathrm{coh}}(K/L)$	the cohomological Brauer group of a field extension, page 81
$\mathrm{Br}^{\mathrm{csa}}(K)$	the central simple algebra Brauer group of a field, page 82
$\mathrm{Br}^{\mathrm{csa}}(K/L)$	the central simple algebra Brauer group of a field extension, page 83
C_F	the idèle class group of a number field, page 87
CFT	class field theory
$\mathrm{char}(K)$	the characteristic of a field
$\mathrm{Cl}(F)$	the ideal class group of a number field, PS-2.1(b)[2]
$\mathrm{Coker}(f)$	the cokernel of a map, page 12
$\mathrm{Cone}(f)$	the cone of a map of chain complexes, page 42
CSA	central simple algebra, page 82
cts	continuous
δ	the boundary map in a long exact sequence
d	a differential in a chain complex, page 24
d^i	the ith differential in a chain complex, page 24
$\dim_K V$	the dimension of a K-vector space
DVR	discrete valuation ring
ϵ	the augmentation map $\mathbb{Z}[G] \to \mathbb{Z}$, page 53
ϵ	the map $\mathbb{Z}_2^\times \to \mathbb{Z}/2\mathbb{Z}$ defined by $\epsilon(a) = 0$ if $a \in 1 + 4\mathbb{Z}_2$ and $\epsilon(a) = 1$ if $a \in 3 + 4\mathbb{Z}_2$, PS-1.2(c)
$\mathrm{End}(A)$	the endomorphism ring of an object

[2] As in the index, we have abbreviated "(Problem m of) Problem Set n" to "PS-n(.m)" throughout.

$\underline{\mathrm{Ext}}^i(X,Y)$	the ith Ext-group of two chain complexes, page 51
$\overline{F}$	the algebraic closure of a field
$f \simeq g$	indicates that maps f and g of chain complexes are homotopic, page 41
$F_n A$	the nth group of a filtration on an abelian group, page 8
$\mathbb{F}_q$	the finite field with q elements
Frob	the frobenius automorphism of a finite field
Frob_q	the Frobenius element associated to an unramified prime
F_v	the completion of a field F with respect to a place v
$[g]$	the element in $R[G]$ corresponding to $g \in G$, page 32
$\widehat{G}$	the profinite completion of a group, page 2
G^{ab}	the abelianization of a group
$\mathrm{Gal}(K)$	the absolute Galois group of a field, page 2
$\mathrm{Gal}_2(K)$	the quotient of $\mathrm{Gal}^{\mathrm{ab}}(K)$ by all squares, page 4
$\mathrm{Gal}^{\mathrm{ab}}(K)$	the abelianized absolute Galois group of a field, page 2
GCFT	global class field theory
$\mathrm{Gr}_n A$	the nth associated graded term of a filtration, page 8
$G_{\chi,\psi}$	the Gauss sum of two multiplicative characters, page 17
$\hat{H}^0(G,A)$	the first Tate cohomology group of a G-module, page 27
$\hat{H}^1(G,A)$	the second Tate cohomology group of a G-module, page 27
$\mathbb{H}$	the Hamiltonians over $\mathbb{R}$
$H_{a,b}$	the Hamiltonian (or quaternion) algebra with respect to two field elements, PS-1.5
$\mathrm{hCoker}(f)$	the homotopy cokernel of a map of chain complexes, page 42
$H \lhd G$	indicates that H is a normal subgroup of G
$\hat{H}^i(G,X)$	the ith Tate cohomology group of a chain complex, page 61
$H^i(G,X)$	the ith group cohomology group of a chain complex, page 62
$H_i(G,X)$	the ith group homology group of a chain complex, page 60
$H^i(X)$	the ith cohomology group of a chain complex, page 40
$\mathrm{hKer}(f)$	the homotopy kernel of a map of chain complexes, page 44
$\mathrm{holim}_i X_i$	the homotopy limit of an inverse system of complexes, PS-6.6
$\underline{\mathrm{Hom}}(X,Y)$	the mapping complex of two chain complexes, page 47
$\mathrm{Hom}_{\mathrm{cts}}(A,B)$	the continuous homomorphisms between two topological objects
$\underline{\mathrm{Hom}}^{\mathrm{der}}(X,Y)$	the derived mapping complex of two chain complexes, page 49
I_G	the augmentation ideal in $\mathbb{Z}[G]$, page 58
$\mathrm{Im}(f)$	the image of a map
$K((t))$	the field of Laurent series over a field
$K_1 \cdot K_2$	the compositum of two fields
K^{ab}	the maximal abelian extension of a field, page 2
$\mathrm{Ker}(f)$	the kernel of a map
K^{sep}	the separable closure of a field
K^{unr}	the completion of the maximal unramified extension of a local field, page 65
LCFT	local class field theory
$\Lambda^d V$	the dth exterior power of a vector space
$\mathrm{M}_n(K)$	the $n \times n$ matrix algebra over a field
μ_n	the group of nth roots of unity
$M[n]$	the n-torsion of an abelian group, page 23

Bibliography

[Boy07] Dmitriy Boyarchenko, *Topics in Algebra*, 2007.

[Dwo58] Bernard Dwork, *Norm residue symbol in local number fields*, Abh. Math. Semin. Univ. Hambg. **22**(1) (December 1958), 180–190.

[Mil13] J.S. Milne, *Class Field Theory*, 2013.

[Ser73] Jean-Pierre Serre, *A Course in Arithmetic*, Springer Science & Business Media New York, 1973.

[Ser79] ———, *Local Fields*, Springer Science & Business Media New York, 1979.

[Wei74] André Weil, *Basic Number Theory*, Springer-Verlag Berlin Heidelberg, 1974.