Math 223a : Algebraic Number Theory notes

Alison Miller

Contents

1 September 7: Global class field theory **4**
1.1 Class fields 4
1.2 $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ and inverse limits 5

2 September 10 **6**
2.1 Frobenius elements; working towards the Artin map 6
2.2 More on $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$, adeles, and the Artin map 7
2.3 Adeles over a general number field 9
2.4 The Artin map and class field theory over a general number field 9

3 September 14 **10**
3.1 A bit more on the global Artin map 10
3.2 Local class field theory, the results 11
3.3 Local-global compatibility 11
3.4 Agenda for this course 12
3.5 $\mathbb{Z}_p$ and $\mathbb{Q}_p$ 12
3.6 Valuations 13

4 September 17 **14**
4.1 Completion and DVRs 14
4.2 Local fields 15
4.3 Global fields 16
4.4 Hensel's Lemma 17

5 September 21 **17**
5.1 More Hensel's Lemma 17
5.2 Extensions of absolute values 18

6 September 24 **19**
6.1 More on extensions of valuations and ramification 19

7 September 28 **22**
7.1 Extension of valuation and tensor products . . . 22
7.2 The decomposition group . . . 24

8 October 1 **26**
8.1 The inertia group . . . 26
8.2 Unramified extensions . . . 27

9 October 5 **28**
9.1 Unramified extension, wrap-up . . . 28
9.2 Totally ramified extensions . . . 28
9.3 Multiplicative structure of $K^\times$: . . . 29

10 October 12 **30**
10.1 Corollaries of last time . . . 30
10.2 Approaches to exponentiation in local fields . . . 31
10.3 p-adic exponential and logarithm . . . 32
10.4 The Artin map for unramified extensions . . . 33

11 October 15 **34**
11.1 Finishing off the unramified Artin map . . . 34
11.2 Ramification groups . . . 35
11.3 Tamely ramified extensions . . . 37
11.4 Upper numbering . . . 37

12 October 19 **38**
12.1 Group and Galois cohomology: references . . . 38
12.2 The category of G-modules . . . 38

13 October 22 **41**
13.1 Co-induced and induced modules . . . 41
13.2 Group cohomology as derived functor . . . 42
13.3 The standard resolution . . . 44

14 October 26 **44**
14.1 Homogeneous and inhomogeneous cochains . . . 44
14.2 H^1, H^2 and group extensions . . . 46
14.3 Torsors . . . 47

15 October 29 **48**
15.1 Torsors, continued . . . 48
15.2 Group homology . . . 49

15.3 Plan for proving local class field theory . . . 50
15.4 Change of group and compatible pairs . . . 51

16 November 2 **51**
16.1 Change of group, continued . . . 51
16.2 The inflation-restriction exact sequence . . . 53
16.3 Tate Cohomology . . . 55

17 November 5 **57**
17.1 Tate Cohomology for Cyclic Groups . . . 57
17.2 Restriction and corestriction for Tate cohomology . . . 57
17.3 Cup Products . . . 60

18 More on Cup Product (not covered in lecture) **61**

19 November 12 **62**
19.1 Galois cohomology and Hilbert's Theorem 90 . . . 62
19.2 Cohomology of profinite groups . . . 63
19.3 $H^2(L/K, L^\times)$ when L/K is unramified. . . . 65

20 November 16 **66**
20.1 inv and change of base field . . . 66
20.2 Construction of the fundamental class $u_{L/K}$ . . . 67
20.3 Bounding the size of $H^2(L/K, L^\times)$ . . . 68
20.4 Tate's theorem . . . 70

21 November 19 **71**
21.1 Proof of Tate's theorem . . . 71
21.2 Another characterization of local reciprocity, and compatibility . . . 73
21.3 Normic Subgroups . . . 75
21.4 Existence . . . 75

22 November 26 **76**
22.1 Normic subgroups, continued . . . 76
22.2 Reciprocity map and ramification . . . 77
22.3 Quadratic extensions . . . 78
22.4 The big picture for $\mathbb{Q}_p$ . . . 79

23 November 30 **79**
23.1 Big picture for $\mathbb{Q}_p$, continued . . . 79
23.2 Motivating Lubin-Tate . . . 80
23.3 Formal groups . . . 80

23.4 Lubin-Tate series 82

24 December 3 **82**
24.1 Lubin-Tate formal groups 82
24.2 The field $K^{\pi,n}$ generated by π^n-torsion of F_f 84
24.3 Building maximal abelian extension and Artin map with Lubin-Tate theory 86

1 September 7: Global class field theory

Today we'll discuss global class field theory for the base field $\mathbb{Q}$, from the historical perspective.

1.1 Class fields

Let $L/\mathbb{Q}$ be a finite extension (not necessarily Galois!), with ring of integers $\mathcal{O}_L$. Let p be any integer prime. We'll look at the question of how $p\mathcal{O}_L$ factors into prime ideals in $\mathcal{O}_L$, and how this depends on p. We know that we have a factorization $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

If all $e_i = 1$ we say p is *unramified* in L; this is the case for all but finitely many p (those that divide the discriminant of $\mathcal{O}_L$. We assume now that p is unramified. In this case we'll define the *decomposition type* of p as the sequence $f_1, \ldots, f_r$, where $f_i = [\mathcal{O}_L/\mathfrak{p}_i : \mathbb{F}_p]$.

For fields where the ring of integers is monogenic you can determine decomposition data as follows :

Proposition 1.1. *Assume that $\mathcal{O}_L = \mathbb{Z}[\alpha]$. If α has minimal polynomial $f(x) \in \mathbb{Z}[x]$, and $\bar{f}(x) = \mathbb{F}_p[x]$ is the reduction of f modulo p, then the decomposition type of p in L is given by the list of degrees of irreducible factors of f.*

Example. $L = \mathbb{Q}[\sqrt{n}]$; if n is squarefree and not 1 mod 4, then : $\mathcal{O}_L = \mathbb{Z}[\sqrt{n}]$. If p is relatively prime to $2n$, then $\mathfrak{p}$ is unramified in L, and we have two possiblities for an integer prime p: either $p\mathcal{O}_L = \mathfrak{p}$ or $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. We can distinguish between the two using the proposition above. We find that the first case holds precisely when $\left(\frac{n}{p}\right) = -1$ and the second when $\left(\frac{n}{p}\right) = 1$. (This also holds when n is 1 mod 4.)

Definition. A finite Galois extension $L/\mathbb{Q}$ is a *class field* if for any (unramified) prime p, the decomposition data of $p\mathcal{O}_L$ depends only on the congruence class of p mod some modulus N. This modulus N is called the *conductor* of the class field.

Example. The field $L = \mathbb{Q}(\sqrt{n})$ is a class field because, using quadratic reciprocity you can calculate that the quadratic residue symbol $\left(\frac{n}{p}\right)$ depends only on the value of p modulo $4n$.

Example. For any n, the cyclotomic field $\mathbb{Q}(\zeta_n)$ is a class field of conductor n. One can prove this directly from Proposition 1.1, but we'll see an easier way next time.

Example. $\mathbb{Q}(\sqrt[3]{2})$ is not a class field: see course Sage demo. If $p \equiv 2 \bmod 3$ the decomposition type is always $\{1,2\}$ (exercise!) but for $p \equiv 1 \pmod 3$ the decomposition type can be either $\{1,1,1\}$ or $\{3\}$.

Example. The field $\mathbb{Q}(\alpha)$ where $\alpha^3 - 3\alpha - 1 = 0$ is another example of a class field, this time of modulus 9. See the online sage demo for an example.

Theorem 1.2 (Classical Main Theorem of Class Field Theory /$\mathbb{Q}$.)**.** *For $L/\mathbb{Q}$ a finite extenion, the following are equivalent*

(i) L *is a class field.*

(ii) $L/\mathbb{Q}$ *is an abelian Galois extension.*

(iii) $L \subset \mathbb{Q}(\zeta_n)$ *for some* n*.*

Example. When $q \equiv 1 \pmod 4$, $\mathbb{Q}(\sqrt{q})$ is contained in $\mathbb{Q}(\zeta_q)$, $q \equiv 1 \pmod 4$.

1.2 $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ and inverse limits

Another way of stating the equivalence of (ii) and (iii) is

Theorem 1.3 (Kronecker-Weber)**.** *The maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ is equal to $\mathbb{Q}(\zeta_\infty) = \bigcup_n \mathbb{Q}(\zeta_n)$.*

Let's compute the Galois group of the infinite extension $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$.

We can define a Galois group $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$ as usual as the group of automorphisms of $\mathbb{Q}(\zeta_\infty)$ fixing $\mathbb{Q}$.

This is what's known as a profinite group, and we'll define a topological group structure on it later. (Short version: take the subgroups $\mathrm{Gal}(\mathbb{Q}^{ab}/L)$ to form a nbhd base at 1.)

We have homomorphisms $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ for each positive integer n. Taking the product of all these gives a map

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \prod_n \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \prod_n (\mathbb{Z}/n\mathbb{Z})^\times$$

. The image here is precisely the set of $\{a_n\}$ such if $n \mid n'$, then the reduction mod n of $a_{n'}$ is equal to a_n.

The construction here is the special case of what's known as an *inverse limit*:

Definition. (See also the beginning of Chapter V of Cassels-Frohlich or V.2 of Neukirch ANT) A directed system I is a partially ordered set in which for any $i, j \in I$ there exists k with $i \le k, j \le k$.

If you have a collection $\{X_i\}_{i\in I}$ of sets, indexed by a directed system I, and maps $\pi_{ij} : X_j \to X_i$ whenever $i \leq j$, the inverse limit $\lim_{\leftarrow} X_i$ is equal to the subset of

$$\{\{x_i\} \in \prod_{i\in I} X_i \mid \pi_{ij}(x_j) = x_i \text{ whenever } i \leq j\}$$

If the X_i are all groups, rings, etc and the π_{ij} are morphisms, the inverse limit $\lim_{\leftarrow} X_i$ picks up the same structure. (This can also be defined categorically as the limit of a diagram.)

With this notation,

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \lim_{\leftarrow} \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \lim_{\leftarrow} (\mathbb{Z}/n\mathbb{Z})^\times.$$

(where the directed system here is the positive integers and divisibility, and all π_{ij} are natural restriction maps).

This group $\lim_{\leftarrow}(\mathbb{Z}/n\mathbb{Z})^\times$ is equal to the group of units $\hat{Z}^\times$ in the ring $\hat{\mathbb{Z}} = \lim_{\leftarrow}(\mathbb{Z}/n\mathbb{Z})$.

2 September 10

Last time we stated

Theorem 2.1 (Classical Main Theorem of Class Field Theory /$\mathbb{Q}$.)**.** *For $L/\mathbb{Q}$ a finite extenion, the following are equivalent*

(i) L *is a class field.*

(ii) $L/\mathbb{Q}$ *is an abelian Galois extension.*

(iii) $L \subset \mathbb{Q}(\zeta_n)$ *for some* n.

Today we're going to take this as given, and deduce the modern statement of class field theory over $\mathbb{Q}$. This will motivate something called the "global Artin map", which we'll then break down into "local pieces", motivating local class field theory.

2.1 Frobenius elements; working towards the Artin map

However, first I'd like to digress a little bit and say some more about prime decomposition in extensions.

More facts from a first course in algebraic number theory. Same situation as before, p unramified in a finite extension $L/\mathbb{Q}$. Choose one of the prime factors $\mathfrak{p}$ of $p\mathcal{O}_L$.

It's known that $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the set of primes above $\mathfrak{p}$, so this set is given by $\{g\mathfrak{p} \mid g \in G\}$, and all f_i are equal, call them f.

Definition. The decomposition group $D_\mathfrak{p} \subset \mathrm{Gal}(L/\mathbb{Q})$ is the stabilizer of $\mathfrak{p}$, that is

$$D_\mathfrak{p} = \{g \in \mathrm{Gal}(L/K) \mid g\mathfrak{p} = \mathfrak{p}\}.$$

There's a natural homomomorphism $\phi : D_\mathfrak{p} \to \mathrm{Gal}(\ell/\mathbb{F}_p)$. where $\ell = \mathcal{O}_L/\mathfrak{p}$. In the general case, ϕ is surjective: because of our assumption that p is unramified, we in fact know that ϕ is an isomorphism. This already tells us that $f = |D_\mathfrak{p}|$.

But also we know that $\mathrm{Gal}(\ell/\mathbb{F}_p)$ is cyclic and generated by the Frobenius automorphism $x \mapsto x^p$, we have the following consequence

Proposition 2.2. *In the situation above (in particular, assuming p unramified) there exists a unique* $\mathrm{Frob}_\mathfrak{p} \in D_\mathfrak{p} \subset \mathrm{Gal}(L/\mathbb{Q})$ *such that* $\mathrm{Frob}_\mathfrak{p}(a) \equiv a^p \pmod{\mathfrak{p}}$ *for all* $a \in \mathcal{O}_L$. *Furthermore* $\mathrm{Frob}_\mathfrak{p}$ *generates* $D_\mathfrak{p}$.

You can check that $\mathrm{Frob}_{g\mathfrak{p}} = g\,\mathrm{Frob}_\mathfrak{p}\,g^{-1}$. So if $L/\mathbb{Q}$ is abelian, $\mathrm{Frob}_\mathfrak{p}$ depends only on the prime p of $\mathbb{Z}$, not the choice of $\mathfrak{p}$ lying above p, and we may write it as Frob_p.

(Note, this all can still be done with $\mathbb{Q}$ replaced by any global field K.)

Hence for any unramified abelian extension $L/\mathbb{Q}$ we have the information of the finite group $\mathrm{Gal}(L/\mathbb{Q})$ along with a map

$$\{\text{primes of } \mathbb{Z}\} \to \mathrm{Gal}(L/\mathbb{Q})$$

sending p to Frob_p. From this information we can determine the splitting data of all primes as explained above. You should think of this information as the "signature" of the extension $L/\mathbb{Q}$; the information uniquely determine L, and also can be used to build the L-function of L.

Example. Cyclotomic fields: $L = \mathbb{Q}(\zeta_n)$. Have map $\mathrm{Gal}(L/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$, sends g to unique k such that $g\zeta_n = \zeta_n^k$, injective because L generated by ζ, surjective because cyclotomic polynomial Φ_n is irreducible over $\mathbb{Q}$. (This is a special fact about $\mathbb{Q}$, and doesn't work for other base fields!)

The unramified primes p are those relatively prime to n. We know that there is a unique element $\mathrm{Frob}_\mathfrak{p}$ with $\mathrm{Frob}_\mathfrak{p}(a) \equiv a^p \pmod{\mathfrak{p}}$ for all $a \in \mathcal{O}_L = \mathbb{Z}[\zeta_n]$. Setting $a = \zeta_n$ we see that we must have $\mathrm{Frob}_\mathfrak{p}(\zeta) = \zeta_n^p$. Hence $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/\mathbb{Q})$ corresponds to the element $p \in (\mathbb{Z}/n\mathbb{Z})^\times$.

From this it is clear that $\mathbb{Q}(\zeta_n)$ is indeed a class field.

2.2 More on $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$, adeles, and the Artin map

We saw last time that $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \varprojlim \mathbb{Z}/n\mathbb{Z} \cong \hat{\mathbb{Z}}$.

Just as each ring $\mathbb{Z}/n\mathbb{Z}$ can be factored via CRT into a product of rings $\mathbb{Z}/(p_1^{e_1})\mathbb{Z} \times \cdots \times \mathbb{Z}/(p_k^{e_k}\mathbb{Z})$, the same is true of

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p.$$

where each factor $\mathbb{Z}_p$ is $\lim_{\leftarrow}(\mathbb{Z}/p^e\mathbb{Z})^\times$.

Hence we can factorize our Galois group into a product of local factors:

$$\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times \cong \prod_p \mathbb{Z}_p^\times.$$

This statement turns out to not generalize correctly when one replaces $\mathbb{Q}$ by number fields without unique factorization, so we'll state things a little differently.

Definition. Define

$$\mathbb{A}_{\mathbb{Q},\mathrm{fin}}^\times = \{\{a_p\} \in \prod_p \mathbb{Q}_p^\times \mid a_p \in \mathbb{Z}_p^\times \text{ for all but finitely many } p\}$$

and

$$\mathbb{A}_{\mathbb{Q}}^\times = \mathbb{A}_{\mathbb{Q},\mathrm{fin}}^\times \times \mathbb{R}^\times.$$

Then (exercise!)

$$\mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{Q}^\times \times \mathbb{R}^{>0}) \cong \prod_p \mathbb{Z}_p^\times.$$

The map

$$\phi : \mathbb{A}_{\mathbb{Q}}^\times \to \mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{Q}^\times \times \mathbb{R}^{>0}) \to \hat{\mathbb{Z}}^\times \cong \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$$

is at the heart of global class field theory. I would like to call this the Artin map, but unfortunately I have some awkward notational issues here. If I call the map above ϕ, then the Artin map is actually given by $\theta_{\mathbb{Q}}(a) = \phi(a)^{-1}$, e.g. we compose with the reciprocal map.

To explain why I'll work out the following example, which shows how the Artin map relates to the Frobenius:

Example. Let ℓ be a prime. Consider an element $a \in \mathbb{A}_{\mathbb{Q}}$ with $\{a_p\} = 1$ for $p \neq \ell$, $a_\infty = 1$, and $a_\ell \in \mathbb{Q}_\ell$ is arbitrary. Write $a_\ell = \ell^e u$. We won't compute all of $\theta(a)$, though we could; instead we'll just compute the image of $\theta(a)$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ for n relatively prime to ℓ (so ℓ is unramified).

First, we find the image of $[a]$ under the isomorphism $\mathbb{A}_{\mathbb{Q}}^\times/(\mathbb{Q}^\times \times \mathbb{R}^{>0}) \to \hat{\mathbb{Z}}^\times$. To do this, we note that a is equivalent mod $\mathbb{Q}^\times$ to the adele $\ell^{-e}a$, which has components $(\ell^{-e}a)_\ell = u$ and $(\ell^{-e}a)_p = \ell^{-e}$. This gives us an element of $\prod_p \mathbb{Z}_p \cong \hat{\mathbb{Z}}$. Since ℓ does not divide n, when we reduce mod n we obtain the element ℓ^{-e} in $\mathbb{Z}/n\mathbb{Z}^\times$. Since Frob_ℓ corresponds to the element $\ell \in \mathbb{Z}/n\mathbb{Z}^\times$, we conclude that the restriction of $\phi(a)$ to $\mathbb{Q}(\zeta_n)$ is given by $\phi(a)|_{\mathbb{Q}(\zeta_n)} = \mathrm{Frob}_\ell^{-e}$, and that $\theta_{\mathbb{Q}}(a)|_{\mathbb{Q}(\zeta_n)} = \mathrm{Frob}_\ell^e$. (This is the reason for taking the reciprocal: to eliminate the negative sign.)

2.3 Adeles over a general number field

We now want to generalize the isomorphism

$$\theta_{\mathbb{Q}} : \mathbb{A}_{\mathbb{Q}}^{\times} \to \mathbb{A}_{\mathbb{Q}}^{\times}/(\mathbb{Q}^{\times} \times \mathbb{R}^{>0}) \cong \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$$

when we replace the base field $\mathbb{Q}$ by an arbitrary number field K. We won't be able to describe K^{ab} so easily, but it's still possible to prove this isomorphism.

For any number field K one can define

$$\mathbb{A}_{K,\mathrm{fin}}^{\times} = \{\{x_{\mathfrak{p}}\} \in \prod_{\mathfrak{p}} K_{\mathfrak{p}}^{\times} \mid x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^{\times} \text{ for all but finitely many } \mathfrak{p}\}$$

(we will formally define these completions $K_{\mathfrak{p}}$ next time), and

$$\mathbb{A}_{K,\infty}^{\times} = \prod_{\text{embeddings} K \hookrightarrow \mathbb{R}} \mathbb{R}^{\times} \times \prod_{\text{embeddings } K \hookrightarrow \mathbb{C}} \mathbb{C}^{\times}$$

where in the second factor we use only the embeddings $K \hookrightarrow \mathbb{C}$ that don't factor through $\mathbb{R}$, and consider complex conjugate embeddings to be the same. Then define

$$\mathbb{A}_K^{\times} = \mathbb{A}_{K,\mathrm{fin}}^{\times} \times \mathbb{A}_{K,\infty}^{\times}.$$

We note here that $\mathbb{A}_{K,\mathrm{fin}}^{\times}$, $\mathbb{A}_{K,\infty}^{\times}$ and $\mathbb{A}_K^{\times}$ can be made into topological groups. For $\mathbb{A}_{K,\mathrm{fin}}^{\times}$ the neighborhood basis at the identity consists of open sets of the form

$$\prod_{\mathfrak{p} \in S} U_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{\mathfrak{p}}^{\times}$$

where S ranges over finite sets of primes and for each $\mathfrak{p} \in S$, $U_{\mathfrak{p}}$ is an open subset of $K_{\mathfrak{p}}$.

The topology on $\mathbb{A}_{K,\infty}^{\times}$ is just the product of the usual topologies on the individual factors $\mathbb{R}^{\times}$ and $\mathbb{C}^{\times}$. Then we give $\mathbb{A}_K^{\times} = \mathbb{A}_{K,\mathrm{fin}}^{\times} \times \mathbb{A}_{K,\infty}^{\times}$ the product topology.

One can check that $\mathbb{A}_{K,\mathrm{fin}}^{\times}$ is totally disconnected, and that the connected component of the identity in $\mathbb{A}_K^{\times}$ is given by

$$(\mathbb{A}_K^{\times})_0 = \prod_{\text{embeddings } K \hookrightarrow \mathbb{R}} \mathbb{R}^{>0} \times \prod_{\text{embeddings } K \hookrightarrow \mathbb{C}} \mathbb{C}^{\times}.$$

2.4 The Artin map and class field theory over a general number field

As over $\mathbb{Q}$, there exists an Artin map

$$\theta_K : \mathbb{A}_K^{\times} \to \mathrm{Gal}(K^{ab}/K).$$

As before $K^\times \subset \ker \theta_K$: this is known as Artin reciprocity. The Artin map then factors through the *adelic class group* $C_K = \mathbb{A}_K^\times / K^\times$. More specifically, it gives isomorphisms

$$C_K/(C_K)_0 \cong \mathrm{Gal}(K^{ab}/K).$$

Where $(C_K)_0$ is the connected component of the identity in C_K. This connected component $(C_K)_0$ is harder to describe than $(\mathbb{A}_K)_0$ but it can be expressed as the closure of the image of $(\mathbb{A}_K)_0$ in C_K.

There's also a version of the Artin map for finite extensions: if L/K is a finite extension, then $\theta_{L/K} : C_K/N(C_L) \to \mathrm{Gal}(L/K)$ is an isomorphism. There is a one-to-one correspondence between finite extensions of K and to open subgroups of finite index in C_K, given by sending an extension L/K to $N(C_L)$.

The main results of global class field theory then break into three parts:

- Construction of the Artin map $\theta : \mathbb{A}_K \to \mathrm{Gal}(K^{ab}/K)$
- Artin reciprocity $K^\times \subset \ker \theta$
- Existence: every finite index open subgroup of C_K is of the form $N(C_L)$ for some L. This implies injectivity of the Artin map.

The last two parts will be done next semester, but by the end of the semester we'll be able to do the first one, constructing the Artin map via local factors. Also, the proofs we do next semester will use the same machinery as this semester's proofs.

3 September 14

3.1 A bit more on the global Artin map

Last time we stated the existence of an isomorphism

$$\theta_K : C_K/(C_K)_0 \cong \mathrm{Gal}(K^{ab}/K).$$

There's also a version of the Artin map for finite extensions: if L/K is a finite extension, then $\theta_{L/K} : C_K/N(C_L) \to \mathrm{Gal}(L/K)$ is an isomorphism. There is a one-to-one correspondence between finite extensions of K and to open subgroups of finite index in C_K, given by sending an extension L/K to $N(C_L)$.

Example. $K = \mathbb{Q}$. Then we've seen that $C_K \cong \hat{\mathbb{Z}}^\times \times \mathbb{R}^{>0}$. The open finite index subgroups of $\hat{\mathbb{Z}}^\times$ are all of the form $\pi_m^{-1}(G)$ for any integer m and any subgroup $G \subset \mathbb{Z}/m\mathbb{Z}^\times$, where π_m is the projection $\hat{\mathbb{Z}} \to \hat{\mathbb{Z}}/m\mathbb{Z}^\times$. The abelian extension corresponding to $\pi_m^{-1}(G)$ is the class field L such that the primes which split completely in L are those whose reduction mod m belongs to G.

3.2 Local class field theory, the results

Now let K be a local field, e.g. $K = \mathbb{Q}_p$. Then there is a local Artin map

$$\theta_K : K^\times \to \mathrm{Gal}(K^{ab}/K).$$

This map is not quite surjective, but it does have dense image, and induces a bijection between (finite index open subgroups of $K^\times$) and (finite index open subgroups of $\mathrm{Gal}(K^{ab}/K)$).

Again, we have a version of the Artin map for finite extensions: if L/K is a finite abelian extension have $\theta_{L/K} : K^\times/NL^\times \to \mathrm{Gal}(L/K)$. (So we have an existence theorem: every open finite index subgroup of $K^\times$ is of the form $NL^\times$ for some finite abelian extension L/K.)

If L/K is unramified, then we can describe the Artin map very explicitly; $\theta_{L/K}(x) = \mathrm{Frob}_{L/K}^{v(x)}$ (Frobenius elements defined in a manner similar to the global clase). Related to this, the fixed field of the subgroup $\theta_K(\mathcal{O}_K^\times) \subset \mathrm{Gal}(K^{ab}/K)$ is the maximal abelian unramified extension of K.

3.3 Local-global compatibility

Now let's let K be a global field again. We can create a completion $K_\mathfrak{p}$ at any prime $\mathfrak{p}$.

Then for any abelian extension L/K, and any prime $\mathfrak{p}'$ of L above $\mathfrak{p}$, we get an extension of completions $L_{\mathfrak{p}'}/K_\mathfrak{p}$. We have map $\mathrm{Gal}(L_{\mathfrak{p}'}/K_\mathfrak{p}) \to \mathrm{Gal}(L/K)$ via restriction. One can show that this is injective with image equal to decomposition group $D_{\mathfrak{p}'}$: for the inverse map, take the automorphism of L and extend continuously to get an automorphism of $L_{\mathfrak{p}'}$. (to define the inverse map $D_{\mathfrak{p}'} \to \mathrm{Gal}(L_{\mathfrak{p}'}/K_\mathfrak{p})$ extend continuously in $\mathfrak{p}'$-adic topology.)

Hence every abelian extension of K embeds in an abelian extension of $\overline{K}$, and so we have an inclusion $K^{ab} \subset K_\mathfrak{p}^{ab}$. (This inclusion requires making some choices, but its image is well-defined as the maximal abelian extension of K contained in $K_\mathfrak{p}^{ab}$.)

The local and global maps are compatible in the sense that the diagram

$$\begin{array}{ccc} K_\mathfrak{p}^\times & \xrightarrow{\theta_{K_\mathfrak{p}}} & \mathrm{Gal}(K_\mathfrak{p}^{ab}/K_\mathfrak{p}) \\ \downarrow & & \downarrow \\ \mathbb{A}_K^\times & \xrightarrow{\theta_K} & \mathrm{Gal}(K^{ab}/K) \end{array}$$

commutes. Since $\mathbb{A}_K^\times$ is generated topologically by the $K_\mathfrak{p}^\times$ and by the copies of $\mathbb{R}^\times$ and $\mathbb{C}^\times$, knowing all the local Artin maps will be enough to construct the global Artin map.

3.4 Agenda for this course

This concludes our brief overview of the results of class field theory. In the rest of the course we will go through

- Theory of local fields
- Ramification
- Galois cohomology
- Lubin-Tate theory (explicit construction of abelian extensions of local fields)
- (time permitting?) Brauer groups
- (time permitting?) applications of global class field theory.

3.5 $\mathbb{Z}_p$ and $\mathbb{Q}_p$

We previously defined $\mathbb{Q}_p$ as the fraction field of $\mathbb{Z}_p$, where $\mathbb{Z}_p$ is the inverse limit $\lim_{\leftarrow} \mathbb{Z}/p^n\mathbb{Z}$. That is, we can specify an element of $\mathbb{Z}_p$ by specifying elements $a_n \in \mathbb{Z}/\mathfrak{p}^n\mathbb{Z}$ such that a_m reduces mod p^n to a_n when $m > n$.

Alternately, if we have a sequence $\{a_i\}$ of elements of $\mathbb{Z}$ such that for every n, the sequence $\{a_i \mod p^n\}$ eventually becomes constant in $\mathbb{Z}/p^n\mathbb{Z}$, then this gives us an element of $\mathbb{Z}_p$, which we denote by $\lim_{i\to\infty} a_i$.

We can also interpret this limit topologically: define an absolute value $|\cdot|_p$ on $\mathbb{Z}$ by $|a|_p = p^{-\nu_p(a)}$, where the *p-adic valuation* $\nu_p(a)$ is the exponent of p in the prime factorization on a. Then $\mathbb{Z}_p$ is the completion (as topological ring) of $\mathbb{Z}$ with respect to $|\cdot|_p$.

Example. We can define the element $-1/2 \in \mathbb{Z}_5$ in multiple ways

- as the element: $\{-2^{-1} \in \mathbb{Z}/p^n\mathbb{Z}\}_{n\geq 0}$ of the inverse limit.
- as a limit $\lim_{i\to\infty} \frac{5^i-1}{2}$
- as an infinite sum $\sum_{i\geq 0} 2 \cdot 5^i$ (this is a special instance of base p expansion)

As with real numbers, you can't do p-adic arithmetic to infinite precision, but you can do finite precision-arithmetic: this is equivalent to working in $\mathbb{Z}/p^n\mathbb{Z}$ for some finite n. SAGE's default is $N = 20$, so it would express $-1/2$ as

```
2 + 2*5 + 2*5^2 + 2*5^3 + 2*5^4 + 2*5^5 + 2*5^6 + 2*5^7 + 2*5^8
+ 2*5^9 + 2*5^10 + 2*5^11 + 2*5^12 + 2*5^13 + 2*5^14 + 2*5^15
+ 2*5^16 + 2*5^17 + 2*5^18 + 2*5^19 + O(5^20)
```

Conveniently, since $\mathbb{Z}/p^n\mathbb{Z}$ is a ring, you don't have the same issues of error propagation that you do over the reals.

Also, $\mathbb{Q}_p$ is even nicer to define this way, as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, or the set of all sums $\sum_{i\geq X} a_i p^i$ where now X can be any (possibly negative) integer. It follows that $\mathbb{Q}_p$ is a field and is equal to the field of fractions of $\mathbb{Z}_p$, and also that $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$.

Another ring and field that are very similar to $\mathbb{Z}_p$ and $\mathbb{Q}_p$ are $\mathbb{F}_p[[t]]$ and $\mathbb{F}_p((t))$. These can also be expressed as completitons of $\mathbb{F}_p[t]$ and $\mathbb{F}_p(t)$.

3.6 Valuations

We'd now like to formally generalize the constructions above.

Definition. A valuation on a field K is a map $\nu : K \to \mathbb{Z} \cup \infty$ satisfying

a) $\nu(0) = \infty$

b) $\nu : K^\times \to \mathbb{Z}$ is a **surjective** group homomorphism (I forgot surjectivity in class)

c) $\nu(x+y) \geq \min(\nu(x), \nu(y))$ for all $x, y \in K$.

Example. For $K = \mathbb{Q}$, we define the p-adic valuation $\nu_p(x)$ as the exponent of p in the prime factorization of x.

Example. More generally, if $\mathcal{O}$ is a Dedekind domain, $K = \mathrm{Frac}(\mathcal{O})$, and $\mathfrak{p}$ a prime ideal of $\mathcal{O}$, we define $\nu_\mathfrak{p}(x)$ to be the exponent of $\mathfrak{p}$ in the prime factorization of the fractional ideal (x).

A related definition

Definition. An absolute value on a field is a map $|\cdot| : K \to \mathbb{R}^{\geq 0}$ satisfying

a) $|0| = 0$

b) $|\cdot| : K^\times \to \mathbb{R}^{>0}$ is a (multiplicative) group homomorphism

c) $|a+b| \leq |a| + |b|$

If the absolute value satisfies c'): $|a+b| \leq \max(|a|, |b|)$ then it is said to be *non-archimedean*, otherwise *archimedean*.

Two absolute values $|\cdot|_1, |\cdot|_2$ are said to be *equivalent* if there exits $a \in \mathbb{R}^{>0}$ such that $|\cdot|_1 = |\cdot|_2^a$.

Note that if ν is an absolute value and $c < 1$ is a positive constant, then $|x|_\nu = c^{\nu(x)}$ is an absolute value whose equivalence class does not depend on c.

Also, embeddings $K \hookrightarrow \mathbb{R}$ or $K \hookrightarrow \mathbb{C}$ also give absolute values by pulling back the standard absolute value on $\mathbb{R}$ or $\mathbb{C}$.

In the case of $\mathbb{Q}$ this follows from

Theorem 3.1 (Ostrowski)**.** *Every absolute value on* $\mathbb{Q}$ *is equivalent to some* $|\cdot|_p$ *or to the absolute value* $|\cdot|_{\mathbb{R}}$ *coming from the embedding* $\mathbb{Q} \hookrightarrow \mathbb{R}$*.*

We won't prove this in class, but Ben might in section.

A similar theorem is true for $K = \mathbb{F}_p(t)$. Let $\mathcal{O}$ equal $\mathbb{F}_p[t]$; then we have valuations coming from the prime ideals of $\mathcal{O}$, and also a valuation given by $\nu(x) = -\deg(x)$ (which you can also think of as coming from the ideal $(1/t)$ in the ring $\mathbb{F}_p[1/t]$). One can show that every place $\mathbb{F}_p(t)$ comes from one of these valuations.

4 September 17

4.1 Completion and DVRs

Observe that if $|\cdot|$ is an absolute value on K then it comes from exponentiating a valuation if and only if the image of $|\cdot| : K^\times \to \mathbb{R}^{>0}$ is a discrete subgroup of $\mathbb{R}^\times$.

Definition. A discrete valuation ring (DVR) is a local PID that is not a field.

If ν is a valuation on a field K then $\mathcal{O} = \{x \in K \mid \nu(x) \geq 0\}$ is a DVR (justifying the name) with principal ideal $\mathfrak{p} = \{x \in K \mid \nu(x) \geq 1\}$ generated by any π with $\nu(\pi) = 1$. Also, $\mathcal{O}$ is both a closed and open ball in K (so the topology on K is totally disconnected).

Conversely if $\mathcal{O}$ is a DVR with maximal ideal $\mathfrak{p}$ and fraction field K, then $\mathcal{O}$ is Dedekind, so we have a valuation $\nu_\mathfrak{p}$ on K (and $\mathcal{O}_{\nu_\mathfrak{p}} = \mathcal{O}$).

Completion: If K is a field with absolute value $|\cdot|$, then the metric space completion $\hat{K}$ of K with respect to the norm $|\cdot|$ is a topological field, and the absolute value $|\cdot|$ extends to $\hat{K}$. If $|\cdot|$ comes from a valuation or a place, this completion is also written as K_ν.

If $\mathcal{O}$ is a complete DVR, then $\mathcal{O} = \varprojlim \mathcal{O}/\mathfrak{p}^n = \varprojlim \mathcal{O}/(\pi)^n$. The argument for this is that any element of $\varprojlim \mathcal{O}/(\pi)^n$ gives a sequence of nested balls in $\mathcal{O}$ with radii shrinking down to 0; completeness means that this must contain a unique point.

Now suppose that $\mathcal{O}$ is an arbitrary ring with prime $\mathfrak{p}$ and $K = \operatorname{Frac}\mathcal{O}$. Then we can complete $\mathcal{O}$ and K with respect to the $\mathfrak{p}$-adic absolute value to obtain rings which we will call $\mathcal{O}_\mathfrak{p}$ and $K_\mathfrak{p}$. One can check that

- $\mathcal{O}_\mathfrak{p}$ is the valuation ring of $K_\mathfrak{p}$
- the maximal ideal of $\mathcal{O}_\mathfrak{p}$ is equal to $\mathfrak{p}\mathcal{O}_\mathfrak{p}$, and is also equal to the closure of $\mathfrak{p}$ in $\mathcal{O}_\mathfrak{p}$
- $\mathcal{O}/\mathfrak{p}^i\mathcal{O} \cong \mathcal{O}_\mathfrak{p}/\mathfrak{p}^i\mathcal{O}_\mathfrak{p}$ for all $i \geq 0$.

From the last item we conclude that

$$\mathcal{O}_\mathfrak{p} \cong \varprojlim \mathcal{O}_\mathfrak{p}/\mathfrak{p}^i\mathcal{O}_\mathfrak{p} \cong \varprojlim \mathcal{O}/\mathfrak{p}^i\mathcal{O}.$$

This generalizes $\mathbb{Z}_p \cong \varprojlim \mathbb{Z}/p^i\mathbb{Z}$.

4.2 Local fields

A local field is a complete field K with absolute value $|\cdot|$ that is locally compact.

Theorem 4.1. *Ostrowski: The only archimedean local fields are $\mathbb{R}$ and $\mathbb{C}$, and indeed the only complete archimedean fields are $\mathbb{R}$ and $\mathbb{C}$.*

Now let K be a non-archimedean local field, with valuation ring $\mathcal{O}$.

Proposition 4.2. *a) $\mathcal{O}$ is compact*

b) $|\cdot|$ is discrete

c) $\mathcal{O}/\pi\mathcal{O}$ is finite (where π is a generator of $\mathfrak{p}$, which we know is principal by b))

Proof. a) Take some $a \in K$ with $|a| < 1$. By local compactness, $a^n\mathcal{O}$ must be compact for sufficiently large n. Then $\mathcal{O}$ is homeomorphic to $a^n\mathcal{O}$ by rescaling.

b) Let $\mathfrak{p} = \{x \in \mathcal{O} \mid |x| < 1\}$ be the maximal ideal of $\mathcal{O}$, or equivalently the open unit ball around 0. We know that $\mathfrak{p}$ is an open subset of $\mathcal{O}$, but also $\mathfrak{p}$ is closed in $\mathcal{O}$ because $\mathcal{O} \setminus \mathfrak{p}$ is a union of additive cosets of $\mathfrak{p}$, hence open. (This is a special case of the fact that an open subgroup of a topological group is also closed.) We've already seen that $\mathcal{O}$ is compact, so its closed subset $\mathfrak{p}$ must also be compact.

The compact set $\mathfrak{p}$ has a nested open cover by the sets $\{a \mid |a| < \delta\}$ for every $\delta \in (0, 1)$. By compactness, there must be a finite subcover, so there must be some $\delta < 1$ such that there is no $a \in K$ with $|a| \in (\delta, 1)$. It follows that the absolute value $|\cdot|$ must be discrete.

c) Because $\pi\mathcal{O}$ is an open subgroup of $\mathcal{O}$, the projection $\mathcal{O} \to \mathcal{O}/\pi\mathcal{O}$ is continuous. Then $\mathcal{O}/\pi\mathcal{O}$ is a compact topological space with discrete topology, hence finite.

□

We also have the following converse: if $|\cdot|$ is discrete and $\mathcal{O}/\pi\mathcal{O}$ is finite, then $\mathcal{O} = \lim_{\leftarrow} \mathcal{O}/\pi^n\mathcal{O}$ is an inverse limit of finite groups, hence compact. (It's a closed subset of the product $\prod_n \mathcal{O}/\pi^n\mathcal{O}$.)

Definition. If K is a nonarchimedean local field with discrete valuation ν, then the normalized absolute value $|\cdot|_K$ on K is

$$|a|_K = |\mathcal{O}/(\pi)|^{-\nu(a)}.$$

This has a measure-theoretic interpretation: if μ is the Haar measure on the topological group K^+, then for any $a \in K$ and any measurable $X \subset K^+$, we have $\mu(aX) = |a|_K\mu(X)$.

We can also define normalized absolute values on $\mathbb{R}$ and $\mathbb{C}$, by $|a|_{\mathbb{R}} = |a|$ and $|a|_{\mathbb{C}} = |a|^2$: these also have the same property.

4.3 Global fields

My axiomatic definition of global field in class was wrong: to be a global field, K *must have a product formula as well as having all completions be local fields. A counterexample is given by the field* $\mathbb{Q}((\mathbb{Q}^\times)^{1/2})$ *which is the compositum of all quadratic extensions of* $\mathbb{Q}$*. Any completion of this field is either* $\mathbb{C}$ *or the compositum of all quadratic extensions of* $\mathbb{Q}_p$ *for all* p *(we'll later see that this is a finite extension of* $\mathbb{Q}_p$*). The product formula fails because* K *has uncountably many valuations and you get an uncountable infinite product instead of a finite product. I've edited this section accordingly.*

Definition. A field K is a global field if it is a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$.

Definition. A *place* v of a field K is an equivalence class of absolute values on K.

Note that every valuation on K gives a place (hence using the same notation for them); places that come from valuations are called *finite* (or *non-archimedean*). Places that come from embeddings into $\mathbb{R}$ or $\mathbb{C}$ are called *infinite* (or *archimedean*). These two categories cover all places of global fields.

One nice property of global fields is:

Proposition 4.3 (Product formula)**.** *If* K *is a global field then* $\prod_v |a|_v = 1$ *for all* $a \in K$ *using normalized valuations (where this is the product over all places* v *of* K*, including the archimedean ones).*

The product formula is easily checked for $K = \mathbb{Q}$ and $K = \mathbb{F}_p(t)$. Later we'll prove the product formula for arbitrary global fields by showing that the product formula for K implies the product formula for any finite extension of K.

There's also an axiomatic characterization of global fields

Theorem 4.4 (Artin-Whaples)**.** *A field* K *is a global field if and only if all completions of* K *are local fields and* K *satisfies the product formula: .*

$$\prod_v |a|_v = 1$$

where all but finitely many terms in this product are 1*, for all* $a \in K$*.*

We won't be proving the "if" direction in this class. Ostrowski's theorem tells us that the "only if" direction holds when K is $\mathbb{Q}$, and the function field analogue gives the same for $\mathbb{F}_q(t)$. We'll later show that if K satisfies the Artin-Whaples criterion, then so does any finite extension of K, which will give the rest of the "only if".

The terminology of places also allows us to define the adeles in a way that puts the finite and infinite factors on a more equal footing.

Indeed,

$$\mathbb{A}_K^\times = \{\{a_v\} \in \prod_v K_v^\times \mid |a_v|_v = 1 \text{ for almost all } v\}.$$

4.4 Hensel's Lemma

Lemma 4.5 (Hensel-Newton). *Let $\mathcal{O}$ be a complete DVR and $f(x) \in \mathcal{O}[x]$ be a polynomial. If there exists $a_0 \in K$ with $|f(a_0)| < |f'(a_0)|^2$ then there exists $a \in K$ with $f(a) = 0$ and $|a - a_0| < \frac{|f(a_0)|}{|f'(a_0)^2|}$ (in fact, this a is unique).*

Sketch. Define a sequence a_i by

$$a_{i+1} = a_i + \frac{f(a_i)}{f'(a_i)}$$

and let a be the limit. □

5 September 21

5.1 More Hensel's Lemma

Last time we stated:

Lemma 5.1 (Hensel-Newton). *Let $\mathcal{O}$ be a complete DVR and $f(x) \in \mathcal{O}[x]$ be a polynomial. If there exists $a_0 \in K$ with $|f(a_0)| < |f'(a_0)|^2$ then there exists $a \in K$ with $f(a) = 0$ and $|a - a_0| < \frac{|f(a_0)|}{|f'(a_0)^2|}$ (in fact, this a is unique).*

In fact, one can sharpen this to $|a - a_0| = \frac{|f(a_0)|}{|f'(a_0)|}$ and can show that a is the only solution in the closed ball of radius $|f'(a_0)|$ around a. We won't go into the details of this.

Corollary 5.2 (Also Hensel's Lemma). *Let $\mathcal{O}$ be a complete DVR and $k = \mathcal{O}/\pi\mathcal{O}$. If, for $f \in \mathcal{O}[x]$, there exists $\overline{a} \in k$ such that $\overline{f}(\overline{a}) = 0$ but $\overline{f}'(\overline{a}) \neq 0$, then $\overline{a}$ lifts to a unique root $a \in \mathcal{O}$ of f.*

Proof. Apply the previous form of Hensel's lemma with $a_0 \in \mathcal{O}$ any lift of $\bar{a}$. □

Example. The polynomial $x^p - x$ has p distinct roots in $\mathbb{F}_p$, so also in $\mathbb{Z}_p$. Hence $\mathbb{Z}_p$ contains all the $p-1$th roots of unity, and they are distinct mod p.

Example. $x \in \mathbb{Z}_p^\times$ is a square iff it is a square mod p, $x \in \mathbb{Q}_p^\times$ is a square iff $x = p^{2r}u$ with $u \in \mathbb{Z}_p^\times$ a square. As a consequence $\mathbb{Q}_p$ has only three quadratic extensions: $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{u})$ and $\mathbb{Q}_p(\sqrt{up})$ where $u \in \mathbb{Z}_p^\times$ is a non-square.

Lemma 5.3 (Hensel, polynomial form). *Let $\mathcal{O}$ be a complete DVR with maximal ideal (π) and residue field $k = \mathcal{O}/\pi$. Suppose $f \in \mathcal{O}[x]$ is such that the reduction $\overline{f}$ factors as $\overline{f} = \overline{g}\overline{h}$ and $\gcd(\overline{g}, \overline{h}) = 1$ in $k[x]$. Then f factors as gh with $g, h \in \mathcal{O}[x]$ and g, h reduce to $\overline{g}, \overline{h}$ mod π and $\deg g = \deg \overline{g}$.*

Proof. Enough to prove that we can factor $f \equiv g_n h_n \mod \pi^n$ for all n compatibly, for polynomials $g, h \in \mathcal{O}[x]$ with $\deg g_n = d_g = \deg \bar{g}$, $\deg h_n = d_h = \deg f - \deg \bar{h}$

For $n = 1$, take g_1 lifting g and h_1 lifting h.

Now suppose we have $g_n, h_n \in \mathcal{O}[x]$ with $g_n h_n \equiv f \pmod{\pi^n}$.

Now let $g_{n+1} = g_n + \pi^n a$, $h_{n+1} = h_n + \pi^n b$ for $a, b \in k[x]$ to be determined. We need

$$\pi^n a h_n + \pi^n b g_n \equiv f - g_n h_n \mod \pi^{n+1}.$$

Dividing out by π^n, we find that we need to find $\bar{a}, \bar{b} \in k[x]$ satisfying

$$\bar{a}\overline{h} + \bar{b}\overline{g} = c \tag{1}$$

for $c = \frac{1}{\pi^n}(f - g_n h_n)$. Let P_n denote the k-vector space of polynomials of deg $\leq n$ in $k[x]$. The map

$$(a, b) \mapsto a\overline{h} + b\overline{g} : P_{d_g} \times P_{d_h} \to P_{d_g + d_h}$$

has kernel spanned by $(-\overline{g}, \overline{h})$, so is surjective by dimension count.

Hence (1) has a solution as desired. □

(This factorization is unique up to multiplication by elements of $\mathcal{O}^\times$).

Corollary 5.4. *If K is a field complete with respect to a discrete valuation ν and $f = a_n x^n + \cdots + a_0 x^0 \in K[x]$ is irreducible, then*

$$\min_{0 \leq i \leq n} \nu(a_i) = \min(\nu(a_n), \nu(a_0)).$$

Proof. WLOG $\min_{0 \leq i \leq n} \nu(a_i) = 0$ Assume by way of contradiction, let m be maximal with $\nu(a_m) = 0$. Then $f \in \mathcal{O}[x]$ and $\overline{f} \in k[x]$ has degree m with $0 < m < n$. Apply Hensel's lemma with $\overline{g} = \overline{f}$, $\overline{h} = 1$ to get that f has a factor of degree m. □

(Comment: there's a generalization known as Newton polygons.)

5.2 Extensions of absolute values

For the next while we're going to be considering the following question: let K be a field with absolute value $|\cdot|_K$, and L/K a finite extension. Can $|\cdot|_K$ be extended to an absolute value $|\cdot|_L$ on L? If so, in how many ways?

Proposition 5.5. *Let K be a field complete with respect to a discrete absolute value $|\cdot|_K$, and L/K a finite extension of degree n. Then there exists a unique extension of $|\cdot|_K$ to L given by $|a|_L = \sqrt[n]{|N_{L/K} a|_K}$, and L is complete with respect to the discrete absolute value $|\cdot|_L$.*

Remark. The norm map $N_{L/K}$ can be defined in a few different ways. We'll define it by

$$N_{L/K}(a) = \det m_a$$

where $m_a : L \to L$ is the map of K-vector spaces given by multiplication by a.

If $f(x) = x^m + \cdots + c_0 \in K[x]$ is the monic minimal polynomial of a, then the characteristic polynomial χ of m_a is given by $\chi(x) = f(x)^{n/m}$, where $n = [L : K]$. Hence we also have $N_{L/K}a = c_0^{n/m}$.

Proof. Existence: Only hard part is to check that $|a + b|_L \leq \max(|a|_L, |b|_L)$. For this wlog $a = 1$ and $|b|_L \leq |a|_L = 1$. Let $f(x) = x^n + c_{n-1}x^{n-1} \cdots + c_0$ be the minimal polynomial of x. Now, $|c_0|_K = |a|_L^m \leq 1$. By the lemma we then have that $\max_i(|c_i|_K) \geq \max(|1|_K, |c_0|_K) = 1$, so the minimal polynomial $f(x)$ of b lies in $\mathcal{O}_K[x]$. Then the minimal poly of $b + 1$ will also have coefficents in $\mathcal{O}[x]$, giving $|N_{L/K}(b + 1)| \in \mathcal{O}_K$ and

$$|b + 1|_L = \sqrt[n]{|N_{L/K}(b + 1)|_K} \leq 1$$

as desired.

To show uniqueness: analytic reasons: for any complete field K, any two norms on a finite-dimensional K-vector space induce the same topology. Then, two absolute values on a field L that give the same topology are equivalent. (HW).

This also gives completeness, since $L \cong K^n$ as vector spaces and K^n is complete in the max norm. □

6 September 24

6.1 More on extensions of valuations and ramification

Let L/K be a finite extension, with K complete with respect to a discrete absolute value $|\cdot|$; by last time, we know there is a unique extension of $|\cdot|$ to L, which we will denote by $|\cdot|$.

Some consequences: L is complete (because the metric on L is equivalent to the metric on K^n). Also if L/K is Galois, then any $g \in \mathrm{Gal}(L/K)$ fixes $|\cdot|$, that is $|ga| = |a|$ for all $a \in L$.

Now let $\mathcal{O}_K$ be the valuation ring of K, with maximal ideal $\mathfrak{p}_K = (\pi_K)$. Likewise let $\mathcal{O}_L$ be the valuation ring of L, with maximal ideal $\mathfrak{p}_L = (\pi_L)$.

Then the ideal $\pi_K\mathcal{O}_L$ must equal $(\pi_L\mathcal{O}_L)^e$ for some positive integer $e = e_{L/K}$. This e is also equal to the index

$$[|L^\times| : |K^\times|] = \left[\mathrm{im}(|\cdot| : L^\times \to \mathbb{R}^{>0}) : \mathrm{im}(|\cdot| : K^\times \to \mathbb{R}^{>0})\right],$$

since the former is generated by $|\pi_L|$ and the latter by $|\pi_K| = |\pi_L|^e$. The positive integer $e = e_{L/K}$ is known as the *ramification index* of L/K.

Additionally, define the *inertia degree* $f = f_{L/K}$ of L/K as the degree of the extension of residue fields $[\ell : k] = [\mathcal{O}_L/(\pi_L) : \mathcal{O}_K/(\pi_K)]$.

Example. $K = \mathbb{Q}_p$, p odd, $|a| = c^{v_p(a)}$, $c < 1$. $L = \mathbb{Q}_p(\sqrt{u})$ for $u \in \mathbb{Z}_p^\times$ not a square mod p and $\mathcal{O}_L = \mathbb{Z}_p[\sqrt{(u)}]$. Then $k = \mathbb{F}_p$, $\ell = \mathbb{F}_p[\sqrt{\overline{u}}]$ so $f = 2$. However $p\mathcal{O}_L$ is prime in $\mathcal{O}_L$, so $\pi_L = p = \pi_K$, and $e = 1$.

Can explicitly describe the absolute value on L by

$$|a + b\sqrt{u}|_L = \max(|a|_K, |b|_K) = c^{\min(v_p(a), v_p(b))}.$$

This is normalized with $c = 1/p^2$.

Example. $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p(\sqrt{p})$, $\mathcal{O}_L = \mathbb{Z}_p[\sqrt{p}]$. In this case $p\mathcal{O}_L = (\sqrt{p}\mathcal{O}_L)^2$, and $\sqrt{p}\mathcal{O}_L$ is prime with quotient $\mathcal{O}_L/\sqrt{p}\mathcal{O}_L \cong \mathbb{F}_p$, so $e = 2$, $f = 1$.

Can explicitly describe the absolute value on L here by

$$|a + b\sqrt{p}| = c^{\min(v_p(a), (1/2) + v_p(b)}.$$

Again, normalized when $c = 1/p^2$.

Up to this point, nothing we do requires that the extension L/K be separable. However, our proof of the next theorem does:

Theorem 6.1. *In the setting above, and assuming* L/K *is separable,* $ef = n = [L : K]$

Proof. The place where we need separability of L/K is to show that $\mathcal{O}_L$ is a finitely generated $\mathcal{O}_K$-module. It's a general theorem that if L/K is a finite separable extension, and $A \subset K$ is integrally closed Noetherian with $\operatorname{Frac} A = K$, then the integral closure B of A inside L is a finitely generated A-module. For a proof see https://stacks.math.columbia.edu/tag/032L – this proof uses nondegeneracy of the trace pairing, so separability is absolutely essential. This theorem applies here because, as you'll show on the HW, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L.

We compute $\dim_k(\mathcal{O}_L/\pi_K\mathcal{O}_L)$ in two different ways.

First of all, $\mathcal{O}_L$ is a finitely generated torsion-free $\mathcal{O}_K$-module, so it must be free of rank equal to $n = [L : K]$. Hence $\mathcal{O}_L/\pi_K\mathcal{O}_L$ is a free k-module of rank n.

Secondly, $\pi_K = \pi_L^e$, so $\dim_k(\mathcal{O}_L/\pi_K\mathcal{O}_L) = e \cdot (\dim_k(\mathcal{O}_L/\pi_L\mathcal{O}_L)) = e$.

Equating the two gives $ef = n$ as desired. □

Remark. Actually, this result still holds if L/K is inseparable, as long as L and K are still complete. See the discussion at the end of Neukirch II.6.

Corollary 6.2. *Let* K *be a local field with normalized absolute value* $\|\cdot\|_K$*, and* L *be any finite extension. Then* L *is a local field, and its normalized absolute value* $\|\cdot\|_L$ *is given by* $\|a\|_L = \|(N_{L/K}a)\|_K$.

Proof. We already know that $\|a\|_L = \|(N_{L/K}a)\|_K^{\delta}$ for some real δ, so it's enough to check that $\|\pi_K\|_L = \|N_{L/K}\pi_K\|_K$. The right hand side is $\|\pi_K\|_K^{[L:K]} = (\#k)^{-[L:K]}$. The left hand side is equal to $\|\pi_L\|_L^e = (\#\ell)^e = (\#k)^{-ef}$ so the two are equal as desired. □

Remark. There is also a conceptual proof using the Haar measure definition of the normalized absolute value, interpreting the norm as a determinant.

Next, we back off on the assumption that K and L are complete, and ask

Question. *Let K be a (possibly not complete) field with a discrete non-arch absolute value $|\cdot|$. If L/K a finite separable extension, can we extend $|\cdot|$ to L? Can we classify all such extensions?*

Important case: where $K = \operatorname{Frac} \mathcal{O}_K$, $\mathcal{O}_K$ Dedekind and our absolute value is of the form $|\cdot| = |\cdot|_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ in L. Let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}_K$ in L, and choose a prime factor $\mathfrak{p}'$ of $\mathfrak{p}\mathcal{O}_L$. Let e be the exponent of $\mathfrak{p}'$ in the factorization of $\mathfrak{p}\mathcal{O}_L$. Then for any $a \in K$ we have $v_{\mathfrak{p}'}(a) = ev_\mathfrak{p}(a)$. Hence, $|\cdot|_{\mathfrak{p}'}^e$ extends $|\cdot|_\mathfrak{p}$.

Theorem 6.3. *In the setting above, any absolute value $|\cdot|'$ on L extending $|\cdot|_\mathfrak{p}$ is equivalent to $|\cdot|_{\mathfrak{p}'}$ for some prime factor $\mathfrak{p}'$ of $\mathfrak{p}\mathcal{O}_L$.*

Proof. First we show that any absolute value $\|\cdot\|'$ extending $\|\cdot\|_\mathfrak{p}$ is non-archimedean and discrete. We do this by looking at completions: the completion $\hat{L}$ of L with respect to $\|\cdot\|'$ will be a finite extension of the completion $\hat{K}$ of K with respect to $\|\cdot\|_\mathfrak{p}$. By what we did last time, the absolute value on $\hat{L}$ extending the absolute value of $\hat{K}$ must be non-archimedean and discrete, so the same is true for $\|\cdot\|'$ on L.

Suppose that $|\cdot|'$ extends $|\cdot|_\mathfrak{p}$.

Then consider $\mathcal{O}_{L,|\cdot|'} = \{a \in L \mid \|a\|' \leq 1\}$; this is an integrally closed ring that contains $\mathcal{O}_K$, so contains $\mathcal{O}_L$. Let $\mathfrak{p}_{L,|\cdot|'} = \{a \in L \mid \|a\|' < 1\}$ be the maximal ideal of $\mathcal{O}_{L,|\cdot|'}$ and let $\mathfrak{p}' = \mathfrak{p}_{L,|\cdot|'} \cap \mathcal{O}_L$. Then $\mathfrak{p}'$ is a nonzero prime ideal of $\mathcal{O}_L$. Then the localization $(\mathcal{O}_L)_{\mathfrak{p}'}$ is contained in $\mathcal{O}_{L,|\cdot|'}$: since both are DVRs they must be equal.

□

Corollary 6.4. *If K is a number field, then any absolute value $|\cdot|$ on K must either come from an embedding $K \hookrightarrow \mathbb{R}$ or $\mathbb{C}$, or be of the form $|\cdot|_\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$.*

Proof. If $|\cdot|$ is archimedean, then the completion $\hat{K}$ of K with respect to $|\cdot|$ is a complete archimedean field, so it must be either $\mathbb{R}$ or $\mathbb{C}$.

Else $|\cdot|$ is non-archimedean. Then the restriction of $|\cdot|$ to $\mathbb{Q}$ must equal $|\cdot|_p$ for some p by Ostrowski's theorem. By the previous theorem, $|\cdot|$ must equal $|\cdot|_\mathfrak{p}$ for some prime $\mathfrak{p}'$ of $\mathcal{O}_K$ dividing $p\mathcal{O}_K$. □

Another approach: this time, drop all assumptions, let K and L be fields with L/K finite separable, let $|\cdot|_v$be an absolute value on K, and let $|\cdot|_v'$ be an absolute value on L extending $|\cdot|_v$. (You should think of v and v' as (possibly archimedean) places of K

and L respectively; this argument works just fine if $|\cdot|_v$, $|\cdot|_{v'}$ are archimedean absolute values).

Now let K_v be the completion of K with respect to $|\cdot|_v$ and $L_{v'}$ be the completion of L with respect to $|\cdot|_{v'}$. Then the compositum $K_vL \subset L_{v'}$ is a complete subspace of $L_{v'}$ containing L, so we have $K_vL = L_{v'}$.

Conversely, if L' is a field with inclusions

$$\begin{array}{ccc} K & \hookrightarrow & L \\ \downarrow & & \downarrow \\ K_v & \hookrightarrow & L'. \end{array} \tag{2}$$

such that $L' = LK_v$, then L' is a finite extension of K_v, so the absolute value $|\cdot|_v$ on K_v extends uniquely to an absolute value $|\cdot|_{L'}$ on L'. The restriction of this absolute value $|\cdot|_{L'}$ to L gives an absolute value on L that extends the absolute value $|\cdot|_v$ on K.

By this means we get a bijection

$$\{\text{absolute values on } L \text{ extending } |\cdot|_v\} \leftrightarrow \{\text{equivalence classes of compositum fields } L' = LK_v\}$$

where on the right hand side, the equivalence class is up to isomorphisms that commute with the maps in the diagram (3).

7 September 28

7.1 Extension of valuation and tensor products

Example. $K = \mathbb{Q}$, $v = v_3$, $L = \mathbb{Q}(\sqrt{7})$. Observe that $\mathbb{Q}_3$ already contains two square roots α_1 and $\alpha_2 = -\alpha_1$ of 7, where $\alpha_1 \equiv 1 \pmod 3$ and $\alpha_2 \equiv 2 \pmod 3$. Then there are two distinct compositum diagrams

$$\begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}(\sqrt{7}) \\ \downarrow & & \downarrow{\scriptstyle \phi_1} \\ \mathbb{Q}_3 & \xhookrightarrow{=} & \mathbb{Q}_3. \end{array} \qquad \begin{array}{ccc} \mathbb{Q} & \hookrightarrow & \mathbb{Q}(\sqrt{7}) \\ \downarrow & & \downarrow{\scriptstyle \phi_2} \\ \mathbb{Q}_3 & \xhookrightarrow{=} & \mathbb{Q}_3. \end{array} \tag{3}$$

where the two injections $\phi_1, \phi_2 : \mathbb{Q}(\sqrt{7}) \hookrightarrow \mathbb{Q}_3$ are determined by $\phi_i(\sqrt{7}) = \alpha_i$.

Proposition 7.1. *If K is a field, v a place of K and L/K is any finite extension, then*

$$K_v \otimes_K L = \prod_{v' \text{ extends } v} L_{v'}$$

Proof. This will follow from the previous discussion, plus the following fact of commutative algebra:

Proposition 7.2. *If L/K is a finite separable extension and K'/K is an arbitrary extension, then*

$$K' \otimes_K L = \prod_{L'=LK'} L'$$

where the right hand side is the product of all composita $L' = LK'$, up to isomorphism in the sense defined above (that is, the isomorphism must commute with the injections $L \hookrightarrow L'$ and $K' \hookrightarrow L'$).

Proof. By the theorem of the primitive element write $L = K(\alpha) = K[x]/(f(x))$ with $f(x)$ squarefree. Then

$$K' \otimes_K L = K'[x]/(f(x)) = \prod_i K'[x]/(f_i(x)).$$

where $f_1, \dots, f_r$ are the irreducible factors of f in $K'[x]$.

Hence, if we write $L_i' = K'[x]/f_i(x)$ for each we have that $K' \otimes_K L = \prod_i L_i'$ is a product of fields. Furthermore we have field homomorphisms

$$K', L \to K' \otimes_K L \to L_i'$$

which let us write each L_i' as a compositum LK'. And if we have any other compositum $L' = LK'$, then the multiplication map $L \times K \to L'$ gives a nonzero homomorphism $L \otimes K \to L'$ which must map some factor L_i' isomorphically to L'.

Finally, the factors L_i' are non-isomorphic (as composita; that is, equipped with the maps $K', L \to L_i'$) because the factors $f_i(x)$ are distinct. □

□

One explicit takeaway from the proof above is that, if $L = K(\alpha)$ with α having minimal polynomial f, then $K_v \otimes_K L = \prod_{f_i | f} K_v[x]/(f_i(x))$, and the fields $K_v[x]/(f_i(x))$ are the completion of L at the absolute values extending v.

Corollary 7.3. *If L/K is a finite extension and $\alpha \in L$ is arbitrary, then*

$$[L : K] = \sum_{v'} [L_{v'} : K_v],$$

$$N_{L/K}\alpha = \prod_{v'} N_{L_{v'}/K_v}\alpha$$

and

$$\mathrm{tr}_{L/K}\,\alpha = \sum_{v'} \mathrm{tr}_{L_{v'}/K_v}\,\alpha.$$

where all products run over the set of places v' extending v.

Proof. The first equality follows from taking dimensions of both sides in Proposition 7.1.

For the second, recall that $N_{L/K}a = \det(\times a : L \to L)$, where $\times a$ is the multiplication by a map viewed as a map of K-vector spaces. Extending scalars to K_v and applying Proposition 7.1, we obtain.

$$N_{L/K}a = \det(\times(a \otimes 1) : L \otimes_K K_v \to L \otimes_K K_v) = \prod_{v'} \det(\times a : L_{v'} \to L_{v'})$$

which is $\prod_{v'} N_{L_{v'}/K_v} a$ as desired.

The proof for the trace is simsiar. □

Corollary 7.4. *If K satisfies the product formula then so does any finite extension of K. In particular, all number fields and function fields satisfy the product formula.*

Proof. Combine Corollary 7.3 with Corollary 6.2. □

Remark. For the function field case, we've actually only shown that all finite separable extensions of $\mathbb{F}_q(t)$ have a product formula. However, for every function field K over $\mathbb{F}_q$ we can find a transcendental element $z \in K$ such that K is a separable (and necessarily finite) extension of $\mathbb{F}_q(z)$, so our proof does in fact apply to arbitrary function fields.

Example. $K = \mathbb{Q}$, $v = v_3$, $L = \mathbb{Q}(\sqrt{7})$. In $\mathbb{Q}_3$ the minimal polynomial $x^2 - 7$ factors as $(x-a)(x+a)$ for a square root a of 7 in $\mathbb{Q}_3$ (exists because Hensel's lemma). Then

$$\mathbb{Q}_3 \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{7}) \cong \mathbb{Q}_3[x]/(x-a) \oplus \mathbb{Q}_3[x]/(x+a) \cong \mathbb{Q}_3 \times \mathbb{Q}_3.$$

That is, there are two different valuations of $\mathbb{Q}[\sqrt{7}]$ extending v_3, and both give completion $\mathbb{Q}_3$.

Example. $K = \mathbb{Q}$, $v = v_3$, $L = \mathbb{Q}(\sqrt{3})$. The polynomial $x^2 - 3$ is irreducible in $\mathbb{Q}_3$, so

$$\mathbb{Q}_3 \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) \cong \mathbb{Q}_3[x]/(x^2-3)$$

is a field. Hence there is a unique extension of v_3 to $\mathbb{Q}[\sqrt{3}]$, and the completion is the ramified quadratic extension $\mathbb{Q}_3[x]/(x^2-3)$ of $\mathbb{Q}_3$.

Example. $K = \mathbb{Q}$, $v = v_3$, $L = \mathbb{Q}(\sqrt[3]{17})$.

On HW will show $\mathbb{Q}_3 \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{17}) \cong \mathbb{Q}_3 \times \mathbb{Q}_3(\omega)$ where ω is a cube root of unity, so there are two different extensions of absolute value, one unramified and the other ramified.

7.2 The decomposition group

We now review the definition of the decomposition group, which you may have already seen in the context of global fields, from the context of valuations. Note that in complete

fields primes/valuations do not split, so in that case the decompostion group is always everything.

Now let L/K be a finite Galois extension of arbitrary fields. Let v be a place of K, and v' a place of L extending v.

Definition. The decomposition group $D_{v'} = D_{v'}(L/K)$ is $\{g \in \mathrm{Gal}(L/K) \mid |ga|_{v'} = |a|_{v'}\}$ for all $a \in L$.

If we are in the following setting: K is the field of fractions of a Dedekind domain $\mathcal{O}_K$, $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L, and we have $v = v_{\mathfrak{p}}$ and $v' = v_{\mathfrak{p}'}$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$ and some prime $\mathfrak{p}'$ of $\mathcal{O}_L$ above $\mathfrak{p}$, then $D_{v'}$ is equal to the decomposition group $D_{\mathfrak{p}'} = \{g \in \mathrm{Gal}(L/K) \mid g\mathfrak{p} = \mathfrak{p}\}$. However this definition also makes sense for v archimedean).

Note that if K is complete, v' is the unique place of L extending v, so $D_{v'}(L/K) = \mathrm{Gal}(L/K)$. Also, if K_v and $L_{v'}$ are the completions of L and K respectively, then $D_{v'}(L/K) = D_{v'}(L_{v'}/K_v) = \mathrm{Gal}(L_{v'}/K_v)$.

In this setting, we define the decomposition field $Z = Z(v')$ as the subfield of L fixed by $D_{v'} \subset \mathrm{Gal}(L/K)$. Let v_Z be the restriction of v' to Z.

Proposition 7.5. *The place v' is the only place of L extending v_Z.*

Proof. The key fact we use here is

Proposition 7.6. *If L/K is a finite Galois extension and v a place of K, then $\mathrm{Gal}(L/K)$ acts transitively on the set of places on L extending v*

Sketch of proof of Proposition . By contradiction. Suppose v_0, v_1 extend v and lie in distinct Galois orbits.

Then one can show (this is a consequence of a more general fact called weak approximation, or if these are $\mathfrak{p}$-adic valuations can use CRT) that there exists $a \in K$ such that $|a|_{gv_0} > 1$ and $|a|_{gv_1} \leq 1$ for all $g \in \mathrm{Gal}(L/K)$.

Then

$$|N_{L/K}(a)|_v = |N_{L/K}(a)|_{v_0} = \prod_{g \in \mathrm{Gal}(L/K)} |ga|_{v_0} = \prod_{g \in \mathrm{Gal}(L/K)} |a|_{g^{-1}v_0} > 1$$

but the same argument gives $N_{L/K}(a) \leq 1$. □

We now apply Proposition 7.2 to the extension L/Z, and observe that $\mathrm{Gal}(L/Z) = D_{v'}$ fixes v', so v' must be the only place of L extending v_Z □

Note that the equality $\mathrm{Gal}(L_{v'}/K_v) \cong D_{v'}(L/K) = \mathrm{Gal}(L/Z)$, implies $Z = K_v \cap L$ (intersection inside $L_{v'}$). Then also: $Z_{v_Z} = K_v$ If v is non-archimedean, it follows that the residue field of Z is the same as K, and that the extension Z/K is unramified when you go from v to v_Z. (I didn't mention this last sentence in class.)

8 October 1

8.1 The inertia group

Definition. If L/K is a finite Galois extension with discrete valuations $v \in K$, $v' \in L$, and DVRs $\mathcal{O}_v$ $\mathcal{O}_{v'}$ with uniformizers π_K, π_L and residue fields k, ℓ, we define the *inertia subgroup* of $\mathrm{Gal}(L/K)$ by

$$I_{v'} = I_{v'}(L/K) = \{g \in \mathrm{Gal}(L/K) \mid v'(ga - a) > 0 \text{ for all } x \in \mathcal{O}_{v'}\}.$$

This is not the most enlightening way of stating the definition, though it generalizes better to give higher inertia groups. We'll give a couple of equivalent definitions.

First of all, $g \in I_{v'}$ if $ga \equiv a \pmod{\pi_L \mathcal{O}_{v'}}$ for all $a \in \mathcal{O}_{v'}$. Secondly, the subgroup $I_{v'}$ is the kernel of the map $D_{v'} \to \mathrm{Gal}(\ell/k)$. (Note that for this last thing to make sense we should assume ℓ/k separable.)

In fact,

Proposition 8.1. *In the above setting, assuming ℓ/k separable, the inertia group $I_{v'}$ fits into an exact sequence $1 \to I_{v'} \to D_{v'} \to \mathrm{Gal}(\ell/k) \to 1$.*

Proof. The only thing to check here is that $D_{v'} \to \mathrm{Gal}(\ell/k)$ is surjective. I've referenced this fact before (eg in discussions of Frob) but will prove it here for completeness.

First, we reduce to the case where $D_{v'} = \mathrm{Gal}(L/K)$, by replacing K with the decomposition field $Z_{v'}$ as necessary.

Pick $\overline{a}$ a generator of the extension ℓ/k, and lift to an element $a \in L$. It will be enough to show that for any $\overline{a'}$ in the Galois orbit of $\overline{a}$, there is some $g \in \mathrm{Gal}(L/K)$ such that the reduction $\overline{ga}$ of ga mod π_L is equal to $\overline{a'}$.

The element $a \in \mathcal{O}'_v$ satisfies the polynomial $h(x) = \prod_g (x - ga) \in \mathcal{O}_v[x]$, so $\overline{a}$ satisfies $\overline{h}(x) = \prod_g (x - \overline{ga}) \in k[x]$. The Galois conjugate $\overline{a'}$ must also be a root of $\overline{h}(x)$, so $\overline{a'}$ must equal $\overline{ga}$ for some $g \in \mathrm{Gal}(L/K)$. □

As a corollary, we have that for L/K an extension of complete disc valued fields, $|I_{v'}| = |\mathrm{Gal}(L/K)|/f_{L/K} = e_{L/K}$.

Let the *inertia field* $T(v')$ be the fixed field of $I_{v'}$.

Definition. Let L/K be a finite extension of complete fields. The extension L/K is unramified if and only if $e_{L/K} = 1$ and the residue field extension ℓ/k is separable, equivalently if $[L : K] = f_{L/K} = [\ell : k]$ and ℓ/k is separable.

(If L and K are local fields, then ℓ/k is automatically separable.)

Proposition 8.2. *Let L/K be a finite Galois extension of local fields. Then $T(v')$ is the maximal subextension of L that is unramified above v.*

Proof. We'll show that T/K is unramified, and that L/T is totally ramified ($f_{L/T} = 1$).

Let t be the residue field of T. Then we have $\mathrm{Gal}(L/T)$ mapping surjectively to $\mathrm{Gal}(\ell/t)$ by the previous proposition. The inertia group $\mathrm{Gal}(L/T) = I_{v'}$ acts as the identity on ℓ. Hence $\ell = t$, giving $f_{L/T} = 1$ and $e_{L/T} = [L : T] = |I_{v'}| = e_{L/K}$. Because e, f are multiplicative in towers have then $f_{T/K} = f_{L/K}$ and $f_{L/T} = 1$. □

8.2 Unramified extensions

Lemma 8.3. *Let L/K be a finite extension of complete discrete valued rings with DVRs $\mathcal{O}_L$, $\mathcal{O}_K$ respectively. Suppose $L = K(\alpha)$ and there exists $f(x) \in \mathcal{O}_K[x]$ such that $f(\alpha) = 0$ and the reduction $\bar{f}(x) \in k[x]$ is separable. Then L/K is unramified and $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.*

Proof. We may assume without loss of generality that $f(x)$ is the minimal polynomial of α. It follows by Hensel that $\bar{f}(x)$ is an irreducible polynomial of the same degree as f: if not we could lift to obtain a factorization of $f(x)$.

Then the reduction $\bar{\alpha} \in \ell$ of α is a root of $\bar{f}(x)$, so

$$[\ell : k] \geq [k(\bar{\alpha}) : k] = \deg(\bar{f}(x)) = \deg(f(x)) = [L : K]$$

but we alse know that $[\ell : k] = f_{L/K}$ divides L/K, hence the two are equal and L is unramified.

To show equality, use Nakayama's lemma. First, by the chain of equalities we have $k(\bar{\alpha}) = \ell$. Hence $\mathcal{O}_L = \mathcal{O}_K[\alpha] + \pi_L\mathcal{O}_L = \mathcal{O}_K[\alpha] + \pi_K\mathcal{O}_L$ since L/K is unramified. Additionally, $\mathcal{O}_L$ is finitely generated as an $\mathcal{O}_K$-module, because it is the integral closure of $\mathcal{O}_K$ in the finite separable extension L/K (HW). Hence we may apply Nakayama's lemma to the $\mathcal{O}_K$-submodule $\mathcal{O}_K[\alpha]$ of $\mathcal{O}_L$ to get $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ as desired. □

A converse to the lemma: if L/K is unramified, choose any primitive element $\bar{\alpha}$ of ℓ/k with min poly $\bar{f}(x)$. Choose any polynomial $f(x) \in \mathcal{O}_K[x]$ lifting $\bar{f}(x)$, and let α be a root of $f(x)$ lifting $\bar{\alpha}$. Then α satisfies the conditions of the lemma.

Example. $L = K(\zeta_m)$ for $(m, p) = 1$. Note specifically that if $k = \mathbb{F}_q$, then $K(\zeta_{(q^n-1)})$ is an unramified extension of degree $= n$.

Proposition 8.4. *For any local field K, there is a unique unramified extension of K of degree n for each positive integer n.*

Proof. Already have existence ($L = K(\zeta_{q^n-1})$): need uniqueness.

Given L and L' we will show that $L = L'$. Use the converse of Lemma 8.3 to write $L' = K(\alpha) \cong K[x]/f(x)$ where the reduction $\bar{f}(x) \in k[x]$ of the minimal polynomial f is separable. As in the proof of Lemma 8.3 we know that $\bar{f}(x)$ must be irreducible of degree $[L : K] = n$ by Hensel. Then, using the fact that the finite field k has a unique extension of degree n, we see that $\bar{f}(x)$ must have a root in the residue field ℓ of L. Hensel's lemma then gives that f also has a root in L. Hence $L' = K(\alpha) = K[x]/f(x)$ injects into L: since $[L' : K] = [L : K] = n$ they must be equal. □

By a similar argument, one can prove a bit more:

Proposition 8.5. *If L, L' are ramified extensions of K with residue fields ℓ, ℓ' respectively, any k-algebra homomorphism $\ell \to \ell'$ lifts to a unique K-algebra homomorphism $L \to L'$.*

(Note that homomorphisms of fields are injections.)

(A special case of this is that $\mathrm{Gal}(L/K)$ is canonically isomorphic to $\mathrm{Gal}(\ell/k)$.)

Categorically, this is saying that there is an equivalence of categories between (finite unramified extensions of K) and (finite extensions of k). In one direction the map takes an extension L to the residue field ℓ. The map in the other direction is harder to construct canonically; however it can be done using a construction known as *Witt vectors*.

9 October 5

9.1 Unramified extension, wrap-up

Corollary 9.1. *Every unramified extension of K is contained in $K(\zeta_m)$ for some m. All unramified extensions are Galois and abelian. The compositum of two unramified extensions is unramified. The maximal unramified extension K^{unr} of K is $\bigcup_{(m,p)=1} K(\zeta_m)$. If L is any finite separable extension of K and $f = f_{L/K}$ then the maximal subfield of L unramified over K is $T = K(\zeta_{q^f-1})$, and L/T is totally ramified.*

(One can also prove the fact about composita directly: e.g. see Proposition 7.2 and Corollary 7.3 in Chapter II of Neukirch ANT.)

Recall from last time than any finite Galois extension L/K of local fields has a unique intermediate field T such that L/T is totally ramified and T/K unramified, and T is the maximal unramified subextension of L/K. Likewise, any separable extension L/K of local fields has a unique maximal unramified subextension T/K.

We can realize T as $K(\zeta_{q^f-1})$ where q is the size of the residue field of K and $f = f_{L/K}$ is the inertia degree. Indeed, Hensel's lemma gives us that $X^{q^f} - X$ splits in L, so $K(\zeta_{q^f-1})$ sits inside L and has the same residue field as L, so $K(\zeta_{q^f-1})/K$ is unramified.

9.2 Totally ramified extensions

Suppose that L/K is a totally ramified extension of local fields with DVRs $\mathcal{O}_L$ and $\mathcal{O}_K$, and valuations v_L, v_K respectively. (It should be OK for L/K to be inseparable here: in fact totally inseparable implies totally ramified.) Choose uniformizers π_L, π_K of L, K respectively. We won't assume L/K Galois. Let $n = [L : K]$.

Proposition 9.2. *$L = K(\pi_L)$ and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.*

Proof. To show the first part, it's enough to show that $1, \pi_L, \ldots, \pi_L^{n-1}$ are linearly independent over K. But

$$\nu_L(\sum_{0 \le i < n} a_i \pi_L^i) = \min_{0 \le i < n} (i + n\nu_K(a_i)) \tag{4}$$

for $a_i \in L$, and so the sum can only be 0 if all terms are 0.

For the second part, write any $b \in L$ as $\sum_{0 \le i < n} a_i \pi_L^i$. Then $b \in \mathcal{O}_L$ if and only if all $\nu_K(a_i) \ge 0$. □

Definition. A polynomial $f = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ is an *Eisenstein polynomial* if it satisfies the conditions of the classical Eisenstein's irreducibility criterion $\nu_K(c_i) > 0$ for $i = 0, \ldots n-1$, but $\nu_K(c_0) = 1$.

Can check for any uniformizer π_L of L, the minimal polynomial $f(x)$ of π_L in $K[x]$ is an *Eisenstein polynomial*. Conversely, if $f \in K[x]$ is Eisenstein of degree n, then the extension $L = K(a) = K[x]/f(x)$ is totally ramified, with uniformizer a. To check this we just observe that

$$|a|_L = |\mathbb{N}_{L/K} a|^{1/n} = |(-1)^n c_0|_K^{1/n}$$

and $(-1)^n c_0$ is a uniformizer of $K[x]$.

Example. Let K be an arbitrary local field. Then the extension $L = K[\sqrt[m]{\pi_K}]$ is totally ramified, with uniformizer, $\pi_L = \sqrt[m]{\pi_K}$ satisfying the Eisenstein polynomial $x^m - \pi_K = 0$.

Example. Let $K = \mathbb{Q}_p$, and $L = \mathbb{Q}_p[\zeta_{p^r}]$. Then $\pi_L = \zeta_{p^r} - 1$. Exercise; the minimal polynomial of π_L is Eisenstein of degree $p^r - p^{r-1}$.

Digression on types of ramification: If L/K is a totally ramified extension of local fields of residue characteristic p, we say L/K is *tamely ramified* if $p \nmid [L : K]$ and L/K is *totally wildly ramified* if L/K is a power of p. For any totally ramified extension L/K we can find an intermediate field M where M/K is tamely ramified and L/M is totally wildly ramified. In the case where L/K is Galois M is the fixed field of the Sylow p-subgroup of $\mathrm{Gal}(L/K)$.

9.3 Multiplicative structure of $K^\times$:

Let K be a local field. Let $\mathcal{O} = \mathcal{O}_K$ be the corresponding DVR. Let k be the residue field, of characteristic p and cardinality q.

We have an exact sequence

$$1 \to \mathcal{O}_K^\times \to K \to^\nu \mathbb{Z} \to 1.$$

This splits, non-canonically. We can make a splitting by choosing a uniformizer $\pi \in K$ with $\nu(\pi) = 1$, and taking the map $\mathbb{Z} \to K$ given by $n \to \pi^n$.

The group $\mathcal{O}_K^\times$ has a filtration on it

$$U_n = \{a \in \mathcal{O}^\times \mid a \equiv 1 \pmod{\pi^n}\}$$

with $\bigcap_n U_n = \{1\}$.

Then $U_0 = \mathcal{O}_K^\times$, $U_0/U_1 \cong k^\times$ canonically, and for $n \geq 1$, $U_n/U_{n+1} \cong k^+$ non-canonically, with the isomorphism $k^+ \to U_n/U_{n+1}$ given by

$$a \mapsto [1 + a\pi^n].$$

We have an exact sequence

$$1 \to U_1 \to \mathcal{O}_K^\times \to k^\times \to 1.$$

As previously mentioned, Hensel's lemma gives us a canonical splitting: for any $\overline{a} \in k^\times$ there is a unique $a \in \mu_{q-1}(\mathcal{O}_K^\times)$ that reduces to a.

Observations:

Proposition 9.3. *a)* $U_n^p \subset U_{n+1}$ *for* $n \geq 1$.

b) If $(m, p) = 1$ *then* $a \mapsto a^m : U_n \to U_n$ *is bijective.*

Proof. a): this is because $U_n/U_{n+1} \cong k^+$ has exponent p.

b): For injectivity, suppose $a \in U_n$ and $a \neq 1$. Choose N maximal with $a \in U_N$, so $[a] \neq 1$ in U_N/U_{N+1}. Since $U_N/U_{N+1} \cong k^+$ has exponent p prime to m, we conclude $[a^m] \neq 1$ in U_N/U_{N+1}, so $a^m \neq 1$.

For surjectivity, apply Hensel's lemma to the polynomial $f(x) = x^m - b$ for any $b \in U_n$.

□

A corollary is that the only roots of unity in $U_1^\times$ can be of order a power of p.

10 October 12

10.1 Corollaries of last time

Proposition 10.1. U_1 *is a finitely generated abelian pro-p-group.*

Proof. $U_1 = \lim_{\leftarrow} U_1/U_n$. □

(one can show that any such is a (possibly infinite) direct sum of summands isomorphic to $(\mathbb{Z}/p^r)^+$ or $\mathbb{Z}_p^+$.)

Proposition 10.2. *If* K *is a local field, then* $(K^\times)^n$ *is both open and closed in* $K^\times$. *Likewise,* $(\mathcal{O}^\times)^n$ *is both open and closed in* $\mathcal{O}^\times$, *and* U_1^n *is both open and closed in* U_1.

Proof. We prove this for U_1^n; the other two cases then follow.

First, note if p is the residue characteristic of K, then $U_1^n = U_1^{p^{v_p(n)}}$ by Proposition 9.3, so it's enough to show this when $n = p^r$ (though the proof is the same in either case).

Now use (the Newton's method version) of Hensel's lemma on the polynomial $x^{p^r} - b$ with $a_0 = 1$ to show that for sufficiently large N (in particular $N > 2rv(p)$) any $b \in U_1(N)$ belongs to U_1^n. Hence U_1^n contains the open subgroup $U_1(N)$ of U_1, so is itself open, hence also closed. □

Corollary 10.3. *Any finite index subgroup of $\mathcal{O}_K^\times$, or of $K^\times$, is open.*

Proof. Any index n subgroup of $\mathcal{O}_K^\times$ contains $(\mathcal{O}_K^\times)^n$, hence is open. Likewise for $K^\times$. □

Proposition 10.4. *The open subgroups $\{(\mathcal{O}_K^\times)^n\}_{n\in\mathbb{Z}}$ form a neighborhood basis of $\mathcal{O}_K^\times$ (so also of $K^\times$) at the identity.*

Proof. Since $(\mathcal{O}_K^\times)^{q-1} = U_1$ (where q is the cardinality of the residue field), it's enough to show that the open subgroups $U_1^{p^r}$ form a neighborhood basis for $\mathcal{O}_K^\times$ at the identity. Repeated application of part a) Proposition 9.3 shows that $U_1^{p^r} \subset U_{r+1}$, and the result follows. □

10.2 Approaches to exponentiation in local fields

Let K be a local field of residue characteristic p. We want to define an exponential function for K that will make it easier to study the structure of the multiplicative group, analogously to the function $e^x : \mathbb{C}^+ \to \mathbb{C}^\times$. There are a few different approaches we could take to this

- We know how to exponentiate to integer powers: we have an exponentiation map $K^\times \times \mathbb{Z} \to K^\times$ given by $(a, n) \mapsto a^n$. We can try to extend this continuously to a map $K^\times \times \mathbb{Z}_p \to K^\times$. The problem here is that our original map is not continuous (using the p-adic topology on $\mathbb{Z}$). However, it is continuous on the open subgroup $U_1 \times \mathbb{Z}$, and so extends continuously to an exponential map $U_1 \times \mathbb{Z}_p \to U_1$: that is, we can define a^x for $a \in U_1$ and $x \in \mathbb{Z}_p$ by continuous extension.

  The shortcoming here is that we can only exponentiate to powers that are in $\mathbb{Z}_p$, not in the local field K. One advantage, though, is that this does work for function fields as well as number fields.

- We could try defining a function $e^x : K \to K$ as a solution to the differential equation $f' = f$. Taking derivatives in local fields is not a problem: define them as a limit. The problem is that solutions to differential equations in local fields are far from unique, because local fields are totally disconnected. The standard way to fix this is to require that e^x be analytic, that is, defined by a power series. Doing that leads to our third approach.

- Define e^x as the power series $\sum_{n\geq 0} \frac{x^n}{n!}$. Note that we're immediately in trouble if our field has characteristic p, but for local fields of characteristic 0 this power series has positive radius of convergence and we'll use it.

Remark. If K is a function field of characteristic p, then $\mathcal{O}_K^+$ and $\mathcal{O}_K^\times$ actually look very different as abelian groups and we won't have much luck finding an exponential function to relate them. For instance,

$$\mathbb{F}_p[[t]]^+ \cong \mathbb{F}_p^{\mathbb{N}}$$

as abelian groups (and in particular has exponent p) while

$$\mathbb{F}_p[[t]]^\times \cong (\mathbb{Z}/(p-1)\mathbb{Z})^+ \times \mathbb{Z}_p^{\mathbb{N}}$$

has no p-torsion.

10.3 p-adic exponential and logarithm

Suppose K is a local field of characteristic 0 and residue characteristic p. Let $\mathcal{O}_K$ be the ring of integers of K. Let π be a uniformizer and let v be the valuation of K, so $v(\pi) = 1$ Let e be the ramification degree of $K/\mathbb{Q}_p$, giving us $p\mathcal{O}_K = (\pi^e)$ and $v(p) = e$. We define a power series

$$\exp_p(x) = \sum_{n\geq 0} \frac{x^n}{n!} \in K[[x]].$$

Exercise: this power series converges provided $v(x) > e/(p-1)$. (The key fact here is that $v_p(n!) = \frac{n-s(n)}{p-1}$, where s_n is the sum of the base p digits of n.)

Can also define

$$\log_p(1+z) = \sum_{n\geq 1} \frac{(-1)^{n+1} z^n}{n}.$$

Exercise: this converges for $1 + z \in U_1$.

Proposition 10.5. *for any* $n > e/(p-1)$ *have* $\exp_p : (\pi)^n \to U_n$ *and* $\log_p : U_n \to (\pi)^n$ *inverse homomorphisms.*

Sketch. We know these are inverses as power series, so it is enough to check that $\exp_p$ maps π^n to U_n and vice versa. This can be done by bounding the p-adic valuation of each term. □

Note that $\log_p : U_1 \to K^+$ is a homomorphism wherever it's defined, however it generally fails to be injective and so doesn't have an inverse function. For instance, if $p = 2$, we know that $\log_2(-1) + \log_2(-1) = \log_2(1) = 0$, so $\log_2(-1) = 0 = \log_2(1)$ giving us a failure of injectivity.

Corollary 10.6. $\mathbb{Z}_p^\times = \mu_p \times U_1 \cong (\mathbb{Z}/(p-1)\mathbb{Z})^+ \times \mathbb{Z}_p^+$ *as abelian groups for* p *odd.*
$\mathbb{Z}_2^\times = \mu_2 \times U_2 \cong (\mathbb{Z}/2\mathbb{Z})^+ \times \mathbb{Z}_p^+$

Proof. For the first part: $e/(p-1) = 1/(p-1) < 1$, so the propostion tells us that $U_1 \cong p\mathbb{Z}_p \cong \mathbb{Z}_p^+$ as abelian groups. We've already shown the rest.

For the second, easy to check that $\mathbb{Z}_2^\times = \mu_2 \times U_2$, and $e/(p-1) = 1 < 2$ so $U_2 \cong 4\mathbb{Z}_2 \cong \mathbb{Z}_2^+$.

□

General local fields of characteristic 0 we can still use the short exact sequence $0 \to U_n \to U_1 \to U_1/U_n \to 0$. When $n > e/(p-1)$, the first term is isomorphic to $\mathcal{O}_K^+ \cong \mathbb{Z}_p^n$ as a topological group. The last term is a finite abelian p-group; but this sequence in general doesn't split.

10.4 The Artin map for unramified extensions

We've previously asserted:

If L/K is a finite abelian extension, then there is an isomorphism

$$\mathrm{Gal}(L/K) \cong K^\times / NL^\times.$$

We'll verify this when L/K is unramified of degree n.

We know already that $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k) \cong (\mathbb{Z}/n\mathbb{Z})^+$, where we can give an explicit isomorphism by sending the Frobenius element to $[1] \in \mathbb{Z}/n\mathbb{Z}$.

Let $v : K^\times \to \mathbb{Z}$ be the discrete valuation: since L/K is unramified, this extends to a valuation $v : L^\times \to \mathbb{Z}$. If $a \in L$, then

$$v(Na) = \sum_{g \in \mathrm{Gal}(L/K)} v(ga) = nv(a).$$

As a result we have the exact sequence

$$1 \to \mathcal{O}_K^\times / N(\mathcal{O}_L^\times) \to K^\times / NL^\times \to^v (\mathbb{Z}/n\mathbb{Z})^+ \to 1.$$

If we can show that $N : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective, we'll have that $K^\times/NL^\times \cong (\mathbb{Z}/n\mathbb{Z})^+$ as needed.

Let π be a uniformizer of K; that is, $v(\pi) = 1$. Note that π is also a uniformizer of L because L/K is unramified.

Recall that the unit groups $\mathcal{O}_K^\times$ and $\mathcal{O}_L^\times$ have filtrations

$$U_{K,i} = \{a \in \mathcal{O}_K^\times \mid a \equiv 1 \pmod{\pi^i \mathcal{O}_K}\}$$

and

$$U_{L,i} = \{a \in \mathcal{O}_L^\times \mid a \equiv 1 \pmod{\pi^i \mathcal{O}_L}\}$$

for $n \geq 0$.

Observe that N maps $U_{L,i}$ to $U_{K,i}$.

Lemma 10.7. *For every non-negative integer i, the map $N : U_{L,i}/U_{L,i+1} \to U_{K,i}/U_{K,i+1}$ is surjective.*

Proof. Case 1: $i = 0$ Then we have $U_{L,0}/U_{L,1} \cong \ell^\times$, $U_{K,0}/U_{K,1} \cong k^\times$. The result then follows from the HW problem saying that $N : \ell^\times \to k^\times$ is surjective.

Case 2: $i \geq 1$ Then we have $U_{L,i}/U_{L,i+1} \cong \ell^+$, $U_{K,i}/U_{K,i+1} \cong k^+$. The result then follows from the HW problem saying that $\mathrm{tr} : \ell^+ \to k^+$ is surjective. □

11 October 15

11.1 Finishing off the unramified Artin map

Now we put the pieces together to show that

Proposition 11.1. $N : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ *is surjective.*

Proof. Enough to show that $N : U_{L,0}/U_{L,i} \to U_{K,0}/U_{K,i}$ is surjective for all i. (Technical point that I didn't state in class: this is enough because, for any $a \in U_{K,0}$, the sets $C_i = \{b \in U_{L,0} \mid Nb \in aU_{K,i}\}$ are closed and nonempty, so their intersection is nonempty by compactness).

We induct on i: we've just shown the case $i = 1$. Now assume that $N : U_{L,0}/U_{L,i} \to U_{K,0}/U_{K,i}$ is surjective. Then we can sandwich the map $N : U_{L,0}/U_{L,i+1} \to U_{K,0}/U_{K,i+1}$ as follows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & U_{L,i}/U_{L,i+1} & \longrightarrow & U_{L,0}/U_{L,i+1} & \longrightarrow & U_{L,0}/U_{L,i} & \longrightarrow & 1 \\ & & \downarrow N & & \downarrow N & & \downarrow N & & \\ 1 & \longrightarrow & U_{K,i}/U_{K,i+1} & \longrightarrow & U_{K,0}/U_{K,i+1} & \longrightarrow & U_{K,0}/U_{K,i} & \longrightarrow & 1 \end{array}$$

where we know that the leftmost vertical map is surjective, and by induction the rightmost vertical map is surjective, so the middle map must also be surjective.

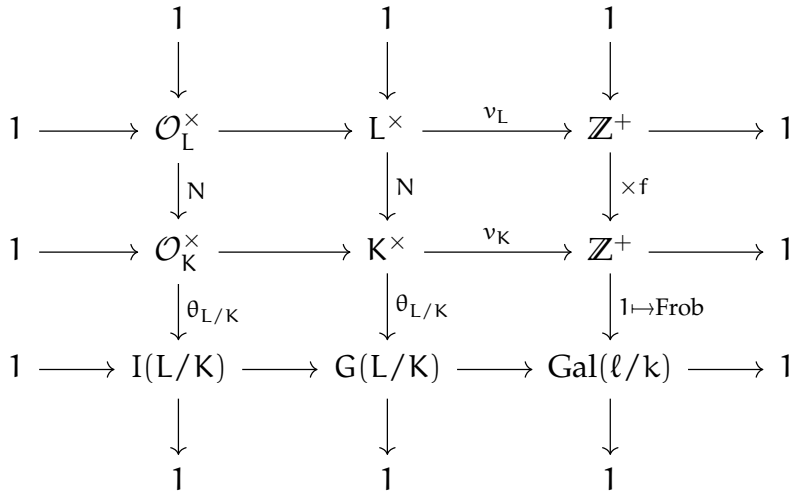
□

We now conclude that, $L^\times/NK^\times \cong (\mathbb{Z}/n\mathbb{Z})^+$ for $n = [L : K] = [\ell : k]$, so we define the Artin map $\theta_{L/K}$ to be the composition

$$L^\times/NK^\times \to (\mathbb{Z}/n\mathbb{Z})^+ \xrightarrow{1 \mapsto \mathrm{Frob}} \mathrm{Gal}(\ell/k) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

which we now know is an isomorphism.

Looking ahead, we'll later show that for any abelian extension L/K of local fields with inertia degree $f = f_{L/K}$, the local reciprocity map $\theta_{L/K}$ fits into a commutative diagram



where we have already defined all maps except for the two labeled $\theta_{L/K}$, and all horizontal and vertical sequences are short exact.

11.2 Ramification groups

Let L/K be an extension of fields with valuations v, v' and valuation rings $\mathcal{O}_v$, $\mathcal{O}_{v'}$. Then define

Definition. The ith ramification group $G_{i,v'}(L/K)$ is

$$G_{i,v'} = G_{i,v'}(L/K) = \{g \in D_{v'}(L/K) \mid v'(ga - a) > i \text{ for all } a \in \mathcal{O}_{v'}\}.$$

Have $G_{0,v'} = I_{v'}(L/K)$. For $N \gg 0$ have $G_{N,v'} = \{1\}$.

The condition $v'(ga - a) > i$ is equivalent to $ga \equiv a \pmod{\pi_L^{i+1}}$. So $g \in D_{v'}$ lies in $G_{i,v}$ if and only if g induces the trivial automorphism of the ring $\mathcal{O}_{v'}/(\pi_L^{i+1})$.

Here L and K needn't be complete fields, but as before, if $L_{v'}$, K_v are the completions of L, K respectively, we have $G_{i,v'}(L/K) = G_{i,v'}(L_{v'}/K_v)$.

For the rest of this, then, we'll assume L and K nonarchimedean local fields; write $v' = v_L$ and $v = v_K$, $\mathcal{O}_{v'} = \mathcal{O}_L$ and $\mathcal{O}_v = \mathcal{O}_K$, and drop the subscript v', so

$$G_i(L/K) = \{g \in \mathrm{Gal}(L/K) \mid v_L(ga - a) > i \text{ for all } a \in \mathcal{O}_L\}.$$

As before, this is the same as saying that $g \in \mathrm{Gal}(L/K)$ acts trivially on the ring $\mathcal{O}_L/(\pi_L^{i+1})$. To check this it's enough to check that g preserves a generator. As a result, we get that

If $\mathcal{O}_L = \mathcal{O}_K[a_0]$ then

$$\{G_i(L/K) = \{g \in \mathrm{Gal}(L/K) \mid v_L(ga_0 - a_0) > i\}. \tag{5}$$

In fact,

Proposition 11.2. *For* $i \geq 0$

$$\begin{aligned} G_i(L/K) &= \{g \in I(L/K) \mid v_L(g\pi_L - \pi_L) > i\} \\ &= \{g \in I_{v'}(L/K) \mid g\pi_L \equiv \pi_L \pmod{\pi_L^{i+1}}\}. \end{aligned} \tag{6}$$

Proof. We first reduce to the case where L/K is totally ramified. (Otherwise, replace K with the inertia field $T(v')$.)

By Proposition 9.2, have $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, so this now follows from (5). □

Now, for each $i \geq 0$, we can define a map

$$\phi_i : G_i(L/K)/G_{i+1}(L/K) \hookrightarrow U_{L,}/U_{L,i+1}$$

given by $g \mapsto [g\pi_L/\pi_L]$. This is a well-defined injection by Proposition 11.2.

The map ϕ_i may look non-canonical, but actually it doesn't depend on the choice of π_L! Indeed, if we replace π_L by $u\pi_L$ for $u \in \mathcal{O}_L^\times$, will multiply the quotient by $gu/u \in U_{L,i+1}$. Exercise: ϕ_i is a group homomorphism.

Recall that for $i = 0$ have $U_{L,0}/U_{L,1} \cong \ell^\times$ canonically, and for $i > 0$ have $U_{L,}/U_{L,i+1} \cong \ell^+$ non-canonically.

If ℓ has characteristic p, then this means that $I(L/K)/G_1(L/K) = G_0(L/K)/G_1(L/K)$ is cyclic of order prime to p, whereas all $G_i(L/K)/G_{i+1}(L/K)$ are abelian p-groups – hence $G_1(L/K)$ is a p-group. In particular, it is the Sylow p-subgroup of $I(L/K)$.

The group $I(L/K)/G_1(L/K)$ is called the *tame inertia group* of L/K and $G_1(L/K)$ is called the *wild inertia group* of L/K. If the wild inertia group G_1 vanishes, then L/K is called *tamely ramified*. This happens if and only if the order $e_{L/K}$ of $I(L/K)$ is relatively prime to p. Note that the condition $(e_{L/K}, p) = 1$ makes sense even if L/K is not Galois: we will say that an arbitrary finite extension L/K is *tamely ramified* if $(e_{L/K}, p) = 1$.

Example. $K = \mathbb{Q}_2$, $L = \mathbb{Q}_2(\zeta_8)$, $\pi_L = \zeta_8 - 1$.

$$\mathrm{Gal}(L/K) = \{g_1, g_3, g_5, g_7\} \cong \mathbb{Z}/8\mathbb{Z}^\times.$$

Here g_i is the element of $\mathrm{Gal}(L/K)$ sending $\zeta_8 \to \zeta_8^i$.

$$\begin{aligned} v_L(g_1\pi_L - \pi_L) &= \infty \\ v_L(g_3\pi_L - \pi_L) &= v_L(\zeta_8 - \zeta_8^3) = 2 \\ v_L(g_5\pi_L - \pi_L) &= v_L(2\zeta_8) = 4 \\ v_L(g_7\pi_L - \pi_L) &= v_L(\zeta_8 - \zeta_8^7) = 2 \end{aligned}$$

So $G_0 = G_1 = \mathrm{Gal}(L/K)$, $G_2 = G_3 = \{g_1, g_5\}$ and $G_4 = G_5 = \cdots = \{g_1\}$.

11.3 Tamely ramified extensions

Let K a local field with residue characteristic p. As noted above, we say that a finite extension of L/K is tamely ramified if $e_{L/K}$ is relatively prime to p. Note that in particular unramified extensions are tamely ramified – being tamely ramified just means that any ramification that happens must be tame.

We won't show this, but the class of tamely ramified extension is a nice class; it's preserved under composita and Galois closures. Hence for any finite extension L/K we can talk about the maximal tamely ramified subextension of L. If L/K is unramified, the maximal tamely ramified subextension is the fixed field of the inertia group $G_1(L/K)$. (See Chapter 1 of Cassels + Fröhlich for more on this)

Theorem 11.3. *Let* L/K *be a tamely ramified extension of residue field characteristic* p*. Then* L/K *is contained in the extension* $K(\zeta_m, \sqrt[e]{\pi_K})$ *for some* m, e *with* $(m, p) = (e, p) = 1$.

Proof. Let T be maximal unramified subextension of L/K. Then L/T is totally ramified of degree e relatively prime to p, so $L = T(\sqrt[e]{\pi'})$ for some other uniformizer π'. Then $L \subset T(\sqrt[e]{\pi'/\pi_K}, \sqrt[e]{\pi_K})$. But $T(\sqrt[e]{\pi'/\pi_K})$ is an unramified extension of K, so is contained in some $K(\zeta_m)$, and we're done. □

11.4 Upper numbering

One more comment: the indexing we've given for the inertia groups has the awkward feature that if $K \subset L \subset L'$ is a tower of fields, there is no relation between $G_i(L'/K)$ and $G_i(L/K)$ (because the two groups are using valuations that have been normalized differently). This is particularly inconvenient if you want to define ramification groups for an infinite extension.

(On the other hand, we do have $G_i(L'/L) = G_i(L'/K) \cap \mathrm{Gal}(L'/L)$.)

One can fix this problem as follows.

Define a function ϕ on $[0, \infty)$ by

$$\phi(u) = \int_0^u \frac{dt}{[G_0(L/K) : G_t(L/K)]}.$$

The function ϕ is the integral of a positive piecewise constant function, so it is piecewise linear and increasing.

Define

$$G^i(L/K) = G_{\phi^{-1}(i)}(L/K).$$

Results that we won't prove here: Herbrand's theorem says that $G^i(L'/K)$ restricts to $G^i(L/K)$. Another important theorem is Hasse-Arf: when L/K is abelian, the jumps in filtration occur at integers. We'll ultimately be able to show that the reciprocity map of class field theory maps $U_i(K) \to G^i(L/K)$.

In our example before of $K = \mathbb{Q}_2$, $L = \mathbb{Q}_2(\zeta_8)$, one can check that $\phi(0) = 0$, $\phi(2) = 2$, $\phi(4) = 3$, and ϕ connects those points piecewise-linearly. As a result, have $G^0 = G_0$, $G^2 = G_2$ and $G^3 = G_4$ are the points where the filtration jumps.

12 October 19

12.1 Group and Galois cohomology: references

Moving on to the next unit of this class: Galois cohomology. Cassels and Fröhlich and Serre's book *Local Fields* are the classic references. Neukirch's book *Class Field Theory: the Bonn Lectures* is a good reference on the material (Neukirch's Algebraic Number Theory only does the minimum necessary amount of cohomology needed to do class field theory, so it's not an adequate reference.) Milne's notes are also good here.

If you want to see group cohomology done in the general context of Ext groups, Dummit and Foote (more elementary) and Weibel's Introduction to Homological Algebra (more advanced) are also good references.

12.2 The category of G-modules

Let G be a group. Then a G-module A is an abelian group with a left action of G preserving the abelian group structure ($g(a+b) = ga + gb$). That is, it's like a representation of G, but on a group rather than a vector space.

As one does for representations, define the morphisms by

$$\mathrm{Hom}_G(A, B) = \{\phi \in \mathrm{Hom}_{\mathbb{Z}}(A, B) \mid g\phi(a) = \phi(ga) \text{ for all } a \in A\}$$

Example. Let $G = \mathrm{Gal}(L/K)$. Then L^+, $L^\times$, $\mu_n(L)$, $\mathcal{O}_L^\times$, $\mathrm{Cl}(L)$, $\mathbb{A}_L^\times$, $\mathbb{G}(L)$ for $\mathbb{G}$ any commutative algebraic group over K, eg $E(L)$ for E an elliptic curve, are all G-modules.

Example. Let G be any group. Then any abelian group A is a G-module with trivial G action, e.g. $A = \mathbb{Z}$.

Definition. The *group ring* $\mathbb{Z}[G]$ is the ring of all formal linear combinations $\sum_{a_g} g$ with addition and multiplication done formally.

Example. If $G = C_n = \langle t \mid t^n = 1\rangle$ then $\mathbb{Z}[G] = \mathbb{Z}[t]/(t^n - 1)$. (This is not $\mathbb{Z}[\zeta_n]$, though it has that ring as a quotient.)

Observe that G-modules are the same thing as $\mathbb{Z}[G]$-modules. In particular, $\mathbb{Z}[G]$ is a G-module.

Definition. The augmentation map is the G-module homomorphism $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ defined by $\epsilon(\sum c_g g) = \sum c_g$. The *augmentation ideal* $I_G \subset \mathbb{Z}[G]$ is equal to $\ker \epsilon$.

As a $\mathbb{Z}$-module I_G is free, with basis $(g-1)$ for $g \in G, g \neq 1$. In the case $G = C_n$ we have $I_G = (t-1)$, however in general I_G is not principal.

When G is finite, the group ring $G[\mathbb{Z}]$ contains a special element

$$N = \sum_{g \in G} g.$$

. Notation here is because if $G = \mathrm{Gal}(L/K)$, $A = L^\times$ treated as a G-module, then N acts as the norm $Na = N_{L/K}(a)$. Note though that if instead $A = L^+$, then N acts as the trace $Na = \mathrm{tr}_{L/K}\, a$.

The category of G-modules is an abelian category: that is to say, you can do all the constructions of kernels, images, quotients, direct sums, etc, in it. A couple more operations in the category of G-modules:

For A and B, G-modules, can put a G-module structure on $\mathrm{Hom}(A,B) = \mathrm{Hom}_{\mathbb{Z}}(A,B)$, where the action is $g\phi = g \circ \phi \circ g^{-1}$. Note that this is not the same as the set $\mathrm{Hom}_G(A,B)$ of G-module homomorphisms from A to B. Also, can put a G-module structure on $A \otimes B = A \otimes_{\mathbb{Z}} B$, by $g(a \otimes b) = ga \otimes gb$. (Notational convention: when we drop the subscript on Hom or $\otimes$ the ring is assumed to be $\mathbb{Z}$.)

Now we write down some functors from G-modules to $\mathbb{Z}$-modules.

Definition. For A a G-module, the group of *invariants* of A is

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

The group of *co-invariants* of A is

$$A_G = A/I_G A.$$

The group A_G can also be expressed as the quotient of A by all elements of the form $ga - a$.

Just as A^G is the maximal submodule of A on which G acts trivially, A_G is the maximal quotient of A on which G acts trivially.

We note now that for any G-module B, $\mathrm{Hom}_G(B,-)$ gives a functor from G-modules to $\mathbb{Z}$-modules. In the special case of $B = \mathbb{Z}$ with trivial G-action, have $\mathrm{Hom}_G(\mathbb{Z},A) = A^G$, so this generalizes the functor of invariants.

Similarly, the functor of coinvariants is a special case of the tensor product functor. However, defining the tensor product $A \otimes_G B$ is is a little subtle as $\mathbb{Z}[G]$ is noncommutative. In general if R is a non-commutative ring can only define $A \otimes_R B$ if A is a right R-module and B is a left R-module, and this is only an abelian group. We can make any G-module A into a right $\mathbb{Z}[G]$-module using the action $r(g)a = g^{-1}a$.

As a result the tensor product $A \otimes_G B$ is defined as the quotient of $A \otimes_{\mathbb{Z}} B$ by all relations of the form $g^{-1}a \otimes b - a \otimes gb$. This only has the structure of a $\mathbb{Z}$-module (because $\mathbb{Z}[G]$ is noncommutative.)

So for any B we get another functor $B \otimes -$ from G-modules to $\mathbb{Z}$-modules. In the case where $B = \mathbb{Z}$, we recover the functor of coinvariants: $\mathbb{Z} \otimes_G A = A_G$.

Two more identities: $\mathrm{Hom}_G(A, B) = \mathrm{Hom}(A, B)^G$ and $A \otimes_G B = (A \otimes B)_G$.

Now we will consider the exactness of these functors. The functor $A \mapsto A^G$ is left exact but not exact. That is, if

$$0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0$$

is an exact sequence, we have an exact sequence

$$0 \to A^G \xrightarrow{\phi} B^G \xrightarrow{\psi} C^G.$$

To verify this: if ϕ is injective, then so is its restriction to A^G. For exactness at the middle, note that if $b \in B^G$ has $\psi(b) = 0$, then exactness of the original sequence gives the existence of some $a \in A$ with $\phi(a) = b$. Furthermore, this a is unique by injectivity of ϕ. But $\phi(ga) = gb = b$ for any $g \in G$, so uniqueness implies $a \in A^G$, giving the required exactness.

More generally, for any G-module B, the functor $\mathrm{Hom}_G(B, -)$ is left-exact; the proof is similar.

Also, the functor $A \mapsto A_G$ is right-exact. Again, this is a special case of the functor $B \otimes_G -$ being right exact. The proofs of these are a bit more involved and we leave them as an exercise. One approach is to use the adjoint functor theorem: the tensor product functor $B \otimes_G - :$ G-mod $\to \mathbb{Z}$-mod is left adjoint to $\mathrm{Hom}(B, -) : \mathbb{Z} - \mathrm{mod} \to G - \mathrm{mod}$:

$$\mathrm{Hom}_{\mathbb{Z}}(B \otimes_G A, C) = \mathrm{Hom}_G(A, \mathrm{Hom}_{\mathbb{Z}}(B, C))$$

Example. To show $A \mapsto A^G$ is not an exact functor: $G = C_2 = \{1, t\}$. Let χ be the character $\chi : G \to \pm 1$ with $\chi(t) = -1$. Define a G-module $\mathbb{Z}_\chi$ which is $\mathbb{Z}$ as an abelian group, and on which g acts by $ga = \chi(g)a$.

Then there is an exact sequence

$$0 \to \mathbb{Z}_\chi \xrightarrow{\times 2} \mathbb{Z}_\chi \to \mathbb{Z}/2 \to 0.$$

The invariants of this sequence are

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

is not exact at $\mathbb{Z}/2$

The coinvariants are:

$$0 \to \mathbb{Z}/2 \xrightarrow{\times 2} \mathbb{Z}/2 \xrightarrow{\sim} \mathbb{Z}/2 \to 0$$

is not exact at the first $\mathbb{Z}/2$.

Example. A number-theoretic example:

Let L/K be a ramified quadratic extension of local fields (though any degree works), eg $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$.

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

is an exact sequence of $G = \mathrm{Gal}(L/K)$ modules but the invariants are

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

which is not exact at $\mathbb{Z}$ by definition of ramification.

A few more properties that modules can have: We say that a G-module is free if it is the direct sum of copies of $\mathbb{Z}[G]$.

If F is free then $\mathrm{Hom}_G(F, -)$ is exact (F is projective). Equivalently, for any surjection $\pi : B \twoheadrightarrow C$, and any $\phi : F \to C$ there is a lifting $\tilde{\phi} : F \to B$.

Also, $F \otimes_G -$ is exact (F is flat).

If A is any G-module, there exists a surjection $F \to A$ where F is a free G-module (this category has "enough projectives" – it also has "enough injectives", but we won't need that)

13 October 22

13.1 Co-induced and induced modules

Definition. For an abelian group X define the G-module $\mathrm{coInd}^G(X)$ to equal $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)$ as abelian groups with G acting as $g\phi(b) = \phi(bg)$ (this is not the standard action on $\mathrm{Hom}(\mathbb{Z}[G], X)$).

Define the G-module $\mathrm{Ind}^G X$ to equal $\mathrm{Ind}^G(X) = \mathbb{Z}[G] \otimes X$ as abelian groups. Here the G-action is the standard one: $g(b \otimes x) = gb \otimes x$.

We say that A is induced if it is of the form $\mathrm{Ind}^G(X)$ for some X. and likewise A is coinduced if it is of the form $\mathrm{coInd}^G(X)$.

When G is finite, these conditions are equivalent to each other, and there exists a sub-$\mathbb{Z}$-module $X \subset A$ such that $A \cong \bigoplus_{g \in G} gX$.

Example. L/K a finite extension. Then, to show that L^+ is a (co)induced $\mathrm{Gal}(L/K)$-module, it's enough to find an element $a \in L$ such that $\{ga \mid g \in \mathrm{Gal}(L/K)\}$ is a basis for L as a K-vector space.

The normal basis theorem says this is always the case. (See http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/linearchar.pdf for a proof.)

(Side question: if L is a local or a global field, you can ask when $\mathcal{O}_L$ is an induced $\mathrm{Gal}(L/K)$-module. This is a more delicate question: sometimes it is, sometimes not. You might enjoy working out the answer when L is a quadratic extension of $\mathbb{Z}$.)

"Baby Frobenius reciprocity:"

$$\mathrm{Hom}_G(B, \mathrm{coInd}^G(X)) \cong \mathrm{Hom}_{\mathbb{Z}}(B, X) \tag{7}$$

$$\mathrm{Hom}_G(\mathrm{Ind}^G(X), B) \cong \mathrm{Hom}_{\mathbb{Z}}(X, B). \tag{8}$$

(That is, coInd is the right adjoint of the forgetful functor from G-modules to $\mathbb{Z}$-modules, and Ind is the left adjoint.)

Every G-module A injects into a co-induced G-module: take $\mathrm{Hom}(G, A)$, then $a \mapsto \phi_a$ where $\phi_a(g) = ga$.

Also every G-module has a surjection from an induced G-module: take $\mathbb{Z}[G] \otimes A$, with map given by $(g, a) \mapsto ga$.

13.2 Group cohomology as derived functor

Now want to define the group cohomology functors $H^i(G, A)$ for $i \geq 1$. We will do this by giving a list of axioms they satisfy and showing that those specify a unique functor.

Theorem 13.1. *There is a unique family of functors $H^i(G, -) : G\text{-mod} \to \mathbb{Z}\text{-mod}$, $i \geq 0$ such that*

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

(ii) Any short exact sequence $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$ *of G-modules induces a long exact sequence*

$$\begin{array}{l} 0 \longrightarrow H^0(G,A) \xrightarrow{i_*} H^0(G,B) \xrightarrow{j_*} H^0(G,C) \xrightarrow{\delta} \\ \quad H^1(G,A) \xrightarrow{i_*} H^1(G,B) \xrightarrow{j_*} H^1(G,C) \xrightarrow{\delta} \\ \quad H^2(G,A) \longrightarrow \cdots \end{array}$$

(iii) $H^i(G, A) = 0$ *for $i \geq 1$ if A is coinduced.*

Proof. First we show existence. To do this, we will first choose a resolution of $\mathbb{Z}$ by free G-modules, that is, an exact sequence

$$\cdots \longrightarrow P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0$$

where all P_i are free G-modules. We can construct this inductively: choose a free module P_0 with a surjective map $\epsilon : P_0 \to \mathbb{Z}$, choose P_1 free with a surjection $d_1 : P_1 \to \ker \epsilon$, and then for each each $i \geq 2$ choose a free module P_i with a surjective map $d_i : P_i \to \ker d_{i-1}$.

Now, define a complex K^* by $K^i = \mathrm{Hom}_G(P_i, A)$; let $d^i : K^{i-1} \to K^i$ be the map induced by $d_i : P_i \to P_{i-1}$. Let $H^i(G, A)$ be the cohomology of the chain complex K^*:

$$H^i(G, A) = \ker(d^{i+1} : \mathrm{Hom}_G(P_i, A) \to \mathrm{Hom}_G(P_{i+1}, A)) / \operatorname{im}(d^i : \mathrm{Hom}_G(P_{i-1}, A) \to \mathrm{Hom}_G(P_i, A))$$

for $i \geq 1$, and

$$\begin{aligned} H^0(G, A) &= \ker(d^1 : \mathrm{Hom}_G(P_0, A) \to \mathrm{Hom}_G(P_1, A)) \\ &\cong \mathrm{Hom}_G(P_0 / d_1(P_1), A) \\ &\cong \mathrm{Hom}_G(\mathbb{Z}, A) \cong A^G. \end{aligned}$$

Now we construct the long exact sequence. Let $0 \to A \to B \to C \to 0$ be a short exact sequence of G-modules. Because P_i is projective, we have a short exact sequence

$$0 \to \mathrm{Hom}_G(P_i, A) \to \mathrm{Hom}_G(P_i, B) \to \mathrm{Hom}_G(P_i, C) \to 0$$

for all i, giving a short exact sequence of chain complexes. The standard snake lemma construction gives the desired long exact sequence.

Finally, if $A = \mathrm{coInd}^G(X)$ is co-induced, then for each i, $K^i = \mathrm{Hom}_G(P_i, A) \cong \mathrm{Hom}_{\mathbb{Z}}(P_i, X)$ by baby Frobenius reciprocity. Because each P_i is a free $\mathbb{Z}$-module, the chain complex K^* is exact and all $H^i(G, A)$ vanish for $i \geq 1$.

We now prove uniqueness by what is known as a *dimension shifting* argument. We induct on i.

For base case of $i = 0$, we know already that $H^0(G, A) = A^G$ is uniquely determined.

Now we do the inductive step. We've seen that an A injects into a co-induced module $A^* = \mathrm{Hom}(\mathbb{Z}[G], A)$. Let A' be the cokernel of the map $A \to A^*$. The short exact sequence $0 \to A \to A^* \to A' \to 0$ gives $H^1(A) \cong \ker(H^0(A^*) \to H^0(A'))$ and $H^{i+1}(A) \cong H^i(A')$ for all $i \geq 1$, so uniqueness follows by induction. □

It's straightforward to show that the long exact sequence is natural in the sense that, if

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{i} & B & \xrightarrow{j} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi_A} & & \downarrow{\scriptstyle \phi_B} & & \downarrow{\scriptstyle \phi_C} & & \\ 0 & \longrightarrow & A' & \xrightarrow{i'} & B' & \xrightarrow{j'} & C' & \longrightarrow & 0 \end{array}$$

is a morphism of short exact sequences, the diagram

$$\begin{array}{ccccccccc}
\longrightarrow & H^i(G,A) & \xrightarrow{i_*} & H^i(G,B) & \xrightarrow{j_*} & H^i(G,C) & \xrightarrow{\delta} & H^{i+1}(G,A) & \longrightarrow \\
& \downarrow{\scriptstyle (\phi_A)_*} & & \downarrow{\scriptstyle (\phi_B)_*} & & \downarrow{\scriptstyle (\phi_C)_*} & & \downarrow{\scriptstyle (\phi_A)_*} & \\
\longrightarrow & H^i(G,A') & \xrightarrow{i'_*} & H^i(G,B') & \xrightarrow{j'_*} & H^i(G,C') & \xrightarrow{\delta'} & H^{i+1}(G,A') & \longrightarrow
\end{array}$$

commutes.

Example. Let $G = C_n = \langle t \mid t^n = 1\rangle$, so $\mathbb{Z}[G] = \mathbb{Z}[t]/(t^n - 1)$ is commutative. Recall that $N = \sum_{g\in G} g = 1 + t + t^2 + \cdots + t^{n-1}$. Then

$$\cdots \mathbb{Z}[G] \xrightarrow{\times(t-1)} \mathbb{Z}[G] \xrightarrow{\times N} \mathbb{Z}[G] \xrightarrow{\times(t-1)} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z}$$

is a free resolution. Since $\mathrm{Hom}_G(\mathbb{Z}[G], A) \cong A$ for any A, the chain complex K^* is

$$A \xrightarrow{\times(t-1)} A \xrightarrow{\times N} A \xrightarrow{\times(t-1)} A \xrightarrow{\times N} \cdots.$$

As a result, we compute $H^0(A) = \ker(t-1) = A^G$, $H^{2i+1}(A) = \ker N/(t-1)A$ for $i \geq 0$, and $H^{2i}(A) = A^G/NA$ for $i \geq 1$.

13.3 The standard resolution

However, we're going to need to be more systematic to get free resolutions for an arbitrary G.

Fortunately, there is a standard way of producing these.

Let $P_i = \mathbb{Z}[G^{i+1}]$ be the span of all $i+1$-tuples $(g_0, \ldots, g_i)$, with diagonal action of G. That is, $g(g_0, \ldots, g_i) = (gg_0, \ldots, gg_i)$. This is a free G-module: one possible basis is the elements of the form $(1, g_1, \ldots, g_i)$.

Define $d_i : P_i \to P_{i-1}$ by $d_i((g_0, \ldots, g_i)) = \sum_j (-1)^j (g_0, \ldots, \widehat{g_j} \ldots, g_i)$.

Then it's straightforward to show that $d_i d_{i+1} = 0$. To show that in fact $\ker d_i = \mathrm{im}\, d_{i+1}$, choose any an element $s \in G$ and define maps $h_i : P_i \to P_{i+1}$ by $h(g_0, \ldots, g_i) = (s, g_0, \ldots, g_i)$. Then h is a chain homotopy: $d_{i+1}h_i + h_{i-1}d_i = 1$, and a standard argument implies that $\ker d_i = \mathrm{im}\, d_{i+1}$. (To be explicit: if $a_i \in \ker d_i$ then $a_i = d_{i+1}h_i a_i + h_{i-1}d_i a_i = d_{i+1}h_i a_i \in \mathrm{im}\, d_{i+1}$.)

14 October 26

14.1 Homogeneous and inhomogeneous cochains

We can interpret the elements of $\mathrm{Hom}(P_i, A)$ as follows.

Definition. A homogeneous i-cochain is a map $f : G^{i+1} \to A$ such that $f(gg_0, \ldots, gg_i) = gf(g_0, \ldots g_i)$. The set of homogeneous i-cochains is denoted by $\tilde{C}^i(G, A)$.

Then we have identifications $\mathrm{Hom}_G(P_i, A) \cong \tilde{C}^i(G, A)$ for all i. The differential $d^i : \tilde{C}^{i-1}(G, A) \to \tilde{C}^i(G, A)$ on homogeneous cochains is given by

$$(d^i f)(g_0, \ldots, g_i) = \sum_j (-1)^j f(g_0, \ldots, \hat{g_j}, \ldots, g_i).$$

The kernel of d^{i+1} in $\tilde{C}^i(G, A)$ is called the group of *homogeneous cocycles* $\tilde{Z}(G, A)$. The image of d^i inside $\tilde{C}^i(G, A)$ is called the *homogeneous coboundaries* $\tilde{B}(G, A)$. We have $H^i(G, A) \cong \tilde{Z}^i(G, A)/\tilde{B}^i(G, A)$.

We will now change variables to something that's easier to work with.

Definition. An inhomogeneous i-cochain is a map $\phi : G^i \to A$. We let $C^i(G, A)$ denote the abelian group of inhomogeneous i-cochains.

We can map homogeneous cochains to inhomogeneous cochains by the following change of variables map. We send a homogeneous cochain f to the inhomogeneous cochain ϕ with

$$\phi(g_1, \ldots, g_n) = f(1, g_1, g_1g_2, \ldots, g_1g_2 \cdots g_n).$$

This map is an isomorphism of abelian groups $\tilde{C}^i(G, A) \cong C^i(G, A)$. Via this isomorphism, the map $d^i : \tilde{C}^{i-1}(G, A) \to \tilde{C}^i(G, A)$ induces a map $d^i : C^{i-1}(G, A) \to C^i(G, A)$.

We can work out what this is explicitly: the map $d^i : C^{i-1}(G, A) \to C^i(G, A)$ sends an inhomogeneous $i-1$-cochain ϕ to the inhomogeneous i-cochain $d^i\phi$ given by

$$\begin{aligned}(d^i\phi)(g_1, \ldots, g_i) &= g_1\phi(g_2, \ldots, g_i) - \phi(g_1g_2, g_3, \ldots, g_i) \\ &\quad + \phi(g_1, g_2g_3, \ldots, g_i) + \cdots (-1)^{i-1}\phi(g_1, g_2, \ldots, g_{i-1}g_i) + (-1)^i\phi(g_1, g_2, \ldots, g_i). \quad (9)\end{aligned}$$

Let the group of *inhomogeneous cocycles* $Z^i(G, A) = \ker(d^{i+1} : C^i(G, A) \to C^{i+1}(G, A))$ and the *inhomogeneous coboundaries* $B^i(G, A) = \mathrm{im}(d^i : C^{i-1}(G, A) \to C^i(G, A))$. Then we have $H^i(G, A) \cong \tilde{Z}^i(G, A)/\tilde{B}^i(G, A) \cong Z^i(G, A)/B^i(G, A)$.

Example. We work out the maps d^i for small i.

The map

$$d^1 : C^0(G, A) \cong A \to C^1(G, A)$$

sends an element $a \in A$ to the 1-cochain $\phi(a) = ga - a$.

The map

$$d^2 : C^1(G, A) \to C^2(G, A)$$

sends a 1-cochain ϕ to the 2-cochain $d^2\phi$ given by

$$(d^2\phi)(g_1, g_2) = g_1\phi(g_2) - \phi(g_1g_2) + \phi(g_1).$$

The map

$$d^3 : C^2(G, A) \to C^3(G, A)$$

sends a 2-cochain ϕ to the 3-cochain $d^3\phi$ given by

$$(d^3\phi)(g_1, g_2, g_3) = g_1\phi(g_2, g_3) - \phi(g_1g_2, g_3) + \phi(g_1, g_2g_3) - \phi(g_1, g_2)$$

In consequence: inhomogeneous 1-cocycles are maps $G \to A$ with

$$\phi(gh) = g\phi(h) + \phi(g).$$

These are also called *crossed homomorphisms*. Inhomogeneous 1-coboundaries are functions of the form $\phi_a(g) = ga - a$.

Note that if G acts trivially on A, $Z^1(G, A) = \mathrm{Hom}_{\mathrm{groups}}(G, A)$ and $B^1(G, A) = 0$, so $H^1(G, A) \cong \mathrm{Hom}_{\mathrm{groups}}(G, A)$.

We have that $Z^2(G, A)$ is the group of maps $G \times G \to A$ with

$$g_1\phi(g_2, g_3) - \phi(g_1g_2, g_3) + \phi(g_1, g_2g_3) - \phi(g_1, g_2) = 0$$

and $B^2(G, A)$ is the group of maps of the form

$$d^2\psi = g_1\psi(g_2) - \psi(g_1g_2) + \psi(g_1)$$

for a function $\psi : G \to A$.

Suppose we have a short exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$. Then we've constructed a corresponding long exact sequence. In particular, we have a connecting homomorphism $\delta : C^G = H^0(G, C) \to H^1(G, A)$, which we can now describe explicitly in terms of inhomogeneous cocycles. Pick $b \in B$ lifting c, then the map $g \mapsto g(b) - b$ lies in $Z^1(G, A)$. Replacing b by $b' = b + a$ adds an arbitrary element of $B^1(G, A)$. Finally, this cohomology class is trivial if and only if we can choose $b \in B^G$, showing that $B^G \to C^G \to H^1(G, A)$ is exact.

14.2 H^1, H^2 and group extensions

We're now going to pause to talk a bit about other places in math where the group $H^1(G, A)$ comes up.

Recall that if a group G acts on an abelian group A, we can define the semidirect product $G \ltimes A$. As a set, $G \ltimes A$ is $G \times A$, but with the product given by

$$(g_1, a_1)(g_2, a_2) = (g_1g_2, a_1 + g_1a_2).$$

We have a short exact sequence

$$0 \to A \to G \ltimes A \to G \to 0. \tag{10}$$

We claim that elements of $Z^1(G, A)$ correspond to splittings of this exact sequence. Indeed, any such splitting must take the form $g \mapsto (g, \phi(g))$, and this is a group homomorphism if and only if

$$(gh, \phi(gh)) = (g, \phi(g))(h, \phi(h)) = (gh, \phi(g) + g\phi(h)).$$

The group A acts on $G \ltimes A$ by conjugation: write $c_a(x) = axa^{-1}$ for $a \in A$, $x \in G \ltimes A$. Hence A acts on the set of splittings $G \mapsto G \ltimes A$ by conjugation. One can show that this conjugation action has the effect of adding the coboundary ϕ_a to ϕ:

$$c_a(g, \phi(g)) = (g, \phi(g) + a - ga).$$

It then follows that elements of $H^1(G, A)$ are in bijection with A-conjugacy classes of splittings of the short exact sequence (10).

There is a similar interpretation of $H^2(G, A)$, involving group extensions

$$0 \to A \to X \xrightarrow{\pi} G \to 0.$$

Given any such group extension, the group X acts on the normal subgroup A by conjugation. Because A is abelian, this action descends to an action of $X/A = G$ on A by conjugation. For any G-module A, the set $H^2(G, A)$ is in bijection with the set of isomorphism classes of group extensions of G by A such that the action of G on A coming from the group extension agrees with the action coming from the G-module structure on A.

We won't do all the details, but we will give the map in one direction. Given a group extension, take a section $s : G \to X$ of the projection map $\pi : X \to G$. Here s is just some function between sets, not necessarily a homomorphism. Then we construct a map $\psi : G \times G \to A$ by

$$\psi(g, h) = s(g)s(h)s(gh)^{-1}.$$

The statement that $\psi \in Z^2(G, A)$ is then equivalent to the associative property for the group X, and replacing s by a different map s' adds an element of $B^2(G, A)$ to ψ.

14.3 Torsors

We now do another interpretation of H^1 that comes up a lot in number theory.

If A is an abelian group, an A-torsor is a set X with a simply transitive action of A. (One way of saying this is that X is nonempty, and $X \times A \cong X \times X$ in the category of sets, via the map $(x, a) \mapsto (x, ax)$.)

If A is a G-module, then we require that X be a G-set that makes the above an isomorphism in the category of G-sets, that is: $ga(gx) = g(ax)$

(For clarity, we'll often prefer to either write the A-action additively, eg $ga + gx = g(a + x)$, or write the G-action in superscript: ${}^g a\, {}^g x = {}^g(ax)$.)

Example. If A is an abelian group or G-module, then A is a torsor for itself, known as the "trivial torsor".

Can show that an A-torsor X is isomorphic to A if and only if there exists some $x_0 \in X$ which is fixed by every element of g. For the "only if" direction, take $x_0 = 0$. For the "if directon", the isomorphism is given by $a \mapsto a + x_0$.

Next time we'll show

Theorem 14.1. *The set of A-torsors is in bijection with $H^1(G, A)$. This bijection sends the trivial A-torsor A to $0 \in H^1(G, A)$.*

15 October 29

15.1 Torsors, continued

Example. A number-theoretic example. Let L/K be a field extension where L contains the nth roots of unity. Let $G = \mathrm{Gal}(L/K)$ and $A = \mu_n(L)$. Then for any $c \in K^\times$, the set $X = \{a \mid a^n = c\}$ is a torsor for $\mu_n(L)$ with action given by multiplication.

This torsor may or may not be trivial: if $c = 1$, then $X = A$. (More generally, if $c \in (K^\times)^n$ then $X \cong A$ as torsors. Later we'll be able to show this is if and only if.) On the other hand, if $\mu_n(K) \subset L$ but $c \notin (K^\times)^n$, then A has trivial G-action, but X does not, so they cannot be isomorphic torsors.

More precisely, one can show that the isomorphism classes of μ_n-torsors for $\mathrm{Gal}(L/K)$ are classified by $(K^\times \cap (L^\times)^n)/(K^\times)^n$.

Example. From arithmetic geometry. Suppose that C is a curve of genus 1 over $\mathbb{Q}$. Then C may or may not have any rational points, but we can construct an elliptic curve $E = \mathrm{Jac}(C)$, such that C is a torsor for E as varieties over $\mathbb{Q}$ (that is, the map $E \times C \to C$ giving the morphism is a morphism of varieties over $\mathbb{Q}$). Since E is an elliptic curve, it has a rational point $[0]$ (the point at infinity).

This torsor is trivial if and only if $C(\bar{\mathbb{Q}})$ has a rational point.

One can show that for a fixed elliptic curve E, all E-torsors arise in this way. As a result, genus 1 curves over $\mathbb{Q}$ whose Jacobian is isomorphic to E are classified to up isomorphism by $H^1(\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}), E(\bar{\mathbb{Q}}))/\mathrm{Aut}_{\mathbb{Q}}(E)$.

Theorem 15.1. *Let A be a G-module. The set of A-torsors is in bijection with $H^1(G, A)$. This bijection sends the trivial A-torsor A to $0 \in H^1(G, A)$.*

Proof. We give maps in both directions. Suppose that $[\phi] \in H^1(G, A)$ is represented by a cocycle $\phi \in Z^1(G, A)$.

Then we define a torsor X as follows. As an A-set, $X = A$ with usual A-action. However, the G-action on A is twisted by ϕ as follows:

$$g *_\phi x = gx + \phi(g).$$

We check that this gives a group action:

$$\begin{aligned} g *_\phi (h *_\phi x) &= g(h *_\phi x) + \phi(g) \\ &= g(hx + \phi(h)) + \phi(g) \\ &= ghx + (\phi(g) + g\phi(h)) \\ &= (gh)x + \phi(gh) \\ &= (gh) *_\phi x, \end{aligned}$$

using the fact that ϕ is a 1-cocyle. We also clearly have $g *_\phi (a + x) = ga + g *_\phi (x)$. Finally, to check that this map is well-defined, if $\phi' = \phi + (ga - a)$, then we have $g *_{\phi'} (x) + a = g_*\phi(x + a)$, giving an isomorphism between the corresponding torsors.

In the other direction, suppose that X is an A-torsor. Choose any $x_0 \in X$. Then we can define a map $\phi : G \to A$ by $\phi(g)$ is the unique element of A satisfying $g(x_0) = \phi(g) + x_0$. Exercise to check that this is an element of $Z^1(G, A)$. If we replace x by $a + x$, the cocycle ϕ is replaced by $\phi + g(a) - a$, so the class $[\phi] \in H^1(G, A)$ is well-defined.

Finally, it's a simple exercise to check that these two maps are inverses.

□

Using torsors, we can give another explicit interpretation of the connecting homomorphism $\delta : H^0(G, C) \to H^1(G, A)$ coming from the exact sequence $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$. For $c \in C^G = H^0(C, G)$, the preimage $j^{-1}(c)$ is a torsor for A, which corresponds to the element $\delta(c) \in H^1(G, A)$ via the bijection above.

15.2 Group homology

We now define group homology functors $H_i(G, A)$ for $i \geq 0$. Recall that we have a right-exact functor $A \mapsto A_G$ from G-modules to $\mathbb{Z}$-modules; here $A_G = A/I_G A = A \otimes_G \mathbb{Z}$.

Theorem 15.2. *There is a unique family of functors $H_i(G, A)$, $i \geq 0$ with the properties that*

a) $H_0(G, A) = A_G$.

b) $H_i(G, A) = 0$ *for* $i \geq 1$ *if* A *is an induced* G*-module.*

c) Any short exact sequence $0 \longrightarrow A \xrightarrow{i} B \xrightarrow{j} C \longrightarrow 0$ *of* G*-modules induces a long exact sequence*

$$\begin{array}{l} \cdots \xrightarrow{i_*} H_2(G, B) \xrightarrow{j_*} H_2(G, C) \xrightarrow{\delta} \\ \quad H_1(G, A) \xrightarrow{i_*} H_1(G, B) \xrightarrow{j_*} H_1(G, C) \xrightarrow{\delta} \\ \quad H_0(G, A) \xrightarrow{i_*} H_0(G, B) \xrightarrow{j_*} H_0(G, C) \longrightarrow 0 \end{array}$$

Proof. The proof here is very similar to that for cohomolgy.

To do the construction, let $\cdots F_2 \to F_1 \to F_0 \to \mathbb{Z}$ be a free (flat) resolution of $\mathbb{Z}$. Let $H_i(G, A)$ be the homology of the chain complex $F_* \otimes_G A$. One checks that this satisfies the required conditions in the same way as one does for cohomology.

The proof of uniqueness is again a dimension-shifting argument, using induced modules rather than co-induced modules, and reversing the directions of the arrows.

□

We can use the standard resolution $\cdots \to \mathbb{Z}[G^2] \to \mathbb{Z}[G] \to \mathbb{Z}$ to compute group homology the same way that we did for cohomology. However, we won't go into the details here. One reason is that, for the purposes of class field theory, what we mostly need is $H_0(G, A) = A_G$, plus one specific case of H_1, which we work out now by dimension shifting:

Proposition 15.3. *Let* G *be a group. Then* $H_1(G, \mathbb{Z}) \cong I_G/(I_G)^2 \cong G^{ab}$.

Proof. We have $H_1(G, \mathbb{Z}[G]) = 0$ because $\mathbb{Z}[G]$ is induced. Hence the short exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$ gives a long exact sequence

$$0 \to H_1(G, \mathbb{Z}) \to I_G/(I_G^2) \to \mathbb{Z}[G]/I_G.$$

Here the last map is the zero map, so $H_1(G, \mathbb{Z}) \cong I_G/(I_G)^2$.

Now, recall that I_G is a free $\mathbb{Z}$-module with basis $a_g = g - 1$ for $g \neq 1 \in G$. To form the quotient $I_G/(I_G^2)$, we impose all relations of the form $(g-1)(h-1) = 0$ for all $g, h \in G$. But

$$(g-1)(h-1) = gh - g - h + 1 = a_{gh} - a_g - a_h.$$

Hence $I_G/(I_G^2)$ is the abelian group with generators $\{a_g\}$ and relations $a_{gh} - a_g - a_h$. This is the same thing as G^{ab}. □

15.3 Plan for proving local class field theory

When G is finite, we'll be able to splice together the group cohomology and homology functors to make what are called *Tate cohomology* functors $\hat{H}^q(G, A)$ for $q \in \mathbb{Z}$, where

$$\hat{H}^q(G, A) = \begin{cases} H^q(G, A) & \text{for } q \geq 1 \\ A^G/NA & \text{for } q = 0 \\ \ker(N : A_G \to A) & \text{for } q = -1 \\ H_{-1-q}(G, A) & \text{for } q \leq -2 \end{cases}$$

In particular, note here that if $G = \mathrm{Gal}(L/K)$ and $A = L^\times$, then $\hat{H}^0(G, L^\times) = K^\times/NL^\times$, which is a group we've seen before in the statements of local class field theory. Additionally $\hat{H}^{-2}(G, \mathbb{Z}) \cong \mathrm{Gal}(L/K)^{ab}$ which is the Galois group of the maximal abelian subextension of L/K

Ultimately we'll be able to define the Artin map $\hat{H}^{-2}(G,\mathbb{Z}) \to \hat{H}^0(G,L^\times)$ as a cup product with a special cohomology class in $H^2(G,L^\times)$.

15.4 Change of group and compatible pairs

So far we've just talked about $H^i(G,A)$ and $H_i(G,A)$ as functors in A. However, they can actually be viewed as functors in the pair (G,A). Cohomology is contravariant in G and covariant in A, while homology is covariant in G and covariant in A.

Compatible pairs for cohomology: Let (G,A) and (G',A') be pairs where A is a G-module and A' is an G'-module. We say that they are compatible (for cohomology) if there are morphisms $\rho : G' \to G$ and $\lambda : A \to A'$ such that $\lambda(\rho(g')a) = g'(\lambda a)$.

Example. If H is a subgroup of G, then (G,A) and (H,A) are compatible via the inclusion map $i : H \to G$ and the identity map $\mathrm{id}_A : A \to A$.

Example. If H is a normal subgroup of G, then $(G/H, A^H)$ and (G,A) are compatible via the quotient map $\pi : G \to G/H$ and the inclusion $i : A^H \to A$.

When (G,A) and (G',A') are compatible, the map $\rho : G' \to G$ gives a map $\rho_* : \mathbb{Z}[(G')^{i+1}] \to \mathbb{Z}[G^{i+1}]$. Recall that the standard resolutions of G' and G respectively are given by $P_i(G') = \mathbb{Z}[(G')^{i+1}]$ and $P_i(G) = \mathbb{Z}[G^{i+1}]$, and ρ_* maps $P_i(G')$ to $P_i(G)$.

We then get a map $\mathrm{Hom}(\rho_*, \lambda) : \mathrm{Hom}_G(P_i(G), A) \to \mathrm{Hom}_{G'}(P_i(G'), A')$. and this map of chain complexes gives an induced map on cohomology $H^i(G,A) \to H^i(G',A')$.

We can also describe this map explicitly in terms of inhomogeneous cochains: if $[\phi] \in H^i(G,A)$ is represented by a cocycle $\phi \in Z^i(G,A)$, the induced map sends it to the class $[\phi']$ of the cocycle $\phi' \in Z^i(G',A')$ given by

$$\phi'(g'_1,\dots,g'_i) = \lambda(\phi'(\rho(g'_1,\dots,g'_i))).$$

Example. For the compatible pair (G,A) and (H,A), with maps $i : H \to G$ and $\mathrm{id}_A : A \to A$, the induced map is denoted $\mathrm{Res} : H^i(G,A) \to H^i(H,A)$ and is called *restriction*. If we work with inhomogeneous cochains, this map is literally restriction: $(\mathrm{Res}\,\phi)(h_1,\dots,h_i) = \phi(h_1,\dots,h_i)$.

Example. For the compatible pair $(G/H, A^H)$ and (G,A) with maps $\pi : G \to G/H$ and $i : A \to A^H$, the induced map is denoted $\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G,A)$ and is called *inflation*. If H is normal, then there is also a natural map $\mathrm{Inf} : H^i(G/H, A^H) \to H^i(G,A)$. Again $\mathrm{Inf}\,\phi(g_1,\dots,g_i) = \phi(g_1H\dots,g_iH)$

16 November 2

16.1 Change of group, continued

Example. For the compatible pair (G,A) and (H,A), with maps $i : H \to G$ and $\mathrm{id}_A : A \to A$, the induced map is denoted $\mathrm{Res} : H^q(G,A) \to H^q(H,A)$ and is called *re-*

striction. If we work with inhomogeneous cochains, this map is literally restriction: $(\mathrm{Res}\,\phi)(h_1,\dots,h_q) = \phi(h_1,\dots,h_q)$.

Example. For the compatible pair $(G/H, A^H)$ and (G, A) with maps $\pi : G \to G/H$ and $i : A^H \to A$, the induced map is denoted $\mathrm{Inf} : H^q(G/H, A^H) \to H^q(G, A)$. If H is normal, then there is also a natural map $\mathrm{Inf} : H^q(G/H, A^H) \to H^q(G, A)$. Again $\mathrm{Inf}\,\phi(g_1,\dots,g_q) = \phi(g_1H\dots,g_qH)$

We claim that for $H \subset G$ a normal subgroup and any G-module A, the composite map $\mathrm{Res} \circ \mathrm{Inf} : H^q(G/H, A^H) \to H^q(G, A)$ is the zero map for all $q > 0$.

There are two ways to prove it, one hands-on and one slicker (though they are fundamentally the same proof).

Hands-on proof (not done in class): Note that for any $\phi \in H^q(G/H, A^H)$, the inhomogeneous cocycle $\psi = \mathrm{Res} \circ \mathrm{Inf}(\phi)$ is a constant map $\psi : H^q \to A$. In class I claimed that any such cocycle ψ that is constant must be the zero cocycle. This is true if q is odd: in that case plugging in all $h_i = 1$ to the cocycle condition gives $\psi(1,\dots,1) = 0$, and so $\psi = 0$. However, if q is even, all one can deduce is that if the function $\psi(h_1,\dots,h_q) = a$ is a cocycle, then $a \in A^H$. In that case, however, $\psi = d\psi'$ where $\psi' \in Z^{q-1}(G, A)$ is the constant cocycle: $\psi'(h_1,\dots,h_{q-1}) = a$.

Slick proof: make a commutative diagram of induced maps

$$\begin{array}{ccc} H^q(G/H, A^H) & \xrightarrow{\mathrm{Inf}} & H^q(G, A) \\ \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} \\ H^q(H/H, A^H) & \xrightarrow{\mathrm{Inf}} & H^q(H, A^H) \end{array}$$

and note that $H^q(H/H, A^H) = H^q(1, A^H) = 0$, so the composition either way is the zero map.)

Compatible pairs for homology: Let (G, A) and (G', A') be pairs where A is a G-module and A' is an G'-module. We say that they are compatible (for homology) if there are morphisms $\rho : G \to G'$ and $\lambda : A \to A'$ such that $\lambda(ga) = \rho(g)\lambda(a)$. Under these conditions, we get morphisms $H_q(G, A) \to H_q(G', A)$, for similar reasons as with cohomology.

Example. The pairs (H, A) and (G, A) are compatible with $i : H \to G$ the inclusion map and $id_A : A \to A$ the identity map.

The induced map $\mathrm{Cor} : H_q(H, A) \to H_q(G, A)$ is know as *corestriction*. For $q = 0$ this is the quotient map $A/I^HA \to A/I^GA$; for $q = 1$ and $A = \mathbb{Z}$, this agrees with the natural map $H^{ab} \to G^{ab}$.

The functors Res and Cor have the property of compatibility with derived long exact sequences: if $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ is a short exact sequence of G-modules, it is also a

short exact sequence of H-modules, and the diagrams

$$\begin{array}{ccccccccccc}
\dots & \longrightarrow & H^q(G,A) & \xrightarrow{i_*} & H^q(G,B) & \xrightarrow{j_*} & H^q(G,C) & \xrightarrow{\delta} & H^{q+1}(G,A) & \longrightarrow & \dots \\
 & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle \mathrm{Res}} & & \\
\dots & \longrightarrow & H^q(H,A) & \xrightarrow{i_*} & H^q(H,B) & \xrightarrow{j_*} & H^q(H,C) & \xrightarrow{\delta} & H^{q+1}(H,A) & \longrightarrow & \dots
\end{array}$$

and

$$\begin{array}{ccccccccccc}
\dots & \longrightarrow & H_q(H,A) & \xrightarrow{i_*} & H_q(H,B) & \xrightarrow{j_*} & H_q(H,C) & \xrightarrow{\delta} & H_{q+1}(H,A) & \longrightarrow & \dots \\
 & & \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} & & \downarrow{\scriptstyle \mathrm{Cor}} & & \\
\dots & \longrightarrow & H_q(G,A) & \xrightarrow{i_*} & H_q(G,B) & \xrightarrow{j_*} & H_q(G,C) & \xrightarrow{\delta} & H_{q+1}(G,A) & \longrightarrow & \dots
\end{array}$$

commute.

In fact, the family of functors $\mathrm{Res} : H^q(G,A) \to H^q(H,A)$ can be characterized by the above compatibility with exact sequences along with the property that $\mathrm{Res} : H^0(G,A) \to H^0(H,A)$ is the inclusion $A^G \to A^H$. Just those properties are enough to compute Res for any q and A by dimension-shifting.

Likewise: $\mathrm{Cor} : H_q(H,A) \to H_q(G,A)$ is characterized by the property Cor is compatible with exact sequences and $\mathrm{Cor} : H_0(H,A) \to H_0(G,A)$ is the quotient map $A_H \to A_G$.

16.2 The inflation-restriction exact sequence

Theorem 16.1. *There exists an exact sequence*

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

Proof. We check this using cochains.

First, if $\phi \in Z^1(G/H, A^H)$ is such that $[\phi]$ lies in the kernel of Inf, then there exists $a \in A$ such that $\phi(gH) = ga - a$ for all $g \in G$. This implies that $ha - a = \phi(H) = a - a = 0$ for all $h \in H$, so $a \in A^H$, and so $\phi \in B^1(G/H, A^H)$.

We've already seen that $\ker \mathrm{Res} \supset \mathrm{im}\, \mathrm{Cor}$. If $\phi \in Z^1(G,A)$ is such that $[\phi]$ lies in the kernel of Res, then there exists $a \in A$ such that for all $h \in H$, $\phi(h) = ha - a$. By subtracting off the coboundary $g \mapsto ga - a$, may assume that $\phi(h) = 0$ for all $h \in H$. Then we have $\phi(gh) = \phi(g)$ for all $g \in G$, $h \in H$, which means that ϕ factors through a map $\tilde{\phi} : G/H \to A$. Also have $\phi(g) = \phi(hg) = h\phi(g)$, so ϕ has image in A^H. Hence $\tilde{\phi}$ maps $G/H \to A^H$, and is a cocycle because ϕ is, and has $\mathrm{Inf}(\tilde{\phi}) = \phi$ by construction. □

This is not in general true for H^q with $q > 1$; the correct generalization to larger q is the Lyndon-Hochschild-Serre spectral sequence. However, in a special case, it does hold:

Theorem 16.2. *If* $H^i(H, A) = 0$ *for* $1 \leq i < q$*, then there exists an exact sequence*

$$0 \longrightarrow H^q(G/H, A^H) \xrightarrow{\text{Inf}} H^q(G, A) \xrightarrow{\text{Res}} H^q(H, A).$$

Proof. This is a dimension-shifting argument. We induct on q, with $q = 1$ already proved.

Now assume $q > 1$ and that we know the inductive hypothesis for $q - 1$.

Let $A^* = \text{coInd}^G(A) = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$. We have a short exact sequence $0 \to A \to A^* \to A' \to 0$ of G-modules.

We observe that A^* is also co-induced as an H-module: $\mathbb{Z}[G] = \bigoplus_{gH \in G/H} g\mathbb{Z}[H]$ is a free right $\mathbb{Z}[H]$-module, so $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$ is a product of copies of $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], A)$, and a product of co-induced modules is co-induced.

Hence the connecting homomorphism gives isomorphisms $H^i(H, A') \cong H^{i+1}(H, A)$ for $i \geq 1$. For $1 \leq i < q - 1$, this gives us $H^i(H, A') = 0$. Therefore, we may apply the inductive hypothesis to A', and we find that

$$0 \longrightarrow H^{q-1}(G/H, (A')^H) \xrightarrow{\text{Inf}} H^{q-1}(G, A') \xrightarrow{\text{Res}} H^{q-1}(H, A').$$

Now we want to use dimension-shifting to identify each term with the corresponding term in the exact sequence that we want to establish.

First of all, because A^* is also a co-induced H-module, the connecting homomorphism $\delta : H^{q-1}(H, A') \to H^q(H, A)$ is an isomorphism.

We also know, from the long exact sequence on G-modules, that $\delta : H^{q-1}(G, A') \to H^q(G, A)$ is an isomorphism.

To handle $H^{q-1}(G/H, (A')^H)$, we note that the short exact sequence $0 \to A \to A^* \to A' \to 0$ of A-modules gives a long exact sequence starting

$$0 \longrightarrow A^H \longrightarrow (A^*)^H \longrightarrow (A')^H \longrightarrow H^1(H, A)$$

but $H^1(H, A) = 0$ by assumption so this is really a short exact sequence

$$0 \longrightarrow A^H \longrightarrow (A^*)^H \longrightarrow (A')^H \longrightarrow 0.$$

Also, $(A^*)^H = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)^H = \text{Hom}_{\mathbb{Z}}(\mathbb{Z}[G/H], A)$ is a co-induced G/H-module. Hence, in the long exact sequence in cohomology, the map $H^{q-1}(G/H, (A')^H) \to H^q(G/H, A^H)$ are isomorphisms.

Putting this all together gives a commutative diagram

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

where the top row is exact by the inductive hypothesis, and all the vertical maps are isomorphisms, hence the bottom row is also exact.

□

16.3 Tate Cohomology

Let G be a finite group. Recall we have the element $N = \sum_{g \in G} g \in \mathbb{Z}[G]$ and have norm map $N : A \to A$ given by left multiplication by g.

Observe that $\operatorname{im} N \subset A^G$ and $\ker N \supset I_G A$, so N induces a map $N^* : H_0(G, A) = A_G \to A^G = H^0(G, A)$.

We now define the Tate cohomology groups for all q:

Definition. The Tate cohomology groups $\hat{H}^q(G, A)$ are defined by

$$\begin{aligned}
\hat{H}^q(G, A) &= H^q(G, A) \quad \text{for } q \geq 1 \\
\hat{H}^0(G, A) &= \operatorname{cok} N^* : A_G \to A^G \\
\hat{H}^{-1}(G, A) &= \ker N^* : A_G \to A^G \\
\hat{H}^{-1-q}(G, A) &= H_q(G, A) \quad \text{for } q \geq 1.
\end{aligned}$$

Using the snake lemma to splice together the long exact sequences

$$\begin{array}{ccccccccccc}
\longrightarrow & \hat{H}^{-2}(G, C) & \longrightarrow & A_G & \longrightarrow & B_G & \longrightarrow & C_G & \longrightarrow & 0 & \\
 & & & \downarrow{\scriptstyle N_A^*} & & \downarrow{\scriptstyle N_B^*} & & \downarrow{\scriptstyle N_C^*} & & & \\
0 & \longrightarrow & A^G & \longrightarrow & B^G & \longrightarrow & C^G & \longrightarrow & \hat{H}^1(G, A) & \longrightarrow &
\end{array}$$

to get a doubly infinite long exact sequence

$$\begin{array}{ccccccccccc}
\longrightarrow & \hat{H}^{-2}(G, C) & \longrightarrow & \hat{H}^{-1}(G, A) & \longrightarrow & \hat{H}^{-1}(G, B) & \longrightarrow & \hat{H}^{-1}(G, C) & & & \\
 & & & & & & \searrow & & & & \\
 & & & \hat{H}^0(G, A) & \longrightarrow & \hat{H}^0(G, B) & \longrightarrow & \hat{H}^0(G, C) & \longrightarrow & \hat{H}^1(G, A) & \longrightarrow
\end{array}$$

Recall that if G is finite, a G-module A is induced if and only if it is co-induced.

Proposition 16.3. *If A is induced (equivalently, co-induced), then $\hat{H}^q(G, A) = 0$ for all $q \in \mathbb{Z}$.*

Proof. We already know this for $q \neq 0, -1$. To resolve those two cases, enough to show that $N^* : A_G \to A^G$ is an isomorphism.

Assume then that $A = \oplus_{g \in G} gX$ is a co-induced G-module. Then, on the one hand, the map $A_G \to X$ given by $[\sum_{g \in G} g x_g] \mapsto \sum_{g \in G} x_g$ is an isomorphism, with inverse induced by the map $X \to A$. On the other hand, the map $X \to A^G$ given by $x \mapsto \sum_{g \in G} gx$

is also an isomorphism. The composition of these two isomorphisms is the norm map $N : A_G \to A^G$, which must also be an isomorphism.

□

We will now give an alternative but equivalent definition of the Tate cohomology groups.

Let

$$\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$$

be a free resolution of $\mathbb{Z}$ in the category of G-modules.

By dualizing, get an exact sequence

$$0 \to \mathbb{Z} \to \mathrm{Hom}(P_0, \mathbb{Z}) \to \mathrm{Hom}(P_1, \mathbb{Z}) \to \mathrm{Hom}(P_2, \mathbb{Z}) \to \cdots$$

For $q \leq -1$ define $P_q = \mathrm{Hom}(P_{-1-q}, \mathbb{Z})$, so

$$0 \to \mathbb{Z} \to P_{-1} \to P_{-2} \to P_{-3} \to \cdots$$

is an exact sequence. We can then join the two exact sequences to get

$$\cdots \to P_2 \to P_1 \to P_0 \to P_{-1} \to P_{-2} \to P_{-3} \to \cdots$$

We can then define $\hat{H}^q(G, A), q \in \mathbb{Z}$ as the homology of the complex $\mathrm{Hom}_G(P_*, A)$, $q \in \mathbb{Z}$.

This is equivalent to our previous definition: we'll check this for the cases of $q \geq 1$ and $q \leq -2$. For $q \geq 1$ we have $\hat{H}^q(G, A) = H^q(G, A)$, as before.

We will now check that for $\hat{H}^{-1-q}(G, A) \cong H_q(G, A)$ for $q \geq 1$. To do this, it will be enough to check that $\mathrm{Hom}_G(P_{-1-q}, A) \cong P_q \otimes_G A$ for $q \geq 0$.

First, we observe that $\mathrm{Hom}_{\mathbb{Z}}(P_{-1-q}, A) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(P_q, \mathbb{Z}), A) \cong P_q \otimes_{\mathbb{Z}} A$ as P_q is a free $\mathbb{Z}$-module. Next, take G-invariants of both sides, to get

$$\mathrm{Hom}_G(P_{-1-q}, A) \cong P_q \otimes_G A.$$

Now, because the free module $P_q \cong \mathbb{Z}[G]^m$ for some m, we have that $P_q \otimes_G A \cong \mathbb{Z}[G] \otimes A^m$, which is induced.

Remark. One has to be a little careful here, because the action on A^m is not the trivial action. However it's still the case that $\mathbb{Z}[G] \otimes A^m \cong \oplus_{g \in G} g(1 \otimes A^m)$, so is induced/coinduced.

From the proof of the previous theorem, we have that $N^* : (P_q \otimes A)^G \to (P_q \otimes A)_G$ is an isomorphism. But $(P_q \otimes A)_G$ is equal to $P_q \otimes_G A$, as desired.

The cases $q = 0, -1$ can be checked separately, see page 103 of Cassels-Frohlich.

17 November 5

17.1 Tate Cohomology for Cyclic Groups

Example. $G = C_n = \langle t \mid t^n = 1 \rangle$. Recall that a free resolution is given by

$$\cdots \longrightarrow \mathbb{Z}[G] \xrightarrow{\times(t-1)} \mathbb{Z}[G] \xrightarrow{\times N} \mathbb{Z}[G] \xrightarrow{\times(t-1)} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z}$$

If we apply $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ to this, we get

$$\mathbb{Z} \xrightarrow{\epsilon^*} \mathbb{Z}[G] \xrightarrow{\times(t^{-1}-1)} \mathbb{Z}[G] \xrightarrow{\times N} \mathbb{Z}[G] \xrightarrow{\times(t^{-1}-1)} \mathbb{Z}[G] \longrightarrow \cdots$$

using the isomorphism of G-modules $\mathbb{Z}[G] \cong \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ given by sending $1 \in \mathbb{Z}[G]$ to the function $\phi_1 : \mathbb{Z}[G] \to \mathbb{Z}$ given by $\phi_1(\sum_g c_g g) = c_1$. More generally, this sends $g \in \mathbb{Z}[G]$ to $\phi_g : \mathbb{Z}[G] \to \mathbb{Z}$.

Joining these up, we can check that the map $P_0 \to P_{-1}$ sends $1 \to N$, so must be multiplication by N, and our complete resolution is:

$$\begin{array}{ccccccccccccccccc}
\cdots & \longrightarrow & \mathbb{Z}[G] & \xrightarrow{\times(t-1)} & \mathbb{Z}[G] & \xrightarrow{\times N} & \mathbb{Z}[G] & \xrightarrow{\times(t-1)} & \mathbb{Z}[G] & \xrightarrow{\times N} & \mathbb{Z}[G] & \xrightarrow{\times(t^{-1})} & \mathbb{Z}[G] & \xrightarrow{\times N} & \mathbb{Z}[G] & \xrightarrow{\times(t^{-1}-1)} & \mathbb{Z}[G] & \longrightarrow & \cdots \\
 & & \| & & \| & & \| & & \| & & \| & & \| & & \| & & \| & & \\
 & & P_3 & & P_2 & & P_1 & & P_0 & & P_{-1} & & P_{-2} & & P_{-3} & & P_{-4} & &
\end{array}$$

Applying the functor $\mathrm{Hom}_G(\cdot, A)$ obtain chain complex

$$\begin{array}{ccccccccccccccc}
\cdots & \longleftarrow & A & \xleftarrow{\times N} & A & \xleftarrow{\times(t-1)} & A & \xleftarrow{\times N} & A & \xleftarrow{\times(t^{-1}-1)} & A & \longleftarrow & \cdots \\
 & & \| & & \| & & \| & & \| & & \| & & \\
 & & \mathrm{Hom}_G(P_2, A) & & \mathrm{Hom}_G(P_1, A) & & \mathrm{Hom}_G(P_0, A) & & \mathrm{Hom}_G(P_{-1}, A) & & \mathrm{Hom}_G(P_{-2}, A) & &
\end{array}$$

Finally obtain: $\hat{H}^{2q}(G, A) = \hat{H}^0(G, A) = A^G/NA$ and $\hat{H}^{2q+1}(G, A) = \hat{H}^{-1}(G, A) = \ker N/(t-1)A$.

17.2 Restriction and corestriction for Tate cohomology

With Tate cohomology, we can dimension shift both up and down.

For any G module A, define A^+ to be the cokernel of the natural map $A \to \mathrm{coInd}^G(A)$, and define A^- to be the kernel of the natural map $\mathrm{Ind}^G(A) \to A$ so that we have short exact sequences

$$0 \to A \to \mathrm{coInd}^G(A) \to A^+ \to 0$$
$$0 \to A^- \to \mathrm{Ind}^G(A) \to A \to 0.$$

Then the long exact sequence in Tate cohomology yields isomorphisms

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

We can use this to define $\mathrm{Res}_q : \hat{H}^q(G, A) \to \hat{H}^q(H, A)$ and $\mathrm{Cor}_q : \hat{H}^q(H, A) \to \hat{H}^q(G, A)$ for all $q \in \mathbb{Z}$.

In the case of restriction, we already have defined these maps for $q \geq 1$. We now define them for all q by downwards induction: assume we already know how to define Res_{q+1}. Then we define Res_q to be the unique map that fills the commutative square

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

Likewise, we can define Cor_q for all q.

The maps Res_q and Cor_q are functorial, and compatible with formation of long exact sequences, in that for every short exact sequence $0 \to A \to B \to C \to 0$ we have commutative diagrams

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

and

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

The proof of this is by dimension shifting/diagram chase.

Furthermore, the functors $\mathrm{Res}_q : \hat{H}^q(G, A) \to \hat{H}^q(H, A)$ are uniquely determined by this property of compatibility with exact sequences plus the property that $\mathrm{Res}_0 : \hat{H}^0(G, A) \to \hat{H}^0(H, A)$ is induced by the inclusion $A^G \to A^H$. The analogous statement is true for Cor_q.

We won't give an explicit description of Res_q and Cor_q in all dimensions, but we will do the following important cases.

Theorem 17.1. *The map* $\mathrm{Cor}_0 : \hat{H}^0(H, A) \to \hat{H}^0(G, A)$ *is induced by the map* $N_{G/H} : A^H \to A^G$ *defined as*

$$N_{G/H}(a) = \sum_{g \in G/H} ga.$$

The map $\mathrm{Res}_{-1} : \hat{H}^{-1}(G, A) \to \hat{H}^{-1}(H, A)$ *is induced by the map* $N'_{G/H} : A_G \to A_H$ *defined as*

$$[a] \mapsto \sum_{g \in G/H} [g^{-1}a] = \sum_{g \in H\backslash G} [ga].$$

Proof. We'll do the argument for Res_{-1}; the argument for Cor_0 is similar.

It's enough to show that if $0 \to A \to B \to C \to 0$ is exact, then the following diagram commutes:

$$\begin{array}{ccc} \hat{H}^{-1}(G, C) & \xrightarrow{\delta} & \hat{H}^{0}(G, A) \\ \downarrow{\scriptstyle N'_{G/H}} & & \downarrow{\scriptstyle \mathrm{Res}_0} \\ \hat{H}^{-1}(H, C) & \xrightarrow{\delta} & \hat{H}^{0}(H, A). \end{array}$$

Indeed suppose $[c] \in \hat{H}^{-1}(G, C) = \ker N^*_G : (C_G \to C^G)$. Let $b \in B$ be a preimage of $c \in C$. Then can compute

$$\mathrm{Res}_0(\delta c) = [N_G(b)] \in \hat{H}^0(H, A) = A^H / N_H A.$$

In the other direction, have $\mathrm{Res}_{-1}(c) = \sum_{g \in H\backslash G} [gc]$, and

$$\delta \,\mathrm{Res}_{-1}(c) = \sum_{g \in H\backslash G} [N_H(gb)] = \sum_{g \in H\backslash G} \sum_{h \in H} [hgb] = [N_G(b)]$$

as desired. □

Proposition 17.2. *If* G *is a group and* H *is any subgroup, then, for all* q*, the map* $\mathrm{Cor} \circ \mathrm{Res} : H^q(G, A) \to H^q(G, A)$ *is multiplication by* $[G : H]$*.*

Proof. By dimension shifting, enough to check this when $q = 0$. If $[a] \in H^0(G, A) = A^G / NA$, then

$$\mathrm{Cor}(\mathrm{Res}\, a) = \sum_{g \in G/H} ga = \sum_{g \in G/H} a = [G : H]a.$$

□

We obtain the following corollaries.

Corollary 17.3. *a) If* $n = |G|$*, then* $\hat{H}^q(G, A)$ *is an* n*-torsion group*

b) If G *is finite and* A *is finitely generated over* $\mathbb{Z}[G]$*, then* $\hat{H}^q(G, A)$ *is finite.*

c) If the multiplication by n *map* $A \to A$ *is an isomorphism, then* $\hat{H}^q(G, A) = 0$*.*

d) If G_p *is a Sylow* p*-subgroup of* G*, then* $\mathrm{Res} : \hat{H}^q(G, A) \to \hat{H}^q(G_p, A)$ *maps the Sylow* p*-subgroup* $(\hat{H}^q(G, A))_p$ *injectively into* $\hat{H}^q(G_p, A)$

e) If for fixed q *and every prime* p, $\hat{H}^q(G_p, A) = 0$ *where* G_p *is a Sylow* p*-subgroup of* G*, then* $\hat{H}^q(G, A) = 0$*.*

Proof. For a), we apply the previous proposition when $H = \{1\}$. This then tells us that the multiplication by n-map $\times n : \hat{H}^q(G, A) \to \hat{H}^q(G, A)$ factors through $\hat{H}^q(H, A) = 0$, so multiplication by n must be the zero map.

For b), the explicit description shows that $\hat{H}^q(G, A)$ is a finitely generated $\mathbb{Z}$-module. By part a) it's also n-torsion, hence finite.

Part c) follows immediately from a).

For d), note that $\mathrm{Cor} \circ \mathrm{Res}$ is multiplication by $[G : G_p]$, which has order prime to p, so is injective on $(\hat{H}^q(G, A))_p$. Hence the same is true of Res.

Finally, e) follows immediately from d), since $(\hat{H}^q(G, A))_p$ must be 0 for all p. □

17.3 Cup Products

If A, B are G-modules, one can define a bilinear cup product $\cup : H^q(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$. If G is finite, can do the same on Tate cohomology, get a cup product map: $\hat{H}^p(G, A) \times \hat{H}^q(G, B) \to \hat{H}^{p+q}(G, A \otimes B)$.

We'll start by giving an axiomatic description:

The family of bilinear maps $\cup : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$ are characterized by the following properties:

a) $\cup$ is natural in both A and B: if $f : A \to A'$, $g : B \to B'$ are morphisms, $f_*(a) \cup g_*(b) = (f \otimes g)_*(a \cup b)$ for all $a \in H^p(G, A)$, $b \in H^q(G, B)$.

b) When $p = q = 0$, $\cup : H^0(G, A) \times H^0(G, B) \to H^0(G, A \otimes B)$ is induced by the map $A^G \otimes B^G \to (A \otimes B)^G$.

c) Suppose that both sequences $0 \to A \to A' \to A'' \to 0$ and $0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$ are exact.

Then for $a'' \in H^p(G, A'')$ and $b \in H^q(G, B)$ have

$$\delta(a'' \cup b) = \delta(a'') \cup b.$$

On the other side, if $0 \to B \to B' \to B'' \to 0$ is exact and so is $0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$, then

$$\delta(a \cup b'') = (-1)^p a \cup \delta(b'').$$

for $a \in H^p(G, A)$ and $b'' \in H^p(G, B'')$

There are multiple different ways of defining these cup-products. One method is to use dimension-shifting: note that the short exact sequences used in dimension-shifting

both split in the category of $\mathbb{Z}$-modules, so they remain exact after tensoring over $\mathbb{Z}$ with another module B.

Another approach uses resolutions. (This is done e.g. in Chapter V of *Cohomology of Groups* by Ken Brown). If one has projective/ complete resolutions for a group G and for for another group H, one can tensor them together to build a resolution for $G \times H$. This then lets one define a cross product

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

If $G = H$ then we compose with the restriction map $H^q(G \times G, A \otimes B) \to H^q(G, A \otimes B)$ coming from the diagonal inclusion $G \hookrightarrow G \times G$ to obtain the cup product.

The cup product maps also have nice descriptions in terms of cochains, which we'll consider next time.

18 More on Cup Product (not covered in lecture)

The cup product maps also have nice descriptions in terms of cochains.

If f and f' are homogeneous cochains, then define $f \cup f'$ by

$$f \cup f'(g_0, \ldots, g_{p+q}) = f(g_0, \ldots, g_p) \otimes f'(g_p, \ldots, g_{p+q}).$$

If ϕ and ϕ' are inhomogeneous cochains, define $\phi \cup \phi'$ by

$$\phi \cup \phi'(g_1, \ldots, g_{p+q}) = \phi(g_1, \ldots, g_p) \otimes g_1 \ldots g_p \phi'(g_{p+1}, \ldots, g_q).$$

Cassels and Fröhlich give explicit descriptions for cup product in negative dimensions, in terms of the standard resolution. Neukirch's Bonn Lectures work out some low-dimensional cases of cup product by dimension-shifting.

Cup product has the following properties:

Associativity: $(a \cup b) \cup c = (a \cup (b \cup c))$.

Supercommutativity. $a \cup b = (-1)^{pq} b \cup a$ Compatibility with restriction/corestriction: $\mathrm{Res}(a \cup b) = \mathrm{Res}(a) \cup \mathrm{Res}\, b$ and $\mathrm{Cor}(a \cup \mathrm{Res}\, b) = \mathrm{Cor}(a) \cup b$.

All of these can be proved by checking for $p = q = 0$ and then dimension-shifting.

For instance, to check the last one, if $H \subset G$, $a \in A^H$, $b \in B^G$, have

$$N_{G/H}(a \otimes b) = \sum_{g \in G} g(a \otimes b) = \sum_{g \in G} ga \otimes b = N_{G/H}(a) \otimes b$$

which proves the result for $q = 0$.

Also we'll later use the following special cases of cup product, which are on the problem set:

Proposition 18.1. *Let* G *be a finite group, and let* A *and* B *be* G*-modules. Let*

$$[a] \in \hat{H}^{-1}(G, A) \cong (\ker N : A \to A)/I_G A$$

be a cohomology class represented by some $a \in A$*. Let*

$$[\phi] \in \hat{H}^1(G, B)$$

be a cohomology class represented by some $\phi \in Z^1(G, B)$*.*

Then

$$[a] \cup [\phi] = -\left[\sum_{g \in G} ga \otimes \phi(g)\right] \in \hat{H}^0(G, A \otimes B)$$

Proposition 18.2.

Let G *be a finite group and let* B *be a* G*-module. Let* $[g] \in \hat{H}^{-2}(G, \mathbb{Z}) \cong G^{ab}$ *be the cohomology class represented by some* $g \in G$*. Let* $[\phi] \in \hat{H}^1(G, B)$ *be a cohomology class represented by some* $\phi \in Z^1(G, B)$*.*

Then

$$[g] \cup [\phi] = [\phi(g)] \in \hat{H}^{-1}(G, B).$$

19 November 12

19.1 Galois cohomology and Hilbert's Theorem 90

Now we're going to do some Galois cohomology.

If L/K is a finite Galois extension and A is a $\mathrm{Gal}(L/K)$-module, we write $H^q(L/K, A) = H^q(\mathrm{Gal}(L/K), A)$, and likewise, for $\hat{H}^q$.

We've previously noted that the Normal Basis theorem says that

Proposition 19.1. L^+ *is a coinduced* G*-module.*

Corollary 19.2. $\hat{H}^q(L/K, L^+) = 0$ *for all* $q \in \mathbb{Z}$*.*

(In the case that L is characteristic 0, this is also a consequence the fact that the multiplication by n map $L^+ \to L^+$ is an isomorphism).

Now we'll show that $L^\times$ has trivial H^1. This is known as *Hilbert's theorem 90*, though Hilbert only actually proved the corollary that we'll give later, and this extension is due to Noether.

Theorem 19.3 (Hilbert 90)**.** $H^1(L/K, L^\times) = 0$*.*

Proof. Suppose $\phi \in C^1(L/K, L^\times)$ is an inhomogeneous cocycle, so $\phi(gh) = \phi(g) \cdot (g\phi(h))$. Must show that ϕ is a coboundary, equivalently that there exists $a \in L$ such that $\phi(g) = a/ga$ for all $g \in G$.

Choose $x \in L$ such that $a = \sum_{g \in G} \phi(g) \cdot gx \neq 0$. This is possible because of linear independence of automorphisms.

Then we manipulate

$$\begin{aligned} a &= \sum_{g' \in G} \phi(g') \cdot g'x \\ &= \sum_{gg' \in G} \phi(gg') \cdot gg'x \\ &= \sum_{g' \in G} \phi(g) \cdot g\phi(g') \cdot gg'x \\ &= \phi(g) \sum_{g' \in G} g(\phi(g') \cdot g'x) \\ &= \phi(g) g(a) \end{aligned}$$

so this a has the desired property. □

In the case where L/K is cyclic, this specializes to

Theorem 19.4 (Original Hilbert 90)**.** *Suppose* L/K *is cyclic with generator* g*. Then if* $x \in L^\times$ *with* $N_{L/K}x = 1$*, there exists* $y \in L^\times$ *with* $x = gy/y$*.*

Proof. By our computation of homology for cyclic groups, we have

$$1 = H^1(L/K, L^\times) = \ker(N : L^\times \to L^\times) / \operatorname{im}(g - 1 : L^\times \to L^\times).$$

□

Example. If $L/K = \mathbb{Q}(i)/\mathbb{Q}$, then this is saying that any $x \in \mathbb{Q}(i)$ with $x\overline{x} = |x|^2 = 1$ is of the form $x = y/\overline{y}$ for $y \in \mathbb{Q}(i)$. If we write out $y = a + bi$, and rescale so $a, b \in \mathbb{Z}$, this gives

$$x = \frac{a + bi}{a - bi} = \frac{(a + bi)^2}{a^2 + b^2} = \frac{a^2 - b^2}{a^2 + b^2} + \frac{2ab}{a^2 + b^2} i$$

leading to the well-known parametrization of Pythagorean triples.

19.2 Cohomology of profinite groups

Let G be a group: we say that G is profinite if $G = \varprojlim G_i$ where each G_i is finite. Recall that in such a setting we have a natural topology on G, in which the sets $\ker : G \to G_i$ form a neighborhood basis at the identity.

Theorem 19.5. *Let* G *be a topological group. TFAE:*

a) G *is profinite*

b) G *is compact Hausdorff and totally disconnected*

c) $G = \varprojlim G/U$ *where* U *runs over the open finite index subgroups of* G*.*

Proof is not hard and is in Cassels-Fröhlich. Note also that if G is profinite, an open subgroup of G must be finite index by compactness. Also any open subgroup $U \subset G$ must contain an open normal subgroup (take the intersection of all conjugates of U).

Definition. If G is a profinite group, a discrete G-module A is an abelian group A with an action of G on A satisfying one of the two equivalent conditions:

- $G \times A \to A$ is continuous with respect to the discrete topology on A.
- $A = \bigcup_{U \subset G \text{ open}} A^U$.

For every $U \subset G$ open normal have a group $H^q(G/U, A^U)$. If $V \subset U$, have an inflation map $\mathrm{Inf}_{U,V} : H^q(G/U, A^U) \to H^q(G/V, A^V)$ (since $G/U = (G/V)/(U/V)$ and $A^U = (A^V)^{(U/V)}$.

Then we define

$$H^q(G, A) = \varinjlim_U H^q(G/U, A^U)$$

where U runs over the open normal subgroups of G $\varinjlim_U$ denotes a direct limit: that is, $\varinjlim_U H^q(G/U, A^U)$ is the quotient of $\coprod_U H^q(G/U, A^U)$ by the equivalence relation generated by $x \sim \mathrm{Inf}_{U,V}(x)$ for all open normal subgroups U, V of G with $V \subset U$ and all $x \in H^q(G/U, A^U)$.

If K is a field and A is a discrete $\mathrm{Gal}(\bar{K}/K)$ module, write $H^1(K, A) = H^1(\mathrm{Gal}(\bar{K}/K), A)$.

Example. Profinite Hilbert's Theorem 90:

$$H^1(K, (K^{\mathrm{sep}})^\times) = \varinjlim H^1(L/K, L^\times) = \varinjlim 1 = 1$$

where the direct limits above run through all finite Galois extensions L/K.

Which parts of group cohomology theory carry over to the profinite setting?

Still have long exact sequence (direct limits preserve exactness).

We can define cohomology using cochains, but they have to be continuous cochains: that is, $\phi : G^n \to A$ must factor through $(G/U)^n$ for some open $U \subset G$.

Inflation and restriction still work, as long as $H \subset G$ is a closed subgroup (in which case it is necessarily profinite).

Can't define Tate cohomology (we don't have inflation in negative dimensions, and the groups aren't compatible in the right way).

Cup products still work.

19.3 $H^2(L/K, L^\times)$ when L/K is unramified.

We'll now compute $H^2(L/K, L^\times)$ for finite unramified Galois extensions L/K of local fields. (Sometimes people just call this $H^2(L/K)$. Also, some terminology: the *Brauer group* of K is $H^2(K^{sep}/K, (K^{sep})^\times)$. This has a special name because it was originally defined in terms of central simple algebras and later recognized as a cohomology group. We'll explain the connection to central simple algebras later in this course, possibly next semester.)

One way to do this is to note that, for L/K finite unramified, we know that $\mathrm{Gal}(L/K)$ is cyclic, so $H^2(L/K, L^\times)$ is canonically isomorphic to $\hat{H}^0(L/K, K^\times) = K^\times/NL^\times$, which we previously saw was cyclic of order $n = [L : K]$.

However, we'll actually compute $H^2(L/K, L^\times)$ in a second way that makes it easier to see what the inflation/restriction maps we get from varying L and K are.

Lemma 19.6. $\hat{H}^q(L/K, \mathcal{O}_L^\times) = 0$ *for all* q.

Proof. Because of periodicity, enough to do $q = 0$ and $q = 1$. For $q = 0$, know that $N : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective. For $q = 1$, the short exact sequence

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0$$

gives a long exact sequence

$$K^\times \xrightarrow{v_L} \mathbb{Z} \to H^1(L/K, \mathcal{O}_L^\times) \to H^1(L/K, L^\times).$$

On the one side, L/K is unramified, so $v_L : K^\times \to \mathbb{Z}$ is surjective. On the other side $H^1(L/K, L^\times) = 0$. Hence $H^1(L/K, \mathcal{O}_L^\times) = 0$. □

Using (again) the long exact sequence coming from the short exact sequence

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

and applying the lemma above, we see that the map $v_* : H^2(L/K, L^\times) \to H^2(L/K, \mathbb{Z})$ is an isomorphism.

Now we dimension-shift, using the short exact sequence

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

to obtain an isomorphism $\delta : H^1(L/K, \mathbb{Q}/\mathbb{Z}) \cong H^2(L/K, \mathbb{Z})$.

Now $H^1(L/K, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$ and $\mathrm{Gal}(L/K)$ is cyclic with canonical generator Frob of order n, so we get a canonical isomorphism $H^1(L/K, \mathbb{Q}/\mathbb{Z}) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ given by $\phi \mapsto \phi(\mathrm{Frob})$.

We let $\mathrm{inv}_{L/K} : H^2(L/K, L^\times) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ be the composition of the maps

$$H^2(L/K, L^\times) \xrightarrow{v_*} H^2(L/K, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(L/K, \mathbb{Q}/\mathbb{Z}) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

We now wish to determine

$$H^2(K^{unr}/K, (K^{unr})^\times) = \varinjlim_{L/K \text{ finite unram}} H^2(L/K, L^\times) = \varinjlim_n H^2(K_n/K, K_n^\times)$$

where K_n/K is the unique unramified extension of degree n. To do this we must determine the inflation maps $H^2(K_n/K, K_n^\times) \to H^2(K_N/K, K_N^\times)$ where $n \mid N$.

To do this, we write out the large diagram

$$\begin{array}{ccccccc} H^2(K_n/K, K_n^\times) & \xrightarrow{v_*} & H^2(K_n/K, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(K_n/K, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \\ \downarrow \text{Inf} & & \downarrow \text{Inf} & & \downarrow \text{Inf} & & \downarrow \\ H^2(K_N/K, K_N^\times) & \xrightarrow{v_*} & H^2(K_N/K, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(K_N/K, \mathbb{Q}/\mathbb{Z}) & \longrightarrow & \frac{1}{N}\mathbb{Z}/\mathbb{Z} \end{array}$$

and observe that it commutes. Indeed, the first two squares commute because inflation is natural and compatible with forming long exact sequences (it's important here that K_n and K_N are both unramified extensions of K, so their valuations agree). The last square commutes because the restriction map $\mathrm{Gal}(K_N/K) \to \mathrm{Gal}(K_n/K)$ sends $\mathrm{Frob}(K_N/K)$ to $\mathrm{Frob}(K_n/K)$ (restricting to a subfield doesn't change the defining property of the Frobenius).

Hence we have

$$H^2(K^{unr}/K, (K^{unr})^\times) \cong \varinjlim_n H^2(K_n/K, K_n^\times) \cong \varinjlim_n \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}.$$

As in the finite case, we denote the isomorphism $H^2(K^{unr}/K, (K^{unr})^\times) \to \mathbb{Q}/\mathbb{Z}$ by inv_K. For any L/K finite we can view $H^2(L/K, L^\times)$ as a subgroup of $H^2(K^{unr}/K, (K^{unr})^\times)$, and then the restriction of inv_K to $H^2(K^{unr}/K, (K^{unr})^\times)$ that we've defined above is $\mathrm{inv}_{L/K}$.

20 November 16

20.1 inv and change of base field

Now, suppose L/K is a finite extension of degree n; don't need to assume unramified or Galois. Then $L^{unr} = L \cdot K^{unr}$, since $K^{unr} = \bigcup_{(r,p)=1} K(\zeta_r)$ (p the residue characteristic) and likewise $L^{unr} = \bigcup_{(r,p)=1} L(\zeta_r)$. It follows that the natural map $\mathrm{Gal}(L^{unr}/L) \to \mathrm{Gal}(K^{unr}/K)$ is injective.

Hence we can make a restriction map:

$\mathrm{Res} : H^2(K^{unr}/K, (K^{unr})^\times) \to H^2(L^{unr}/L, (L^{unr})^\times)$.

Proposition 20.1. $\mathrm{inv}_L \circ \mathrm{Res} = n \cdot \mathrm{inv}_K$.

Proof. Again this is proof by large commutative diagram. Let $e = e_{L/K}$ be the ramification index, and let $f = [\ell : k]$ be the inertia degree, so $n = ef$.

We write down the following diagram:

$$\begin{array}{ccccccc}
H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times) & \xrightarrow{e\cdot(v_K)_*} & H^2(K^{\mathrm{unr}}/K, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(K^{\mathrm{unr}}/K, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{f\cdot \mathrm{eval}_{\mathrm{Frob}_K}} & \mathbb{Q}/\mathbb{Z} \\
\downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \downarrow \mathrm{Res} & & \| \\
H^2(L^{\mathrm{unr}}/L, (L^{\mathrm{unr}})^\times) & \xrightarrow{(v_L)_*} & H^2(L^{\mathrm{unr}}/L, \mathbb{Z}) & \xrightarrow{\delta^{-1}} & H^1(L^{\mathrm{unr}}/L, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\mathrm{eval}_{\mathrm{Frob}_L}} & \mathbb{Q}/\mathbb{Z}
\end{array}$$

The first square commutes because

$$\begin{array}{ccc}
(K^{\mathrm{unr}})^\times & \xrightarrow{e\cdot v_K} & \mathbb{Z} \\
\downarrow & & \| \\
(L^{\mathrm{unr}})^\times & \xrightarrow{v_L} & \mathbb{Z}
\end{array}$$

commutes (definition of e) and restriction is natural. The second square commutes because restriction is compatible with long exact sequences. The third square commutes because the image of Frob_L in $\mathrm{Gal}(K^{\mathrm{unr}}/K)$ is equal to $f \cdot \mathrm{Frob}_K$ (they both act as $x \mapsto x^{p^f}$ on the residue field extension $\bar{k}/k$.) □

20.2 Construction of the fundamental class $u_{L/K}$

Let L/K be a finite Galois extension of local fields, of degree n.

Let K_n/K be the unique unramified extension of degree n, and let $L_n = LK_n$ (so L_n/L is an extension of degree dividing n).

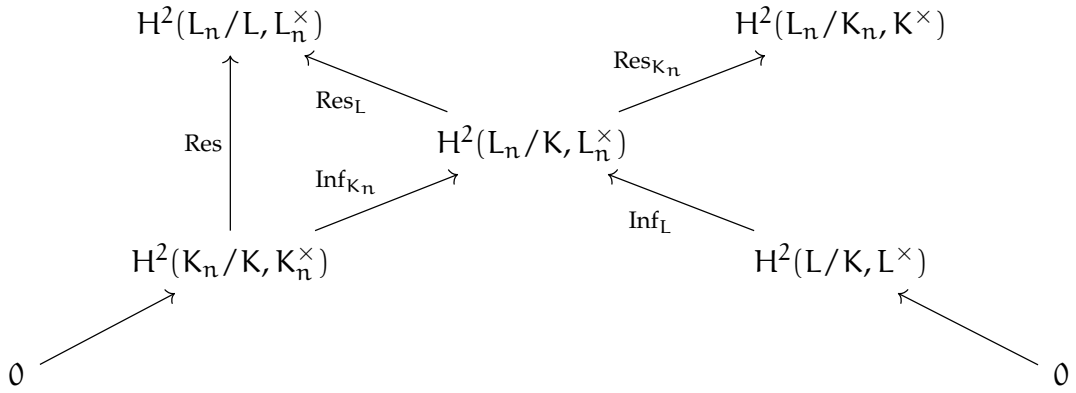
Let $u_n = u_{K_n/K} \in H^2(K_n/K, K_n^\times)$ be the element such that $\mathrm{inv}_{K_n/K}(u_n) = \frac{1}{n}$. Then we have a diagram

$$\begin{array}{ccccc}
H^2(L_n/L, L_n^\times) & \hookrightarrow & H^2(L^{\mathrm{unr}}/L, (L^{\mathrm{unr}})^\times) & \xrightarrow{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z} \\
\mathrm{Res}\uparrow & & \mathrm{Res}\uparrow & & \| \\
H^2(K_n/K, K_n^\times) & \hookrightarrow & H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times) & \xrightarrow{n\cdot\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z}.
\end{array}$$

The maps in the bottom row send the element $u_n \in H^2(K_n/K, K_n^\times)$ to $0 \in \mathbb{Q}/\mathbb{Z}$. Since the maps in the top row are all injections, we must have $\mathrm{Res}(u_n) = 0$.

Now, we note that the restriction map $\mathrm{Res} : H^2(K_n/K, K_n^\times) \to H^2(L_n/L, L_n^\times)$ factors as a composition of the inflation map $\mathrm{Inf}_{K_n} : H^2(K_n/K, K_n^\times) \to H^2(L_n/K, L_n^\times)$ with the restriction map $\mathrm{Res}_L : H^2(L_n/K, L_n^\times) \to H^2(L_n/L, L_n^\times)$. We can put this inside a large

commutative diagram



In this diagram, both diagonals are inflation-restriction exact sequences. We have $0 = \mathrm{Res}(u_n) = \mathrm{Res}_L(\mathrm{Inf}_{K_n} u_n)$, so $\mathrm{Inf}_{K_n} u_n \in \ker \mathrm{Res}_L = \mathrm{im}\, \mathrm{Inf}_L$. Define $u_{L/K}$ to be the unique element $H^2(L/K, K^\times)$ with $\mathrm{Inf}_L(u_{L/K}) = \mathrm{Inf}_{K_n}(u_n)$. Since u_n has order n, and both inflation maps are injective, $u_{L/K}$ has the same order n.

This shows that $H^2(L/K, L^\times)$ contains a cyclic subgroup of order n generated by $u_{L/K}$. Next we'll show that $|H^2(L/K, L^\times)| \leq n$, so in fact we have equality and $u_{L/K}$ generates.

20.3 Bounding the size of $H^2(L/K, L^\times)$

We first consider the case when L/K is cyclic of degree n. Then $H^2(L/K, L^\times) = \hat{H}^0(L/K, L^\times) = K^\times / NL^\times$. In this case we'll be able to in fact directly prove that $|\hat{H}^0(L/K, L^\times)| = n$.

I know two proofs of this: one is for the case when L/K is cyclic of prime order, and is a very hands-on proof using the filtrations of $\mathcal{O}_K^\times$ and $\mathcal{O}_L^\times$: it can be found in these notes of Barry Mazur at https://canvas.harvard.edu/courses/34189/files/folder/251A/Lecture_Notes_and_Homework_98295/Lecture_Notes?preview=4354316.

The other is cohomological and uses the Herbrand quotient: this is the one we'll do.

Lemma 20.2. *There exists an open (hence finite index) subgroup V of $\mathcal{O}_L^\times$ such that $\hat{H}^q(L/K, V) = 0$ for all q.*

Proof. (Characteristic 0 only: for characteristic p see the second proof of Cassels-Frohlich page 134, which does a similar thing while avoiding use of the p-adic exponential).

Actually, we'll show that V is co-induced. First, recall that L/K is co-induced, so there exists $a \in L$ such that $L = \bigoplus_{g \in G} K \cdot ga$. Without loss of generality $v_L(a) > r$, where r will be chosen later. Let $A = \bigoplus_{g \in G} \mathcal{O}_K \cdot ga$. Then A is an open subgroup of $\pi_L^r \mathcal{O}_L$. Now take r large enough that $\exp_p : \pi_L^r \mathcal{O}_L \to U_{L,r}$ is an isomorphism. Let $V = \exp_p(A)$: then V is open in $\mathcal{O}_L^\times$, and $V \cong A$ which is co-induced by construction. □

Recall from HW that if G is a cyclic group and A a G-module, the Herbrand quotient $h(A)$ is defined by

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

Proposition 20.3. *The Herbrand quotient* $h(\mathcal{O}_L^\times) = 1$.

Proof. Use short exact sequence $0 \to V \to \mathcal{O}_L^\times \to \mathcal{O}_L^\times/V \to 0$. The Herbrand quotient $h(V) = 1$ by the previous lemma, and the Herbrand quotient $h(\mathcal{O}_L^\times/V) = 1$ by homework since V is finite index.

So apply the HW again for multiplicativity of Herbrand quotient in long exact sequences. □

Proposition 20.4. *The Herbrand quotient* $h(L^\times) = [L : K]$

Proof. Use short exact sequence $0 \to \mathcal{O}_L^\times \to L^\times \to \mathbb{Z} \to 0$ and HW. □

Now, we know $|\hat{H}^1(L/K, L^\times)| = 1$, so $|\hat{H}^0(L/K, L^\times)| = [L : K] = n$. as desired.

To do the general case:

Theorem 20.5. *If* L/K *is a Galois extension of local fields of degree* n*, then* $|H^2(L/K, L^\times)| \leq n$*. (in fact* $| n$*)*

Proof. We induct on $[L : K]$: if $[L : K]$ is prime the extension is cyclic, which we already know. Otherwise, since $\mathrm{Gal}(L/K)$ is solvable (ramification filtration!) there exists a nontrivial normal subgroup of $\mathrm{Gal}(L/K)$, which leads to an intermediate Galois exension M/K. We then have an inflation-restriction sequence

$$0 \to H^2(M/K, M^\times) \to H^2(L/K, L^\times) \to H^2(L/M, L^\times)$$

so, using the inductive hypothesis

$$|H^2(L/K, L^\times)| \leq |H^2(M/K, M^\times)| \cdot |H^2(L/M, L^\times)| \leq [L : M][M : K] = [L : K].$$

and the induction goes through. □

We can now draw some conclusions:

Theorem 20.6. *If* L/K *is a finite Galois extension of local fields, then* $H^2(L/K, L^\times)$ *is cyclic of order* $n = [L : K]$*, with generator* $u_{L/K}$.

Proof. As explained above, this follows from the previous theorem plus the fact that $u_{L/K}$ has order n. □

Theorem 20.7. *If K is a local field, then the inflation map*

$$H^2(K^{unr}/K, (K^{unr})^\times) \to H^2(K^{sep}/K, (K^{sep})^\times)$$

is an isomorphism.

Hence have isomorphism $\mathrm{inv}_K : H^2(K^{sep}/K, (K^{sep})^\times) \to \mathbb{Q}/\mathbb{Z}$.

Proof. We already know that inflation is injective. To prove surjectivity: any element of $H^2(K^{sep}/K, (K^{sep})^\times)$ is represented by some element in some $H^2(L/K, L^\times)$, which we can write as $a \cdot u_{L/K}$ for some $a \in \mathbb{Z}/[L:K]\mathbb{Z}$.

Let K_n be the unramified degree n extension of K. By construction, $u_{L/K}$ and $u_{K_n/K}$ map to the same element in $H^2(L_n/K, L_n^\times)$. Hence $a \cdot u_{L/K}$ and $a \cdot u_{K_n/K}$ also map to the same element: so $a \cdot u_{L/K}$ lies in the image of the inflation map as desired. □

Proposition 20.8. *if L/K is a finite extension of local fields, of degree n, then the diagram*

$$\begin{array}{ccc} \mathrm{Br}(K) & \xrightarrow{\mathrm{inv}_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow \mathrm{Res} & & \downarrow n\cdot \\ \mathrm{Br}(L) & \xrightarrow{\mathrm{inv}_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

commutes (where the map on the right is multiplication by n).

Proof. Immediate consequence of Theorem 20.7 and Proposition 20.1. □

Proposition 20.9. *If $E/L/K$ is a tower of local fields with E/K Galois, then* $\mathrm{Res}\, u_{E/K} = u_{E/L}$.

Proof. The elements $u_{E/K} \in H^2(E/K, E^\times)$ and $u_{E/L} \in H^2(E/L, E^\times)$ are uniquely determined by $\mathrm{inv}_K(u_{E/K}) = \frac{1}{[E:K]}$ and $\mathrm{inv}_L(u_{E/L}) = \frac{1}{[E:L]}$. Now use previous proposition. □

Likewise, if $E/L/K$ is a tower with E/K and L/K both Galois, $\mathrm{Inf}(u_{E/K}) = [L:K] \cdot u_{L/K}$).

20.4 Tate's theorem

We are one cohomological theorem away from proving the main theorem of class field theory. We'll state the theorem now and prove it next time.

Theorem 20.10 (Tate)**.** *Let G be a finite group. Suppose that A is a G-module such that for each subgroup $H \subset G$ we have $H^1(H, A) = 0$ and $H^2(H, A)$ is cyclic of order $|H|$. If a generates $H^2(G, A)$ then the cup product map*

$$- \cup a : \hat{H}^q(G, \mathbb{Z}) \to \hat{H}^{q+2}(G, A)$$

is an isomorphism for all $q \in \mathbb{Z}$.

We now check that, if L/K is a Galois extension of local fields, then $G = \mathrm{Gal}(L/K)$, $A = L^\times$ satisfies the requirements. Any subgroup $H \subset G$ is equal to $\mathrm{Gal}(L/M)$ for some M, and then $H^1(H, A) = H^1(L/M, L^\times) = 0$ by Hilbert 90, while $H^2(H, A) = H^2(L/M)$ is cyclic of order $|H|$ by Theorem 20.6.

We now use the conclusion when $q = -2$, taking $a = u_{L/K}$. We have that

$$- \cup u_{L/K} : \hat{H}^{-2}(L/K, \mathbb{Z}) \to \hat{H}^0(L/K, L^\times)$$

is an isomorphism: however we know $\hat{H}^{-2}(L/K, \mathbb{Z}) \cong \mathrm{Gal}(L/K)^{ab}$ while $\hat{H}^0(G, L^\times) \cong K^\times / NL^\times$.

Hence we get a canonical isomorphism:

$$- \cup u_{L/K} : \mathrm{Gal}(L/K)^{ab} \to K^\times / NL^\times$$

the inverse of which is what we'll call the Artin map $\theta_{L/K}$.

Finishing by saying a few words about the proof:

We'll use the problem from the last homework, where we showed that if A is a G-module such that $\hat{H}^q(H, A) = \hat{H}^{q+1}(H, A) = 0$ for all $H \subset G$, then $\hat{H}^q(G, A) = 0$ for all $q \in \mathbb{Z}$.

We'll construct a G-module M with the property that there exists an exact sequence

$$\cdots \to \hat{H}^q(H, \mathbb{Z}) \xrightarrow{-\cup a} \hat{H}^{q+2}(H, A) \to \hat{H}^q(H, M) \to \hat{H}^{q+1}(H, \mathbb{Z}) \xrightarrow{-\cup a} \hat{H}^{q+3}(H, A) \to \cdots$$

for any $H \subset G$. We'll then show that M satisfies the conditions of the homework problem, so $\hat{H}^q(G, A) = 0$ for all q, and hence cup product with a is an isomorphism in all dimensions.

21 November 19

21.1 Proof of Tate's theorem

Last time we stated

Theorem 21.1 (Tate)**.** *Let G be a finite group. Suppose that A is a G-module such that for each subgroup $H \subset G$ we have $H^1(H, A) = 0$ and $H^2(H, A)$ is cyclic of order $|H|$. If a generates $H^2(G, A)$ then the cup product map*

$$- \cup a : \hat{H}^q(G, \mathbb{Z}) \to \hat{H}^{q+2}(G, A)$$

is an isomorphism for all $q \in \mathbb{Z}$.

Proof. The first thing we'll do is dimension-shift twice. We know there exists a module $B = (A^+)^+$ with dimension-shifting isomorphisms $\hat{H}^q(G, B) \cong \hat{H}^{q+2}(G, A)$. Let $[b] \in \hat{H}^0(G, B)$ be the preimage of $a \in \hat{H}^2(G, A)$.

We have the following commutative triangle:

$$\begin{array}{ccc} \hat{H}^q(G, \mathbb{Z}) & \xrightarrow{-\cup a} & \hat{H}^{q+2}(G, A) \\ & \searrow^{-\cup b} & \downarrow \wr \\ & & \hat{H}^q(G, B) \end{array}$$

So it's enough to show that if $\hat{H}^{-1}(H, B) = 0$ for all $H \subset G$ and $\hat{H}^0(H, B)$ is cyclic of order $|H|$, then

$$- \cup b : \hat{H}^q(G, \mathbb{Z}) \to \hat{H}^q(G, B)$$

is an isomorphism for any generator b of $\hat{H}^0(G, B)$.

As mentioned last time, we want to fit the maps

$$- \cup b : \hat{H}^q(G, \mathbb{Z}) \to \hat{H}^q(G, B)$$

into a long exact sequence. Fortunately for us, these maps are all induced by the map $\mathbb{Z} \to B$ given by $n \mapsto n\tilde{b}$ for any $\tilde{b} \in B$ representing the class $b \in H^0(G, B)$. The problem is that the map $n \mapsto n\tilde{b}$ is not necessarily injective. To fix this, we'll replace B by another $\mathbb{Z}[G]$ module with the same cohomology. (If you like topology, you should think of this as a "mapping cylinder" construction.)

Consider the SES

$$0 \to \mathbb{Z} \xrightarrow{i} B \oplus \mathbb{Z}[G] \to M \to 0$$

where: $i : \mathbb{Z} \to B \oplus \mathbb{Z}[G]$ is given by $i(n) = (n\tilde{b}, nN)$ (here as usual $N = \sum_{g \in G} g \in \mathbb{Z}[G]$.)

and $M = \operatorname{cok} i$.

This gives a LES

$$\cdots \xrightarrow{i_*} \hat{H}^{-1}(H, B') \to \hat{H}^{-1}(H, M) \to \hat{H}^0(H, \mathbb{Z}) \xrightarrow{i_*} \hat{H}^0(H, B') \to \hat{H}^0(H, M) \to \hat{H}^1(H, \mathbb{Z}) \xrightarrow{i_*} \cdots$$

Using the commutative triangle

$$\begin{array}{ccc} \hat{H}^q(H, \mathbb{Z}) & \xrightarrow{i_*} & \hat{H}^q(H, B') \\ & \searrow^{\cup b} & \downarrow \wr \\ & & \hat{H}^q(H, B) \end{array}$$

we may replace B with B' everywhere in the long exact sequence to get

$$\cdots \xrightarrow{\cup b} \hat{H}^{-1}(H, B) \to \hat{H}^{-1}(H, M) \to \hat{H}^0(H, \mathbb{Z}) \xrightarrow{\cup b} \hat{H}^0(H, B) \to \hat{H}^0(H, M) \to \hat{H}^1(H, \mathbb{Z}) \xrightarrow{\cup b} \cdots$$

Note that $\hat{H}^{-1}(H, B) = 0$ (assumption) and $\hat{H}^1(H, \mathbb{Z}) = \mathrm{Hom}(H, \mathbb{Z}) = 0$.

We can compute $\hat{H}^0(H, \mathbb{Z}) \cong \mathbb{Z}/|H|\mathbb{Z}$. The group $\hat{H}^0(H, B) = B/N_H B$ is a quotient of $B/N_G B = \hat{H}^0(G, B)$, so it is generated by the class of $[b]$, which has order equal to $|H|$ by assumption. We conclude that the map $- \cup b : \hat{H}^0(H, \mathbb{Z}) \to \hat{H}^0(H, B)$ which sends $n \mapsto n[b]$ is an isomorphism.

We conclude that $\hat{H}^{-1}(H, M) = \hat{H}^0(H, M) = 0$ for all $H \subset G$. By the previous HW we conclude that $\hat{H}^q(G, M) = 0$ for all $q \in \mathbb{Z}$. Applying the long exact sequence again, we get that

$$- \cup b : \hat{H}^q(G, \mathbb{Z}) \to \hat{H}^q(G, B)$$

is an isomorphism for all q, as desired. □

21.2 Another characterization of local reciprocity, and compatibility

We explained last time how to use Tate's theorem to get an isomorphism $\mathrm{Gal}(L/K)^{ab} \to K^\times/NL^\times$. The inverse isomorphism is the local reciprocity map denoted $\theta_{L/K} : K^\times/NL^\times$ or by the *norm residue symbol* $(a, L/K) = \theta_{L/K}(a)$.

We now give another way of characterizing the local reciprocity map:

Proposition 21.2. *Let L/K be a finite extension with Galois group G. Then for any*

$$\chi \in H^1(L/K, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(G^{ab}, \mathbb{Q}/\mathbb{Z})$$

and any

$$[a] \in H^0(L/K, L^\times) = K^\times/NL^\times$$

we have

$$\chi(\theta_{L/K}([a])) = \mathrm{inv}_{L/K}([a] \cup \delta\chi).$$

where $\delta : H^1(G, \mathbb{Q}/\mathbb{Z}) \to H^2(G, \mathbb{Z})$ is the connecting homomorphism coming from the exact sequence $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$.

Furthermore, $\theta_{L/K}([a])$ is determined by the above property.

Proof. By definition of $\theta_{L/K}$, $[a] = \theta_{L/K}([a]) \cup u_{L/K}$. Plugging this in and using associativity/commutativity properties of cup product,

$$\begin{aligned}\mathrm{inv}([a] \cup \delta\chi) &= \mathrm{inv}(\theta_{L/K}([a]) \cup u_{L/K} \cup \delta\chi) \\ &= \mathrm{inv}((\delta\chi \cup \theta_{L/K}([a])) \cup u_{L/K}) \\ &= \mathrm{inv}(\delta(\chi \cup \theta_{L/K}([a])) \cup u_{L/K})\end{aligned}$$

By the HW, we have

$$\chi \cup \theta_{L/K}([a]) = [\chi(\theta_{L/K}(a))] \in \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \cong \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}.$$

Also, the connecting homomorphism δ from $\hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \cong \frac{1}{|G|}\mathbb{Z}/\mathbb{Z}$ to $\hat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}/|G|\mathbb{Z}$ is given by multiplication by $|G|$.

Hence

$$\mathrm{inv}([a] \cup \delta\chi) = \mathrm{inv}(\delta(\chi \cup \theta_{L/K}([a])) \cup u_{L/K}) = \mathrm{inv}(|G| \cdot \chi(\theta_{L/K}(a)) \cdot u_{L/K}) = \chi(\theta_{L/K}(a))$$

since $\mathrm{inv}(u_{L/K}) = 1/|G|$.

□

As a consequence of this characterization we can show

Proposition 21.3. *Let $E/L/K$ be a tower of local fields with E/K and L/K Galois. Let $\pi^{ab}_{E/L}$ be the canonical surjection $\mathrm{Gal}(E/K)^{ab} \to \mathrm{Gal}(L/K)^{ab}$ For any $a \in K^\times$ we have*

$$\pi^{ab}_{E/L}(\theta_{E/K}([a])) = \theta_{L/K}([a])$$

Proof. By the characterization we've just proved it's enough to show that

$$\chi(\pi^{ab}_{E/L}(\theta_{E/K}([a]))) = \mathrm{inv}_{L/K}([a] \cup \delta\chi).$$

for every homomorphism $\chi : \mathrm{Gal}(L/K) \to \mathbb{Q}/\mathbb{Z}$.

Let $\chi' : \mathrm{Gal}(E/K) \to \mathbb{Q}/\mathbb{Z}$ be given by $\chi' = \chi \circ \pi^{ab}_{E/L}$. Note that $\chi' = \mathrm{Inf}_{E/L}\chi \in H^1(E/K, \mathbb{Q}/\mathbb{Z})$,

Then

$$\begin{aligned}
\chi(\pi^{ab}_{E/L}(\theta_{E/K}([a]))) &= \chi'(\theta_{E/K}([a])) = \mathrm{inv}_{E/K}([a] \cup \delta\chi') \\
&= \mathrm{inv}_{E/K}([a] \cup \delta(\mathrm{Inf}_{E/L}\chi)) \\
&= \mathrm{inv}_{E/K}(\mathrm{Inf}_{E/L}([a] \cup \delta\chi)) \\
&= \mathrm{inv}_{L/K}([a] \cup \delta\chi)
\end{aligned}$$

by compatibility of inv with inflation. □

We can restate this proposition as saying that we have a commutative diagram:

$$\begin{array}{ccc}
K^\times & \xrightarrow{\theta_{E/K}} & \mathrm{Gal}(E/K)^{ab} \\
& \searrow^{\theta_{L/K}} & \downarrow{\scriptstyle \pi_{E/L}} \\
& & \mathrm{Gal}(L/K)^{ab}
\end{array}$$

Hence the maps $\theta_{L/K}$ for L/K finite Galois combine to give a map

$$\theta_{/K} : K^\times \to \varprojlim_{L/K \text{ finite Galois}} \mathrm{Gal}(L/K)^{ab} \cong \mathrm{Gal}(K^{ab}/K).$$

Because each $\theta_{L/K}$ is surjective, the map $\theta_{/K}$ has dense image. However, $\theta_{/K}$ is not surjective.

(We have a commutative diagram

$$\begin{array}{ccc} K^\times & \xrightarrow{\theta_{/K}} & \mathrm{Gal}(K^{ab}/K) \\ \downarrow{\scriptstyle v} & & \downarrow \\ \mathbb{Z} & \hookrightarrow & \hat{\mathbb{Z}} \cong \mathrm{Gal}(K^{unr}/K). \end{array}$$

Since the bottom row is not surjective, neither is the top row. But we'll see that this is the only way in which $\theta_{/K}$ fails to be surjective.)

The map $\theta_{/K}$ is injective, but showing this will take some work. Note that

$$\ker \theta_{/K} = \bigcap_{L/K \text{ finite Galois}} NL^\times$$

is the group of *universal norms* in $K^\times$. We wish to show that the only universal norm is 1, which implies injectivity of $\theta_{/K}$.

21.3 Normic Subgroups

Definition. A subgroup A of $K^\times$ is called *normic* if there exists L/K Galois such that $A = NL^\times$.

In this definition L/K need not be abelian; however if L'/K is the maximal abelian subextension of L, then $N_{L'/K}(L'^\times) = N_{L/K}(L^\times)$. To show this, note that $N_{L'/K}(L'^\times) \subset N^{L/K}(L^\times)$ and the two groups both have index in $K^\times$ equal to $|\mathrm{Gal}(L/K)|^{ab}$. (In fact this is still true even if L/K is not Galois, but it takes more work: see Serre local fields for a proof.)

We wish to show that every finite index open subgroup of $K^\times$ is normic. This is true for any local field K, but for now we'll only show for characteristic 0 (the proof uses Kummer theory): so for the rest of the section assume that K has characteristic 0.

Remark. $K^\times$ is not profinite, so there are open subgroups, such as $\mathcal{O}_K^\times$ that are *not* finite index! On the other hand, every finite index subgroup of $K^\times$ contains $(K^\times)^n$, which is open in $K^\times$, (for sufficiently large r, $(K^\times)^n \cap U_r = U_{r+v(n)}$), so finite index subgroups are open.

21.4 Existence

Proposition 21.4. *There is a bijection between finite abelian extensions* L/K *and normic subgroups* A *of* $K^\times$ *given by* $L \mapsto NL^\times$. *This bijection is order-reversing and* $[L : K] = [K^\times : A]$ *if* $L \leftrightarrow A$.

Proof. We already know that the map $L \mapsto NL^\times$ is surjective, and it is order-reversing because of compatibility of norms in towers. Also we have

$$[L : K] = |\mathrm{Gal}(L/K)| = |K^\times/NL^\times| = [K^\times : NL^\times]$$

by class field theory.

To show that $L \mapsto NL^\times$ is a bijection, we construct the inverse map. We send $A \subset K^\times$ to the fixed field $(K^{ab})^{\theta_{/K}(A)}$ of the subgroup $\theta_{/K}(A) \subset \mathrm{Gal}(K^{ab}/K)$.

Since $L \mapsto NL^\times$ is surjective, it's enough to check that $L = (K^{ab})^{\theta_{/K}(NL^\times)}$. For one inclusion, note that $\theta_{L/K}(NL^\times) = 1$ so $\theta_{/K}(NL^\times)$ fixes all elements of L and $L \subset (K^{ab})^{\theta_{/K}(NL^\times)}$.

On the other hand, we have

$$[(K^{ab})^{\theta_{/K}(NL^\times)} : K] = [\mathrm{Gal}(K^{ab}/K) : \overline{\theta_{/K}(NL^\times)}] = [\overline{\theta_{/K}K^\times} : \overline{\theta_{/K}NL^\times}] = [K^\times : NL^\times] = [L : K]$$

where the bar denotes topological closure, and the third equality uses that the kernel of $\theta_{/K}$ is contained in $NL^\times$. Hence we have equality. □

22 November 26

22.1 Normic subgroups, continued

Proposition 22.1. *If A is normic any $B \supset A$ is normic. If A and B are normic, so is $A \cap B$. More precisely: if $A = NL^\times$ and $B = NM^\times$ then $A \cap B = N(LM^\times)$.*

Proof. Suppose $A = NL^\times$, so $\mathrm{Gal}(L/K) \cong K^\times/A$. Then for any $B \supset A$ take M to be the fixed field of $\theta_{L/K}(B/A)$. Have diagram

$$\begin{array}{ccc} K^\times/NL^\times & \xrightarrow{\theta_{L/K}} & \mathrm{Gal}(L/K) \\ \downarrow & & \downarrow \\ K^\times/NM^\times & \xrightarrow{\theta_{M/K}} & \mathrm{Gal}(M/K) \end{array}$$

where the vertical maps are the natural projections and the horizontal maps are isomorphisms. Then $\theta_{L/K}(B/A) = \mathrm{Gal}(M/L)$ is the kernel of the projection $\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$, so $B/A = \ker(K^\times/NL^\times) \to (K^\times/NM^\times) = (NM^\times)/A$, hence $B/NM^\times$ is normic.

For the second part: if $A = NL^\times$ and $B = NM^\times$ are normic then $A \cap B = N(LM^\times)$. To see this, note that $N(LM^\times) \subset N(L^\times) \cap N(M^\times)$. On the other hand, if $a \in NL^\times \cap NM^\times$ then $\theta_{M/K}(a) = 1 \in \mathrm{Gal}(M/K)$ and $\theta_{L/K}(a) = 1 \in \mathrm{Gal}(L/K)$, so $\theta_{LM/K}(a) = 1$ in $\mathrm{Gal}(LM/K)$. □

(Eg normic subgroups form a neighborhood base at 1 for a topology on $K^\times$.)

Everything up to this point actually works in arbitrary characteristic. For the next bit, however we need characteristic 0.

To show that every finite index subgroup of $K^\times$ is normic, it's enough to show that

Proposition 22.2. *Assume K has characteristic 0. Then, for every n, the subgroup of nth powers $(K^\times)^n$ is normic.*

Proof. First do the case where $K \supset \mu_n$. We claim that if L is the extension of K generated by taking all nth roots, or equivalently (Kummer theory) the maximal degree n abelian extension of K, then $NL^\times = (K^\times)^n$. We have $NL^\times \supset (K^\times)^n$ since L is a compositum of degree n extensions.

Since $\mathrm{Gal}(L/K)$ is an abelian group of exponent n, $|\mathrm{Gal}(L/K)| = |\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)|$. By Kummer theory however,

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) \cong \mathrm{Hom}(\mathrm{Gal}(K^{ab}/K), \mu_n) \cong (K^\times)/(K^\times)^n$$

so

$$|K^\times/NL^\times| = |\mathrm{Gal}(L/K)| = |\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)| = |(K^\times)/(K^\times)^n|$$

and hence we must have equality $NL^\times = (K^\times)^n$.

Now, let $K' = K(\mu_n)$. We know there is a Galois extension L' of K' such that $N_{L'/K'}(L')^\times = (K'^\times)^n$. The extension L'/K need not be Galois, so enlarge to a Galois extension L/K.

Then

$$N_{L/K}L \subset N_{L'/K}L' = N_{K'/K}(N_{L'/K'}L') = N_{K'/K}(K')^n \subset K^n.$$

Hence K^n contains a normic subgroup, so is itself normic. □

(Observe that we used duality in the first part of the argument: if $K \supset \mu_n$, then Kummer theory gives us an isomorphism $K^\times/(K^\times)^n \cong H^1(L/K, \mu_n)$, but also class field theory gives us an isomorphism $K^\times/(K^\times)^n \cong \mathrm{Gal}(L/K)$. These two groups are (Pontryagin) duals of each other: one way of describing this is that we have a perfect pairing $K^\times/(K^\times)^n \times K^\times/(K^\times)^n \to \mu_n$, and this is elaborated on in the problem set.)

Comment about characteristic p: we can't just transfer this proof over, because Artin-Schreier theory as we've stated it only works for exponent p extensions, not for exponent p^r. Need something more complicated for that. Alternative approaches involve: use formal groups.

22.2 Reciprocity map and ramification

Theorem 22.3. *Let L/K be a finite unramified extension of local fields (automatically Galois and abelian). Then $\theta_{L/K}([a]) = \mathrm{Frob}_{L/K}^{v(a)}$.*

Proof. Check this using the characterization

$$\chi(\theta_{L/K}([a])) = \mathrm{inv}_{L/K}([a] \cup \delta\chi).$$

Recall how we constructed $\mathrm{inv}_{L/K}$ when K is unramified:

$$H^2(L/K, L^\times) \xrightarrow{v_*} H^2(L/K, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(L/K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{eval}_{\mathrm{Frob}}} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

So

$$[a] \cup \delta\chi \mapsto v_p(a) \cdot \delta\chi \mapsto v_p(a)\chi \mapsto \chi(\mathrm{Frob}_p^{v(a)}).$$

□

Proposition 22.4. *Suppose* L/K *is a Galois extension: then* $\theta_{L/K}$ *sends* $(\mathcal{O}^K)^\times$ *onto the inertia group* $I(L/K)$.

Proof. Let T be the inertia field so $I(L/K) = \mathrm{Gal}(L/T)$.

Then if $a \in \mathcal{O}_K^\times$, then $\theta_{T/K}(a) = 1$ so $\theta_{L/K}(a) \in \mathrm{Gal}(L/T) = I(L/K)$.

Since $\theta_{L/K}$ is onto, it's enough now to show that if $\theta_{L/K}([a]) \in I(L/K)$ then $[a] = [b]$ where $[b] \in \mathcal{O}_K^\times$.

Let $f = [T : K]$ be the inertia degree. Running previous argument backwards get $f \mid v_K(a)$. Then let $b = a \cdot N(\pi_L)^{-v_K(a)/f}$. □

22.3 Quadratic extensions

Suppose L/K is a quadratic extension of local fields. Then $\mathrm{Gal}(L/K)$ and $K^\times/NL^\times$ are both of order 2, so $\theta_{L/K}$ is the unique isomorphism $K^\times/NL^\times \to \mathrm{Gal}(L/K)$.

Example. $K = \mathbb{Q}_p$, p odd. By Kummer theory: $L = K(\sqrt{a})$ for some nontrivial $a \in K^\times/(K^\times)^2$.

The group $K^\times/(K^\times)^2 = (1, u, p, up)$ where u is a nonresidue mod p.

If $a = u$, then L/K is unramified, and $NL^\times$ is $\{x \mid v_p(x) \text{ even}\}$ (generated by $(K^\times)^2$ and u.

If $a = p$, $NL^\times$ is generated by $(K^\times)^2$ and $-p$.

If $a = up$ $NL^\times$ is generated by $(K^\times)^2$ and $-up$.

Example. A global example: ℓ is an odd prime, $\ell^* = (-1)^{(\ell-1)/2}\ell \equiv 1 \pmod 4$.

Let $K = \mathbb{Q}(\sqrt{\ell^*})$. Identify $\mathrm{Gal}(K/\mathbb{Q})$ with ± 1.

Let $a \in \mathbb{Z}$, $a > 0$, $(a, 2\ell) = 1$.

For each place v of $\mathbb{Q}$ consider the function $a \mapsto (a, K_w/\mathbb{Q}_v) = \theta_{K_w/\mathbb{Q}_v}([a])$ where w is a place of $\mathbb{Q}$ above v.

If $v = \ell$, then

$$(a, K_w/\mathbb{Q}_\ell) = \left(\frac{a}{\ell}\right).$$

If $v = p$ where $p \neq \ell$ is odd, then $(a, K_w/\mathbb{Q}_p) = 1$ if $\left(\frac{\ell^*}{p}\right) = 1$, otherwise $(a, K_w/\mathbb{Q}_p) = (-1)^{v_p(a)}$; either way

$$(a, K_w/\mathbb{Q}_p) = \left(\frac{\ell^*}{p}\right)^{v_p(a)}.$$

If $v = 2$, then

$$(a, K_w/\mathbb{Q}_2) = 1$$

always since $K_w/\mathbb{Q}_2$ is unramified ($K_w = \mathbb{Q}_2$ or $\mathbb{Q}_2(\sqrt{5})$) and a is a unit at 2.

Also if $v = \infty$ we have $\mathbb{Q}_v = \mathbb{R}$. We haven't defined the reciprocity map for archimedean extensions, but it's straightforward. If $K_w = \mathbb{R}$ then $(a, \mathbb{R}/\mathbb{R}) = 1$ of necessity, and if $K_w = \mathbb{C}$ then $(a, \mathbb{C}/\mathbb{R}) = \operatorname{sgn} a$ which in this case is 1 by assumption.

Now set $a = p$ where p is an odd prime distinct from ℓ.

Then statement $\prod_v (a, K_w/\mathbb{Q}_v) = 1$, which is a form of global reciprocity, is equivalent to

$$\left(\frac{\ell^*}{p}\right) = \left(\frac{p}{\ell}\right),$$

which is a form of quadratic reciprocity.

22.4 The big picture for $\mathbb{Q}_p$

For any local field K and any uniformizer $\pi \in K$, have $\mathrm{Gal}(K^{ab}/K) \cong \mathcal{O}_K^\times \times \pi^{\hat{\mathbb{Z}}}$.

We recognize the fixed field of $\mathcal{O}_K^\times$, as K^{unr}, and define K^π to be the fixed field of $\pi^{\hat{\mathbb{Z}}}$. Note that K^π depends on the choice of π, so it's not canonical. Then $K^{unr} \cap K^\pi = K$, and $K^{ab} = K^{unr}K^\pi$. The Artin map gives isomorphisms of Galois groups $\hat{\mathbb{Z}} \cong \mathrm{Gal}(K^{unr}/K)$ and $\mathcal{O}_K^\times \cong \mathrm{Gal}(K^\pi/K)$.

Now, in the case of $K = \mathbb{Q}_p$ and $\pi = p$ can identify these fields: we have $\mathbb{Q}_p^{unr} = \mathbb{Q}_p(\zeta_n)_{(n,p)=1}$ and $\mathbb{Q}_p^\pi = \mathbb{Q}_p(\zeta_{p^\infty})$.

23 November 30

23.1 Big picture for $\mathbb{Q}_p$, continued

Can make explicit the Artin maps here. If $a = p^r u$, $u \in \mathbb{Z}_p^\times$, we've already seen

$$\theta_{/\mathbb{Q}_p}(a)(\zeta_n) = (\zeta_n)^{p^r}$$

for $(n, p) = 1$.

What's also true is that

$$\theta_{/\mathbb{Q}_p}(a)(\zeta_{p^m}) = (\zeta_{p^m})^{u^{-1}}$$

for all m.

Two main proofs of this:

Deduce from global reciprocity law ($\mathbb{Q}^\times$ is in kernel of global reciprocity map $\theta_{\mathbb{Q}(\zeta_{p^m}/\mathbb{Q}}$: $\mathbb{A}_\mathbb{Q} \to \mathrm{Gal}(\mathbb{Q}(\zeta_{p^m}/\mathbb{Q}))$, already know what the local reciprocity map is at all places other than p.)

Proof using local methods: most easily done with machinery of Lubin-Tate formal group laws, which we'll now develop.

Additionally, the Lubin-Tate theory will also give us K^π and the local reciprocity map for all local fields K.

23.2 Motivating Lubin-Tate

Cyclotomic fields: the theory of cyclotomic fields is great, we want to generalize it p-adically. One disappointing thing here is that we can't define ζ_n analytically as $e^{2\pi i/n}$ because we don't have a $2\pi i$ in $\mathbb{Z}_p$.

So instead we'll describe the fields algebraically: the polynomials $X^n - 1$ have the property that for any ring R the set $\mu_n(R)$ of roots of X^n in R forms a cyclic group under multiplication (in other words, $\mu_n = \mathrm{Spec}(\mathbb{Z}[X]/(X^n - 1))$ is a group scheme!).

Actually, we'll change variables a little bit, in a way that we've done before. Let $f_n(X) = (X+1)^n - 1$. Then the set of roots of f_n can still be viewed as group, with multiplication law is $a * b = ab + a + b$, and the identity element is now 0.

We can actually make sense of f_a for $a \in \mathbb{Q}_p$ arbitrary, as a power series

$$f_a(X) = \sum_{k \geq 1} \binom{a}{k} X^k$$

. Since all coefficients are p-integral, this gives a function $f_a : p\mathbb{Z}_p \to p\mathbb{Z}_p$: more generally it's a function $f_a : \mathfrak{p}\mathbb{Z}_p^{\mathrm{sep}} \to \mathfrak{p}\mathbb{Z}_p^{\mathrm{sep}}$. It's a homomorphism with respect to $*$: we have the identity $f_a(X * Y) = f_a(X) * f_a(Y)$ of formal power series. Observe that $f_{ab} = f_a \circ f_b$ and that if u is a unit then $f_u : p\mathbb{Z}_p \to p\mathbb{Z}_p$ is an invertible function with inverse $f_{u^{-1}}$.

Now consider the set $\{x \in \mathbb{Q}_p^{\mathrm{sep}} \mid |x| < 1, f_a(x) = 0\}$. This is a group with respect to $*$, and it only depends on $e = v_p(a)$. If $a = up^e$, this is exactly $\{\zeta - 1 \mid \zeta \in \mu_{p^e}\}$.

We will want to mimic this setup for a local field K. We want to make functions $f_a(X)$ for every $a \in \mathcal{O}_K$, and define a multiplication law $*$. For every $a \in \mathcal{O}_K$, the set of roots $E_{f,a}$ of x of f_a in K^{sep} with $|x| < 1$ will be not only a group, but a $\mathcal{O}_K$-module, using the action $[b]x = f_b(x)$, and as an $\mathcal{O}_K$-module it will be isomorphic to $\mathcal{O}_K/a\mathcal{O}_K$.

23.3 Formal groups

Definition. A one-parameter commutative formal group law (or just "formal group") over a ring A is a power series $F(X,Y) \in A[[X,Y]]$ such that

- $F(X,Y) = X + Y \pmod{\deg 2}$ (that is, modulo all monomials of degree ≥ 2)
- $F(X,Y) = F(Y,X)$
- $F(F(X,Y),Z) = F(X,F(Y,Z))$
- exists $i_F(X) \in A[[X]]$ with $F(X, i_F(X)) = 0$ (exercise: this axiom is redundant!)
- $F(0,Y) = Y$ and $F(X,0) = X$.

Note that if A is contained in a local field $\mathcal{O}_K$, then for any finite extension L/K, the formal group law F makes $\pi_L\mathcal{O}_L$ into a group with group operation $a * b = F(a,b)$.

Example. The additive formal group $F(X,Y) = X + Y$.

Example. The multiplicative formal group $F(X,Y) = X + Y + XY$.

Example. Formal group of an elliptic curve: if E is an elliptic curve with homogeneous Weierstrass equation $Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$ over a local field K (assume char K not 2 or 3), then a neighborhood of the origin $[0:1:0]$ in $E(K)$ can be parametrized in terms of $z = Z/Y$ (that is, points look like $[w(z), 1, z]$ where $w(Z)$ is a power series).

Then the addition law can be given by $z(P_1 + P_2) = F(z(P_1), z(P_2))$, and this power series F is a formal group over K. If $a_4, a_6 \in \mathcal{O}_K$ then F is a formal group over $\mathcal{O}_K$.

A homomorphism $h : F \to G$ of formal groups is a power series $h \in A[[X]]$ with zero constant term such that $G(h(X), h(Y)) = h(F(X,Y))$. We say that h is an isomorphism if h has an inverse (under composition of power series), and h is an endomorphism if $F = G$.

The set $\mathrm{Hom}(F,G)$ of formal group homomorphisms from F to G is an abelian group under the addition law $h_1 +_G h_2 = G(h_1, h_2)$. Additionally, if $F = G$ the group $\mathrm{End}(F) = \mathrm{Hom}(F,F)$ is a (possibly noncommutative) ring with multiplication given by composition.

If $h : F \to G$ is an homomorphism of formal groups over $\mathcal{O}_K$, then the function defined by h, that is, $a \mapsto h(a) : F(\pi_L\mathcal{O}_L) \to G(\pi_L\mathcal{O}_L)$ is also a homomorphism.

Also, last time we just defined $F(\pi_L\mathcal{O}_L)$ for L a finite extension of K, but we can do the analogous construction for infinite extensions. E.g. let K^{sep} be the separable closure of K, with ring of integers $\mathcal{O}_{K^{sep}}$ and maximal ideal $\mathfrak{p}_{K^{sep}}$ Then define $F(\mathfrak{p}_{K^{sep}})$ to be $\mathfrak{p}_{K^{sep}}$ with group law given by $a +_F b = F(a,b)$.

As with the finite case, the function $a \mapsto h(a)$ also gives a homomorphism $F(\mathfrak{p}_{K^{sep}}) \to G(\mathfrak{p}_{K^{sep}})$.

Example. Let $A = \mathbb{Q}_p$, $F(X,Y) == X + Y$, $G(X,Y) = X + Y + XY$.

Then $f(X) = \exp_p(X) - 1$ is an isomorphism $F \to G$, with inverse $f^{-1}(X) = \log_p(1+X)$.

However, as formal groups over $\mathbb{Z}_p$, F and G are not isomorphic. This is because $F(\pi_L\mathcal{O}_L) = \pi_L\mathcal{O}_L^+$ is always a torsion-free group for any finite extension L of $\mathbb{Z}_p$, while $G(\pi_L\mathcal{O}_L) \cong (1 + \pi_L\mathcal{O}_L)^\times$ may contain p-torsion. (E.g. if $L = \mathbb{Q}_p(\zeta_p)$, the element $\zeta_p - 1 \in G(\pi_L\mathcal{O}_L)$ is p-torsion.)

Example. Let $A = \mathbb{Z}_p$, $F(X,Y) = X + Y + XY$, then the functions

$$f_a(X) = (X+1)^a - 1 = \sum_{k \geq 1} \binom{a}{k} X^k.$$

for $a \in \mathbb{Z}_p$ previously defined are endomorphisms of F.

Let F and G be formal groups over $\mathcal{O}_K$, and let $h \in \mathrm{Hom}(F, G)$. Then we can try to make sense of the kernel of h. First we can look at the kernel of the group homomorphism $F(\mathfrak{p}_{K^{sep}}) \to G(\mathfrak{p}_{K^{sep}})$. This is

$$\{a \in \mathfrak{p}_{K^{sep}} \mid h(a) = 0\},$$

that is, the set of solutions of $h(a) = 0$ in $\mathfrak{p}_{K_{sep}}$. Note that this kernel is acted on by $\mathrm{Gal}(K^{sep}/K)$.

23.4 Lubin-Tate series

Let K be a local field with uniformizer π, and such that $|\mathcal{O}_K/\pi\mathcal{O}_K| = q$. We will choose a formal group F, so that the kernels of endomorphisms of F become modules for $\mathrm{Gal}(K^{sep}/K)$, and use this to construct abelian extensions. We don't want to take an arbitrary formal group F because we might not get abelian extensions. So we'll specialize to a special type of formal group.

Definition. The set $\mathcal{F}_\pi$ of *Lubin-Tate series* is the set of all $f(x) \in \mathcal{O}_K[[X]]$ such that $f(x) \equiv \pi X \bmod \deg 2$ and $f(x) \equiv X^q \mod \pi$

Example. $K = \mathbb{Q}_p$, $\pi = p$, $f(X) = (X+1)^p - 1$.

Example. K and π arbitrary, $f(X) = X^p + \pi X$.

24 December 3

24.1 Lubin-Tate formal groups

Today we construct Lubin-Tate formal groups and use them to construct the maximal abelian extension of a local field K. We'll be skipping a lot of details for time, see Milne for more details.

Theorem 24.1. *For any $f \in \mathcal{F}_\pi$ there's a unique formal group F_f for which f is an endomorphism. For any $a \in \mathcal{O}_K$ there's a unique $[a]_f$ such that $[a]_f$ commutes with f and $[a]_f \equiv aX \pmod{\deg 2}$. Then $[a]_f$ is also an endomorphism of F_f. The map $a \to [a]_f : \mathcal{O}_K \to \mathrm{End}(F_f)$ is an injective homomorphism of rings. For the case $a = \pi$ we have $[\pi]_f = f$.*

Any two Lubin-Tate group laws for the same π are isomorphic over $\mathcal{O}_K$.

Remark. In class I said that $a \to [a]_f : \mathcal{O}_K \to \mathrm{End}(F_f)$ was an isomorphism. I'm not sure if this is true, but we won't need it here. It is however true that any endomorphism of F_f as a formal $\mathcal{O}_K$-module is of the form $[a]_f$ for some a (because any such must commute with $[\pi]_f = f$.)

The proof is essentially repeated application of the following "workhorse lemma".

Lemma 24.2. *For $f, g \in \mathcal{F}_\pi$, and any linear polynomial $\Phi_1 \in \mathcal{O}_K[X_1, \dots, X_r]$ (with zero constant term), the equation*

$$f(\Phi(X_1, \dots, X_r)) = \Phi(g(X_1), g(X_2), \dots, g(X_r)))$$

has a unique solution $\Phi \in \mathcal{O}_K[[X_1, \dots, X_r]]$ such that $\Phi \equiv \Phi_1 \pmod{\deg 2}$.

The proof of the workhorse lemma is pretty straightforward: you can solve for the coefficients inductively, and we'll skip it.

Sketch of Proof of Theorem 24.1. We first show that there's a unique formal group F_f for which f is an endomorphism. First we apply the workhorse lemma directly to get that there is a unique power series F_f such that

$$f(F_f(X, Y)) = F_f(f(X), f(Y))$$

with $F_f \equiv X + Y \pmod{\deg 2}$.

We need to show that F_f satisfies the formal group axioms: this will follow by applying uniqueness repeatedly. For instance, commutativity follows since also

$$f(F_f(Y, X)) = F_f(f(Y), f(X))$$

associativity follows from applying uniqueness to the two power series $F_f(F_f(X, Y), Z)$ and $F_f(X, F_f(Y, Z))$. Likewise 0 is a left identity because the power series $F_f(X, 0)$ and X both commute with f, and a right identity for the same reason.

Existence of an inverse follows from the other axioms (as previously mentioned), but we can also define i_{F_f} directly as the unique power series $i_{F_f} \in \mathcal{O}_K[X]$ which commutes with f and has constant term equal to $-X$. (This is also what we are calling $[-1]_f$.) Again this satisfies the required property by uniqueness.

For $f, g \in \mathcal{F}_\pi$ define $[a]_{g,f} \in \mathcal{O}_K[[X]]$ to be the unique power series congruent to aX mod $\deg 2$ that satisfies

$$[a]_{g,f} \circ f = g \circ [a]_{g,f},$$

and define $[a]_f = [a]_{f,f}$.

We have

$$F_f([a]_{g,f}(X), [a]_{g,f}(Y)) = [a]_{g,f}(F_g(X, Y))$$

by uniqueness in workhorse lemma, so $a_{g,f}$ is a homomorphism $F_f \to F_g$.

Also,

$$[a]_{g,f} +_G [b]_{g,f} = [a+b]_{g,f}$$

and

$$[a]_{h,g}[b]_{g,f} = [ab]_{h,f}$$

also follow by uniqueness.

If we specalize to $f = g$, we see that $[a]_f$ is an endomorphism of F_f, and the map $a \to [a]_f$ is a ring homomorphism by uniqueness. Also, the uniqueness property means that any element of $\mathrm{End}(F_f)$ is equal to $[a]_f$ for some $a \in \mathcal{O}_K$, so $a \mapsto [a]_f$ is an isomorphism.

Also, if a is a unit, then $[a]_{g,f}$ is an isomorphism of formal groups $F_f \to F_g$ with inverse $[a^{-1}]_{f,g}$.

Finally $[\pi]_f = f$ by uniqueness again. □

Definition. A formal $\mathcal{O}_K$-module F is a formal group F along with a homomorphism $\mathcal{O}_K \to \mathrm{End}(F)$, which we write as $a \mapsto [a]_F$, such that $[a]_F(X) = aX \pmod{\deg 2}$.

The above discussion shows that F_f is a formal $\mathcal{O}_K$-module with $[a]_{F_f} = [a]_f$.

We also have a notion of endomorphism of formal $\mathcal{O}_K$-modules. The homomorphism $[a]_{g,f}$ of formal groups defined above is also a homomorphism of formal $\mathcal{O}_K$-modules.

Note that if F is a formal $\mathcal{O}_K$-module, then $F(\mathfrak{p}_{K^{sep}})$ is an $\mathcal{O}_K$-module. We will now look at the torsion submodules of this $\mathcal{O}_K$-module, in the case where $F = F_f$ comes from a Lubin-Tate series.

24.2 The field $K^{\pi,n}$ generated by π^n-torsion of F_f

Let E_{f,π^n} be the set $\{x \in \mathfrak{p}_{K^{sep}} \mid [\pi^n]_f(x) = 0\}$ all π^n torsion of F_f. Then E_{f,π^n} is an $\mathcal{O}_K$-module via the action $a * x = [a]_f x$, and is annihilated by $\pi^n\mathcal{O}_K$. Let $K^{\pi,n}$ be the field generated by E_{f,π^n}.

Proposition 24.3. *The power series $[1]_{g,f}$ gives an isomorphism $E_{f,\pi^n} \to E_{g,\pi^n}$. The field $K^{\pi,n}$ is not dependent on the choice of Lubin-Tate formal group (but does depend on π).*

Proof. For the first part: $[\pi^n]_f(x) = 0$ iff

$$[1]_{g,f}[\pi^n]_f(x) = [\pi^n]_g 1_{g,f}(x) = 0$$

so we have a map $E_{f,\pi^n} \to E_{g,\pi^n}$. This is a morphism of $\mathcal{O}_K$-modules with inverse map $[1]_{f,g}$.

The second part follows from the first, because for any $x \in E_{f,\pi^n}$, the field $K(x)$ is complete so contains $[1]_{g,f}(x)$. □

Theorem 24.4. *E_{f,π^n} is isomorphic as $\mathcal{O}_K$-module to $\mathcal{O}_K/(\pi^n)\mathcal{O}_K$. This isomorphism is not canonical.*

Proof. By the above, WLOG $f = [\pi]_f$ is a monic polynomial of degree q. Then $[\pi^n]_f = f \circ \cdots \circ f$ is a monic polynomial of degree q^n, and is separable (it has nonzero linear term). Hence it has q^n roots in K^{sep} for all n.

Conclude that $|E_{f,\pi^n}| = q^n$ for all n. Because $\mathcal{O}_K$ is a DVR, any $\mathcal{O}_K$-module is isomorphic to $\bigoplus_{i=1}^{m} \mathcal{O}_K/(\pi^{d_i})$. Now observe that the π-torsion submodule of E_{f,π^n} is equal to $E_{f,\pi}$, which has order q. It follows that $m = 1$ and $d_1 = n$.

□

Although this isomorphism is not canonical, the isomorphism $\mathrm{Aut}_{\mathcal{O}_K}(E_{f,\pi^n}) \to (\mathcal{O}_K/(\pi^n\mathcal{O}_K))^\times$ is canonical, and the inverse map is given by $a \mapsto [a]_f$.

Corollary 24.5. *Let* $E_f = E_{f,\pi^\infty} = \bigcup E_{f,\pi^n}$ *Then* $E_f \cong K/\mathcal{O}_K$ *as* $\mathcal{O}_K$*-modules, but this isomorphism is not canonical.*

Proof. Choose $\alpha_n \in E_{f,\pi^n}$ inductively for each $n \geq 1$ so that α_1 generates $E_{f,\pi}$ and $[\pi]_f\alpha_n = \alpha_{n+1}$. The annihilator in $\mathcal{O}_K$ of α_n is π^n, so α_n generates E_{f,π^n}.

Now, define an isomorphism $E_f \to K/\mathcal{O}_K$ by sending α_n to π^{-n}. □

Again, we have a canonical isomorphism

$$\mathrm{Aut}(E_f) \cong \varprojlim_n \mathrm{Aut}(E_{f,n}) \cong \varprojlim_n (\mathcal{O}_K/(\pi^n\mathcal{O}_K))^\times \cong \mathcal{O}_K^\times.$$

Now, note that $\mathrm{Gal}(K^{\pi,n}/K)$ acts on $E_{f,n}$ (since the latter is the set of roots of the polynomial $[\pi^n]_f$), and this action is compatible with the $\mathcal{O}_K$-module structure on $E_{f,n}$.

Proposition 24.6. *The map* $\mathrm{Gal}(K^{\pi,n}/K) \to \mathrm{Aut}_{\mathcal{O}_K}(E_{f,n})$ *is an isomorphism. In particular this implies that* $\mathrm{Gal}(K^{\pi,n}/K)$ *is abelian.*

Proof. First of all this map is injective because $K^{\pi,n}$ is generated by $E_{f,n}$.

We now show that both groups have the same order. On the one hand, $K^{\pi,n} = K(\alpha_n)$ where α_n is a generator of $E_{f,n}$, so is a root of $\frac{[\pi]_f^n}{[\pi]_f^{n-1}}$.

Now we observe that for all $n \geq 1$, $\frac{[\pi]_f^n}{[\pi]_f^{n-1}}$ is an Eisenstein polynomial of degree $q^k - q^{k-1}$, with constant term π. Hence

$$|\mathrm{Gal}(K^{\pi,n}/K)| = [K(\alpha) : K] = q^n - q^{n-1}$$

On the other hand, we already have $|\mathrm{End}_{\mathcal{O}_K}(E_{f,n})| = |\mathcal{O}_K/(\pi^n)|^\times = q^n - q^{n-1}$.

□

We now take then union $K^\pi = \bigcup_n K^{\pi,n} = K(E_f)$.

Corollary 24.7. *The map* $\mathrm{Gal}(K^\pi/K) \to \mathrm{End}_{\mathcal{O}_K}(E_f) \to \mathcal{O}_K^\times$ *is an isomorphism.*

We've now constructed a field extension K^π/K, depending only on π, such that $\mathrm{Gal}(K^\pi/K) \cong \mathcal{O}_K^\times$. We previously saw how to construct such a K^π using class field theory. We'll ultimate prove that these two constructions give the same field. The first step towards this is:

Proposition 24.8. $\pi \in N_{K^{\pi,n}/K}(K^{\pi,n})^\times$.

Proof. Because $K^{\pi,n} = K(\alpha_n)$ and α_n is the root of an Eisenstein polynomial with constant term π, we have $N(-\alpha_n) = \pi$. □

In fact, it will be true that any finite abelian extension L/K such that $\pi \in NL^\times$ is a contained in K^π (as this agrees with the definition of K^π we gave previously) but we don't yet have the ability to prove this.

24.3 Building maximal abelian extension and Artin map with Lubin-Tate theory

Can now construct a candidate L^π for K^{ab} and a candidate Artin map $K^\times \to \mathrm{Gal}(L/K)$ as follows:

$L^\pi = K^{unr}K^\pi$, $r_\pi : K^\times \to \mathrm{Gal}(L/K)$ is given by:

- For $u \in \mathcal{O}_K^\times$, $r_\pi(u)|_{K^{unr}} = \mathrm{id}$ and $r_\pi(u)|_{K^\pi}$ is determined by

$$r_\pi(u)(x) = [u^{-1}]_f(x)$$

  for every $x \in E_f$.

- $r_\pi(\pi)|_{K^{unr}} = \mathrm{Frob}$ and $r_\pi(\pi)|K^\pi = \mathrm{id}$.

Theorem 24.9. *$L^\pi = K^{ab}$ and $r_\pi = \theta_{/K}$ is the Artin map.*

Sketch. First step is to show that $L = L^\pi$ and $r = r_\pi$ don't depend on our choice of π. Proof of this is a big computation, and we'll skip it.

Observe that $K^\times$ is generated by uniformizers ($u\pi^n = \pi^{n-1} \cdot (u\pi)$). Hence it's enough to check that $r(\pi) = \theta_{L/K}(\pi)$ for every uniformizer π of K.

Our first hypothesis gives

$$r(\pi)|_{K^{unr}} = \mathrm{Frob} = \theta_{L/K}(\pi)|_{K^{unr}}$$

But $\pi \in (NK^{\pi,n})^\times$ for any n, so

$$r(\pi)|_{K^\pi} = \mathrm{id}\,|_{K^\pi} = \theta_{L/K}(\pi)|_{K^\pi},$$

since $L = K^\pi K^{unr}$.

Hence $r = \theta_{L/K}$. Because r is injective must have $L = K^{ab}$. □