Math 223a : Algebraic Number Theory notes

Alison Miller

1 August 31: 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 Galois extension, 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 $p\mathcal{O}_L = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$.

We now invoke some facts from a first course in number fields (see Neukirch ANT I.8-9 for proofs.) The group $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the set $\{\mathfrak{p}_1, \dots \mathfrak{p}_r\}$, and that all exponents $e_1 = \cdots = e_n = e$ are the same. If $e = 1$ we say p is *unramified* in L; this is the case for all but finitely many p. We assume now that p is unramified. In this case we'll say that the "splitting data" of p is the number r of primes that p splits into. (This is a somewhat crude definition, but we'll refine it later.)

A useful theorem for determining splitting data, is the following :

Proposition 1.1. *Assume that $\mathcal{O}_L = \mathbb{Z}[\alpha]$. If α has minimal polynomial $f(x) \in \mathbb{Z}[x]$, the prime factors $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ of $p\mathcal{O}_L$ are in bijection with the factors of the mod p reduction $\bar{f}(x) \in \mathbb{F}_p[x]$ of the polynomial f. (This bijection can be made explicit.)*

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. (Alternatively, in class, we did this by checking when $p\mathcal{O}_L$ is prime, by checking whether $\mathcal{O}_L/(p)$ is an integral domain.) 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 on $\mathbb{Q}$ is a *class field* if for any (unramified) prime p, the splitting data of $p\mathcal{O}_L$ depends only on the congruence class of p mod some modulus N.

Example. The field $L = \mathbb{Q}[\sqrt{n}]$ is a class field because a calculation with quadratic reciprocity 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. One can prove this directly from Proposition 1.1, but we'll see an easier way below.

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

- L *is a class field.*
- $L/\mathbb{Q}$ *is abelian*
- $L \subset \mathbb{Q}[\zeta_n]$ *for some* n*.*

Example. when $q \equiv 1 \pmod 4$, $\mathbb{Q}[\sqrt{q}]$ is contained in $\mathbb{Q}[\zeta_q]$, $q \equiv 1 \pmod 4$.

Today we're going to take these two assertions as givens, 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.

1.2 Frobenius elements; working towards the Artin map

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 $p\mathcal{O}_L$.

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

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

Note that the orbit stabilizer-formula on the prime factors of $p\mathcal{O}_L$ lets you compute the splitting data from $D_\mathfrak{p}$, as $r = [L : \mathbb{Q}]/|D_\mathfrak{p}|$.

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. Because $\mathrm{Gal}(\ell/\mathbb{F}_p)$ is generated by the Frobenius automorphism $x \mapsto x^p$, we have the following consequence

Proposition 1.3. *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 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 p 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 $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/\mathbb{Q})$ correspondes 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.

1.3 $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ and projective limits

Now we will give a way of packaging together all finite abelian extensions of $\mathbb{Q}$. Define $\mathbb{Q}^{\mathrm{ab}}$ to be the maximal abelian extension of $\mathbb{Q}$ (check that this definition makes sense; that is, the compositum of two abelian extensions is abelian). By Kronecker-Weber we know that $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}(\zeta_\infty) = \bigcup_n \mathbb{Q}(\zeta_n)$.

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

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

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

. 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 $i \leq k, j \leq k$.

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,

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

(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 $\hat{\mathbb{Z}} = \lim_{\leftarrow}(\mathbb{Z}/n\mathbb{Z})$.

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:

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

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

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

and

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

Then (exercise!)

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

(I stated this incorrectly in class as $\mathbb{A}_{\mathbb{Q},\mathrm{fin}}/\mathbb{Q}^{\times} \cong \prod_p \mathbb{Z}_p^{\times}$, which is not quite right.)

The map

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

is known as the Artin map and is at the heart of global class field theory.

2 September 5

2.1 Adeles over a general number field

Last time we defined the Artin map

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

for the base field $\mathbb{Q}$. We now give the generalization for number fields.

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 the completions at the end of this lecture), 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

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

2.2 The Artin Map and class field theory over a general number field

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

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

This map must contain $(\mathbb{A}_K^\times)_0$ in its kernel for purely topological reasons; $\mathrm{Gal}(K^{ab}/K)$ is totally disconnected. What is substantially harder to show is *Artin reciprocity*: that $K^\times \subset \ker\theta_K$. This means that the Artin map factors through the *adelic class group* $C_K = \mathbb{A}_K/K^\times$. More specifically, it gives isomorphisms

$$C_K/(C_K)_0 \cong \mathbb{A}_K^\times/K^\times(\mathbb{A}_K)_0 \cong \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}).$$

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 surjectivity 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.

2.3 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 matter 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.

2.4 Local-global compatibility:

Now back to K is a global field. 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 go in other direction 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

$$\begin{tikzcd}
K_{\mathfrak{p}}^{\times} \arrow[r, "\theta_{K_{\mathfrak{p}}}"] \arrow[d] & \mathrm{Gal}(K_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}}) \arrow[d] \\
\mathbb{A}_K^{\times} \arrow[r, "\theta_K"] & \mathrm{Gal}(K^{ab}/K)
\end{tikzcd}$$

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 consturct the global Artin map.

2.5 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.

2.6 Valuations

Motivation for defining local fields is to generalize $\mathbb{Q}_p$, $\mathbb{F}_p((t))$. In the end it turns out that the only local fields are finite extensions of those two, but we'll have a nice theory that treats them all in a uniform manner.

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

a) $v(0) = \infty$

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

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

Example. For $K = \mathbb{Q}$, we define the p-adic valuation $v_p(x)$ 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 $v_\mathfrak{p}(x)$ to be the exponent of $\mathfrak{p}$ in the prime factorization of the 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 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 em 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 $|\cdot|_1 = |\cdot|_2$.

Note that if v is a valuation and $c < 1$ is a positive constant, then $|x|_v = c^{v(x)}$ is a valuation whose equivalence class does not depend on v.

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 $\mathbb{C}$.

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*. As you can guess from this terminology, these two categories cover all places of global fields.

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

Theorem 2.1 (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 $\mathbb{Q} \hookrightarrow \mathbb{R}$.*

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.

Next time we'll show that these theorems imply their analogues for finite extensions of $\mathbb{Q}$ and $\mathbb{F}_p(t)$.

One more bit of algebraic definition, which we recall from commutative algebra.

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

Exercise: if ν is a valuation on a field K then $\mathcal{O}_\nu = \{x \in K \mid \nu(x) \geq 0\}$ is a DVR (justifying the name) with principal ideal $\mathfrak{p}_\nu = \{x \in K \mid \nu(x) \geq 1\}$ generated by any π with $\nu(\pi) = 1$. 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.

As a final comment: the terminology of places allows us to define the adeles in a way that puts the finite and infinite factors on a more equal footing.

Indeed,

$$\mathbb{A}_K^\times = \{\{a_\nu\} \in \prod_\nu K_\nu^\times \mid |a_\nu|_\nu = 1 \text{ for almost all } \nu\}.$$

3 September 7

3.1 Properties of complete fields and completions

First we dispose of the theory of fields complete with respect to an archimedean valuation.

Theorem 3.1 (Ostrowski)**.** *The only fields that are complete with respect to an archimedean absolute value are $\mathbb{C}$ and $\mathbb{R}$.*

Now let K be a complete field with respect to discrete absolute value. Since K is not $\mathbb{R}$ or $\mathbb{C}$, this absolute value must be be non-archimedean and come from exponentiating a valuation: $|x| = c^{-\nu(a)}$ $(c > 1)$.

The subring

$$\mathcal{O} = \{a \in K \mid |a| \leq 1\}$$

is closed (and also open!) inside K, as is the prime ideal $\mathfrak{p} = (\pi) = \{a \in K \mid |a| \leq c^{-1}\}$. The subring $\mathcal{O}_K$ is a complete DVR.

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

if $\mathcal{O}$ is a ring with prime $\mathfrak{p}$ and completion $\hat{K}$, then : the closure of $\mathcal{O}$ in $\hat{K}$ is the valuation ring (elements of valuation ≥ 0). $\hat{\mathfrak{p}}$ is the maximal ideal. $\mathcal{O}/\mathfrak{p}^i \cong \hat{\mathcal{O}}/\hat{\mathfrak{p}}^i$ for all $i \geq 0$.

Lemma 3.2 (Hensel). *Let $\mathcal{O}$ be a complete DVR with prime $\mathfrak{p} = (\pi)$ and $k = \mathcal{O}/\mathfrak{p}$. 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 $\mathfrak{p}$ 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 $g_n, h_n \in \mathcal{O}/\pi^n$ with $\deg g_n = d_g = \deg g$, $\deg h_n = d_h = \deg f - \deg h$

We do this by induction: the base case $n = 1$ is already given to us, take $g_1 = \overline{g}$ and $h_1 = \overline{h}$.

Now suppose we have $g_n, h_n \in (\mathcal{O}/\pi^n)[x]$ with $g_n h_n = f \mod \mathfrak{p}^n$. Take arbitrary lifts $g'_{n+1}, h'_{n+1} \in (\mathcal{O}/\pi^{n+1})[x]$.

Now write $g_{n+1} = g'_{n+1} + \pi^n a$, $h_{n+1} = h'_{n+1} + \pi^n b$ for $a, b \in k[x]$to be determined. We need

$$\pi^n a h_n + \pi^n b g_n = f - g'_{n+1} h'_{n+1} \mod \pi^{n+1}.$$

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

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

for $c = \frac{1}{\pi^n}\left(f - g'_{n+1} h'_{n+1}\right)$. Let P_n denote the k-vector space of polynomials of deg $\leq n$ in $k[x]$. Then 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 court.

Hence (1) has a solution as desired. □

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

Corollary 3.3. *If, for $f \in \mathcal{O}[x]$, there exists $\overline{a} \in \overline{k}$ such that $\overline{f}(\overline{(a)}) = 0$ but $f'(\overline{(a)}) \neq 0$, then $\overline{a}$ lifts to a unique root $a \in \mathcal{O}$ of f.*

Example. $x^p - 1$ splits into distinct linear factors in $\mathbb{F}_p[x]$, so also in $\mathbb{Z}_p[x]$; therefore $\mathbb{Z}_p$ contains all the pth 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.

Corollary 3.4. *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 $\min_{0\leq i\leq n} v(a_i) = 0$ Assume by way of contradiction, let m be maximal with $v(a_m) = 0$. Then $f \in \mathcal{O}[x]$ and $\overline{f} \in k[x]$ has degree m with $0 < m < n$. Apply Hensel's lemma $\overline{g} = \overline{f}$, $\overline{h} = 1$ to get that f has a factor of degree m. □

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

3.2 Extensions of fields

Proposition 3.5. *Let K be a field complete with respect to a discrete absolute value $|\cdot|_K$, L/K a finite extension of deg 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 $|\cdot|_L$.*

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 $N_{L/K}a = c_0^{n/m}$. This is the definition we'll use here.

Proof. Only hard part is to check that $|a|_L + |b|_l \leq \max(|a|_L, |b|_L)$. 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 $|b|_L = \sqrt[n]{|N_{L/K}b|_K}$ 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 abs.vals. on a field L that give the same topology are equivalent. (to do this, note that $|a| < 1$ iff $\{a^k\} \to 0$; exercise to complete the argument).

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

4 September 12

4.1 More on extensions of valuations and ramification

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

$$[(\operatorname{im}|\cdot| : K \to \mathbb{R}^>0) : (\operatorname{im}|\cdot| : L \to \mathbb{R}^{>0})],$$

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

Example. $K = \mathbb{Q}_p$, $L = \mathbb{Q}_p[\sqrt{p}]$. 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 $e = 2$ $f = 1$.

Theorem 4.1. *In the setting above,* $ef = n = [L : K]$

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

First of all, $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module of rank n, so $\mathcal{O}_L/\pi_K\mathcal{O}_L$ is a free k-module of rank n.

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

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

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

Question 1. *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?*

One approach: if $K = \operatorname{Frac}\mathcal{O}_K$, $\mathcal{O}_K$ 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 $\nu_{\mathfrak{p}'}(a) = e\nu_\mathfrak{p}(a)$. Hence, after suitable renormalization, the valuation $|\cdot|_{\mathfrak{p}'}$ extends $|\cdot|_\mathfrak{p}$.

Theorem 4.2. *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* $\mathfrak{p}$*.*

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 competion $\hat{K}$ 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 $\mathcal{O}_{L,\nu'} = \{a \in \mathcal{O}_L \mid \|a\|' \leq 1\}$; this is an integrally closed ring that contains $\mathcal{O}_K$, so contains $\mathcal{O}_L$. Let $\mathfrak{p}' = \mathfrak{p}_{L,\nu'} \cap \mathcal{O}_L$; this is a nonzero prime ideal of $\mathcal{O}_L$.

Then the localization $(\mathcal{O}_L)_{\mathfrak{p}'}$ is contained in $\mathcal{O}_{L,\nu'}$: since both are DVRs they must be equal.

□

Corollary 4.3. *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 $|\cdot|_\nu$be an absolute value on K, and let $|\cdot|'_\nu$ be an absolute value on L extending $|\cdot|_\nu$. (You should think of ν and ν' as (possibly archimedean) places of K and L respectively; this argument works just fine if $|\cdot|_\nu$, $|\cdot|_{\nu'}$ are archimedean absolue values).

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

Conversely, if L' is a field with inclusions

$$\begin{tikzcd} K \arrow[r, hook] \arrow[d, hook] & L \arrow[d, hook] \\ K_\nu \arrow[r, hook] & L'. \end{tikzcd} \tag{2}$$

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

By this means we get a bijection

$$\{\text{absolute values on } L \text{ extending } |\cdot|_\nu\} \leftrightarrow \{\text{equvalence classes of compositum fields } L' = LK_\nu\}$$

where on the right hand side, the equivalence class is up to isomorphism that commute with the maps in the diagram (2).

Proposition 4.4. *In the setting above,*

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

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

Proposition 4.5. *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 fields L' *which are composita* $L' = LK'$*, up to isomorphism in the sense defined above.*

Proof. By the theorem of the primitive element write $L = K(a) = K[x]/(f(x))$. 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 $L = K(a)$ with a 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 about norms and traces.

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

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

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 $\mathbb{Q}_3 \otimes_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{17}] \cong \mathbb{Q}_3 \oplus K$ so there are two different extensions of absolute value, one unramified and the other ramified.

4.2 Local fields

A local field is a complete field K with absolute value $|\cdot|$ that is locally compact. Archimedean local fields are the same as complete archimedean fields: they are precisely $\mathbb{R}$ or $\mathbb{C}$.

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

Proposition 4.6. *a)* $\mathcal{O}_K$ *is compact*

b) $|\cdot|$ *is discrete*

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

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

b) The compact set $\mathcal{O}_K$ has a nested open cover by the sets $\{a \mid |a| < c\}$ for every $c > 1$. By compactness, there must be a finite subcover, so there must be some $c > 1$ such that there is no $a \in K$ with $|a| \in (1, c)$..

c) $\mathcal{O}_K/\pi\mathcal{O}_K$ is a compact topological space with discrete topology.

□

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

If K is a local field with discrete valuation $\nu : K \to \mathbb{Z}$, then we can define a normalized absolute value $|\cdot|_K$ on K by

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

(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 $\mu(aX) = |a|_K\mu(X)$. This point of view will be more important when we get to the adeles.)

5 September 14

5.1 Local Fields and Global Fields

Last time: a complete field K is a local field if it is locally compact.

If K is nonarchimedean, it is a local field if and only the absolute value is discrete and has finite residue field.

Hence $\mathbb{Q}_p$, $\mathbb{F}_p((t))$ are of local fields. Finite extensions of local fields are also local fields. In fact, we won't prove it, but:

Theorem 5.1. *Every local field is a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$.*

Another definition:

Definition. K is a global field if and only if every completion of K is a local field.

$\mathbb{Q}$ is then a global field by Ostrowski's theorem, likewise $\mathbb{F}_p(t)$. Finite extensions of global fields are global fields.

Again, we won't prove it, but:

Theorem 5.2. *Every global field is a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$.*

One comment about global fields:

Proposition 5.3 (Product formula). *If K is a global field then $\prod_v |a|_v = 1$ for all $a \in K$ using normalized valuations.*

Proof. For $K = \mathbb{Q}$, this is equivalent to $|a|_{\mathbb{R}} = \prod_p p^{v_p(a)}$. Likewise one can check this for $\mathbb{F}_p((t))$.

To deduce it for any global field, use

Claim: L/K an extension,

$$\prod_{v' \text{ extends } v} |a|_{v'} = |N_{L/K} a|_v.$$

Prof of this is exercise. Sketch: use the decomposition $L \otimes_K K_v = \prod_{v' \text{ extends } v} L_{v'}$. For $a \in L$, look at the determinant of the multiplication-by-a map on each side, and take absolute values.

Using the claim, we see that if K satisfies the product formula, the same is true of any finite extension L/K. Since all global fields are extensions of L and $\mathbb{F}_p((t))$ □

5.2 Multiplicative structure of $K^\times$:

Let K be a local field.

We have an exact sequence

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

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

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

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

Then $U_0 = \mathcal{O}^\times$, $U_0/U_1 \cong k^\times$ 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

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

The exact sequence

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

splits because by Hensel's lemma for any $\overline{a} \in k^\times$ there is a unique $a \in \mu_{q-1}(\mathcal{O}^\times)$ that reduces to a.

Observations:

Proposition 5.4. *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 $x^m - a$.

□

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

5.3 p-adic logarithm and exponential

Suppose K is a local field of characteristic 0 and residue characteristic p. Let $\mathcal{O}_K$ be the ring of integers of K, and let π be a uniformizer. Let e be the ramification degree of $K/\mathbb{Q}_p$, aso with $p\mathcal{O}_K = (\pi^e)$. 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 5.5. *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. □

Corollary 5.6. $\mathbb{Z}_p^\times = \mu_p \times U_1 \cong (\mathbb{Z}/(p-1)\mathbb{Z})^+ \times \mathbb{Z}_p^+$ *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: $e/(p-1) < 1$, so the corollary 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 have $0 \to U_n \to U_1 \to U_1/U_n \to 0$, where the first term is isomorphic to $\mathcal{O}_K^+ \cong \mathbb{Z}_p^n$ as a topological group, and the last one is a finite p-group; but this sequence in general doesn't split.

5.4 Unramified extensions

Let L/K be a finite extension of complete fields.

Definition. 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.)

Lemma 5.7. *Suppose* $L = K[a]$*, and there exists* $f(x) \in K[x]$ *such that* $f(a) = 0$ *and* $\overline{f} \in k[x]$ *is separable. Then* L/K *is unramified and* $\mathcal{O}_L = \mathcal{O}_K[a]$.

Proof. Without loss of generality, $f(x)$ is the minimal polynomial of a. Then we claim $\overline{f}(x)$ is also irreducible: otherwise Hensel's lemma would lift any factorization to a factorization of $f(x)$.

Then $\overline{a} \in \ell$ is a root of $\overline{f}(x)$, so

$$[\ell : k] \geq [k(\overline{a})/k] = \deg(\overline{f}(x)) = \deg(f(x)) = [L : K]$$

hence the two are equal and L is unramified.

To show equality, use Nakayama's lemma. First, by the chain of equalities we have $k(\overline{a}) = \ell$. Hence $\mathcal{O}_L = \mathcal{O}_K[a] + \pi_L O_L = \mathcal{O}_K[a] + \pi_K \mathcal{O}_L$ 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 extension L/K (exercise). Hence we may apply Nakayama's lemma to the $\mathcal{O}_K$-submodule $\mathcal{O}_K[a]$ of $\mathcal{O}_L$ to get $\mathcal{O}_L = \mathcal{O}_K[a]$ as desired. □

To give a converse to the lemma: if L/K is unramified, and choose any primitive element $\overline{a}$ of ℓ/k with min poly $\overline{f}(x)$. Lift $f(x) \in \mathcal{O}_K(x)$ and lift a be a root of $f(x)$ lifting $\overline{a}$. Then a 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 $= n$.

At the start of next time we'll show that this is the only unramified extension of K of degree n.

6 September 19

6.1 Unramified extensions, continued

Proposition 6.1. *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 $L = L'$. For this, recall that we have $L' = K(a)$ with a such that the minimal polynomial $f(x)$ of a has the property that the reduction $\bar{f}(x) \in k[x]$ has no repeated roots. In fact, $\bar{f}(x)$ must be irreducible, since a factorization of $\bar{f}(x)$ in $k[x]$ would lift to one of $f(x)$ by Hensel's lemma. Then, using the fact that the finite field k has a unique extension of degree n, $\bar{f}(x)$ must have a root in the residue field ℓ of L. Applying Hensel's lemma we have that f has a root in L. Hence $L' = K(a) = K[x]/f(x)$ injects into L: since $[L' : K] = [L : K] = n$ they must be equal. □

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

Proposition 6.2. *If* L, L' *are ramified extension 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 $\mathrm{Gal}(\ell/k)$.)

In fact, there is an equivalence of categories between (finite unramified extensions of K) and (finite extension 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*.

Corollary 6.3. *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* $\bigcup_{(m,p)=1} K(\zeta_m)$.

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

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

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

As a result we have the exact sequence

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

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, $\nu(\pi) = 1$. 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 $n \geq 0$.

Lemma 6.4. *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 $U_{L,i}/U_{L,i+1} \cong \ell^+$, $U_{K,i}/U_{K,i+1} \cong k^\times$. The result then follows from the HW problem saying that $\mathrm{tr} : \ell^+ \to k^+$ is surjective. □

Now we put the pieces together to show that

Proposition 6.5. *$N : \mathcal{O}_L^\times \to \mathcal{O}_K^\times$ is surjective.*

Proof. Let $a \in \mathcal{O}_K^\times$ be bitrary.

By induction and the previous proposition, can find a sequence $\{b_n\}$ of elements of $\mathcal{O}_L^\times$ such that $Nb_n \equiv a \pmod{\pi^n}$, and $b_{n+1} \equiv b_n \pmod{\mathfrak{p}_L^n}$. Then $b = \lim_{n\to\infty} b_n$ satisfies $Nb = a$. □

6.3 Decomposition and inertia groups:

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

Definition. The decomposition group $D_{\nu'} = D_{\nu'}(L/K)$ is $\{g \in \mathrm{Gal}(L/K) \mid |ga|_{\nu'} = |a|_{\nu'}\}$ 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 $\nu = \nu_{\mathfrak{p}}$ and $\nu' = \nu_{\mathfrak{p}'}$ for some prime $\mathfrak{p}$ of $\mathcal{O}_K$ and some prime $\mathfrak{p}'$ of $\mathcal{O}_L$ above $\mathfrak{p}$, then $D_{\nu'}$ 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 ν archimedean).

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

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

Proposition 6.6. *The place ν' is the only place of L extending ν_Z.*

Proof. The key fact we use here is that $\mathrm{Gal}(L/Z)$ *acts transitively on the set of places on L extending ν_Z.* In class I justified this in the non-archimedean case where $\nu_Z = \nu_{\mathfrak{p}_Z}$ by invoking the result about $\mathrm{Gal}(L/Z)$ acting transitively on primes above $\mathfrak{p}_Z$. However, one can also give a direct proof that deals with the archimedean and non-archimedean places simultaneously:

By homework, we have

$$[L : Z] = \sum_{\nu_L \text{ extends } \nu_Z} [L_{\nu_L} : Z_{\nu_Z}]. \tag{3}$$

Now, if ν_L is in the same Galois orbit as ν', then $[L_{\nu_L} : Z_{\nu_Z}] = |D_{\nu'}|$. Futhermore, there are $|\mathrm{Gal}(L/Z)|/|D_{\nu'}|$ places in this Galois orbit. Hence the total contribution to (3) from the Galois orbit of ν' is $|\mathrm{Gal}(L/Z)| = [L : Z]$ and there can be no other Galois orbits.

For a different direct proof, see Neukirch ANT II.9.1

Using this key fact, we are done since $\mathrm{Gal}(L/z) = D_{\nu'}$ fixes ν', so ν' must be the only place of L extending ν_Z □

Note that the equality $\mathrm{Gal}(L_{\nu'}/K_\nu) \cong D_{\nu'}(L/K) = \mathrm{Gal}(L/Z)$, implies $Z = K_\nu \cap L$ (intersection inside $L_{\nu'}$). Then also: $Z_{\nu_Z} = K_\nu$ If ν 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 ν to ν_Z. (I didn't mention this last sentence in class.)

6.4 The inertia group

Definition. If L/K is a 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. then 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 $D_{v'} \to \mathrm{Gal}(\ell/k)$.

In fact,

Proposition 6.7. *$I_{v'}$ 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.

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 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 same is true of the Galois conjugate $\overline{a'}$, so 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 $I_{v'}$.

Proposition 6.8. *Let L/K be a finite Galois extension of local fields. Then $T(v')$ is the maximal subextension of L that is unramified at 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. On the $\mathrm{Gal}(L/T) = I_{v'}$ 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 $e_{L/T} = 1$.

□

7 September 21

Recall from last time than any finite Galois extension L/K of local fields has an intermediate field T such that L/T is totally ramified and T/K unramified. Last time, we

7.1 Totally ramified extensions

Suppose that L/K is a totally ramified extension of local fields with DVRs $\mathcal{O}_L$ and $\mathcal{O}_K$ respectively. We won't assume L/K Galois. Let the exension be $[L : K] = n$, .

Proposition 7.1. $L = K(\pi_L)$ *and* $\mathcal{O}_L = \mathcal{O}_K(\pi_L)$.

Proof. Note that

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

for $a_i \in L$, and in particular is finite. Hence the $1, \pi_L, \dots, \pi_L^{n-1}$ are linearly independent over K, so form a basis giving $L = K(\pi_L)$.

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

The minimal polynomial $f(x)$ of π_L in $K[x]$ is an *Eisenstein polynomial*, that is, one that satisfies the conditions of the classical Eisenstein's irreducibility criterion.: $f = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ has the property that $\nu_K(c_i) > 0$ for $i = 0, \dots n$, but $\nu_K(c_0) = 1$.

Conversely, if $f \in K[x]$ is Eisenstein, then $L = K(a) = K[x]/f(x)$ is totally ramified, with uniformizer a, since, if $|\cdot|_K$ is an absolute value coming from ν_K and $|\cdot|_L$ is the unique extension to L, we have $|a|_L = |c_0|_K^{1/n}$.

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 $x^m - \pi_L = 0$.

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 $p^r - p^{r-1}$.

7.2 Ramification groups

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

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

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

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

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

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

For the rest of this, though, we'll assume L and K nonarchimedean local fields; write $\nu' = \nu_L$ and $\nu = \nu_K$, $\mathcal{O}'_\nu = \mathcal{O}_L$ and $\mathcal{O}_\nu = \mathcal{O}_K$, and drop the subscript ν', so

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

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

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

In fact,

Proposition 7.2. *For* $i \geq 0$

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

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

By Proposition 7.1, have $\mathcal{O}_L = \mathcal{O}_K[\pi]$, so this now follows from (5). □

Now, for each $i \geq 1$, we can define a map

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

given by $g \mapsto [g\pi_L/\pi_L]$. This is a well-defined injection by Proposition 7.2.

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 $gu/u \in U_{i+1,L}$. Exercise: ϕ_i is a group homomorphism.

Recall that for $i = 0$ have $U_{0,L}/U_{1,L} \cong \ell^\times$ canonically, and for $i > 0$ have $U_{i,L}/U_{i+1,L} \cong \ell^+$ 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 $\zeta_8 \to \zeta_8^i$.

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

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

7.3 Tamely ramified extension

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 7.3. *Let L/K be a tamely ramified Galois extension. Then L/K is contained in the extension $K(\zeta_m, \sqrt[d]{\pi_K})$ for some m, d with $(m, p) = (d, p) = 1$.*

Proof. First of all, WLOG can assume $[L : K]$ totally ramified. If not, replace K with the maximal unramified subextension of K contained in L.

Then L/K is a cyclic extension of $[L : K] = n$ with $(n, p) = 1$.

Let $K' = K(\zeta_n)$, $L' = L(\zeta_n)$. Then $\mathrm{Gal}(L'/K')$ injects into $\mathrm{Gal}(L/K)$, so is cyclic of order d with $d \mid n$. Now use Kummer theory to get $L' = K'(\sqrt[d]{a})$ for some $a \in K'^{\times}$: write $a = \pi_K^r u$. Then $L \subset K'(\sqrt[d]{u}, \sqrt[d]{\pi_K})$. The extension $K'(\sqrt[d]{u})/K$ is unramified, so must be contained in $K(\zeta_m)$ for some m, and we're done. □

(By the discussion above, one can drop the condition that L/K is Galois.)

7.4 A few comments on the big picture

Let's step back and think about abelian extensions of $\mathbb{Q}_p$. First of all, we know that the maximal unramified extension of $\mathbb{Q}_p$ is $\mathbb{Q}_p^{\mathrm{unr}} = \mathbb{Q}_p(\zeta_{\text{prime to } p})$, and this is abelian with $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{unr}}/\mathbb{Q}_p) = \hat{\mathbb{Z}}$.

Assuming class field theory, one obtains that $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{unr}}) = \mathbb{Z}_p^{\times}$.

One can show that the maximal abelian tamely ramified extension of $\mathbb{Q}_p$ is $\mathbb{Q}_p^{\mathrm{ab,tame}} = \mathbb{Q}_p^{\mathrm{unr}}(p^{p-1})$: and $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab,tame}}/\mathbb{Q}_p^{\mathrm{unr}}) = \mathbb{F}_p^{\times}$ is the prime-to-p part of $\mathbb{Z}_p^{\times}$.

7.5 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). 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 piecewise linear.

Define

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

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.

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.

8 September 26

Moving on to the next unit of this class: Galois cohomology. I plan to loosely follow Cassels and Fröhlich. Neukirch's book *Class Field Theory: the Bonn Lectures* is good as a less terse 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.) Dummit and Foote also has a decent introduction to the basics of group cohomology.

8.1 The category of G-modules

Let G be a finite 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.)

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 $g \in G$. If $G = C_n$ then $I_G = (t-1)$, but in general I_G is not principal.

Also element $N = \sum_g g \in \mathbb{Z}[G]$. 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 that if instead $A = L^+$, then N acts as 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 $ga - a$.

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 non-commutative. In general if R is a non-commutative ring 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 identity $B \otimes_G - : \mathbb{Z} - \mathrm{mod} \to G - \mathrm{mod}$ has a left adjoint $\mathrm{Hom}(B, -) : G - \mathrm{mod} \to \mathbb{Z} - \mathrm{mod}$:

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

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

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

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

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

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")

Definition. A G-module is *co-induced* if it is of the form $\mathrm{coInd}^G(X) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)$ for an abelian group with G action given by $g\phi(b) = \phi(bg)$ (this is not the standard action on $\mathrm{Hom}(\mathbb{Z}[G], X)$).

A G-module is *induced* if it is of the form $\mathrm{Ind}^G(X) = \mathbb{Z}[G] \otimes X$. Here the G-action is the standard one: $g(b \otimes x) = gb \otimes x$.

(These definitions are actually equivalent for finite G!)

"Baby Frobenius reciprocity:"

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

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

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 $(g, a) \mapsto ga$.

8.2 Our plan

We will construct group cohomology functors $H^q(G, A)$, $q \geq 0$ such that $H^0(G, A) = A^G$, and such that a short exact sequence of modules gives a long exact sequence in cohomology.

We'll also construct group homology functors $H_q(G, A)$, $q \geq 0$, such that $H_0(G, A) = A_G$ and such that a short exact sequence of modules gives a long exact sequence in homology.

We'll then splice them together, to get what's 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 $H^0(G, L^\times) = K^\times/NL^\times$, which is a group we've seen before in the statements of local class field theory. Ultimately we'll be able to define the Artin map as a cup product with a given cohomology element.

9 September 28

9.1 Clarification about co-induced modules:

Last time we defined $\mathrm{coInd}^G X = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], X)$. This is correct as abelian groups, but the standard way of giving $\mathrm{coInd}^G X$ a G-module structure is not by using the module structure on $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ that I defined last time. That would give $(g\phi)(b) = \phi(g^{-1}b)$. Instead, we will define the G-module structure on $\mathrm{coInd}^G(X)$ by $g\phi(b) = \phi(bg)$.

The upshot here is that if R is any non-commutative ring, in order to make $\mathrm{Hom}_{\mathbb{Z}}(A, B)$ into a left R-module, we need to choose a left R-module structure on B and a right R-module structure on A. For $\mathbb{Z}[G]$ there are two different natural right R-module structures.

Ultimately, this doesn't actually affect the definition of co-induced modules, since the two different right G-module structures on $\mathbb{Z}[G]$ are isomorphic to each other via the map $\sum c_g g \mapsto \sum c_g g^{-1}$.

However, last time I stated that the map $A \mapsto \mathrm{coInd}(A)$ given by $a \mapsto \phi_a$ where $\phi_a(g) = ga$ is a G-module homomorphism; this is true with the G-module structure we have just defined, as $(h\phi_a)(g) = \phi_a(gh) = gha = \phi_{ha}(g)$.

9.2 Group cohomology as derived functor

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

Theorem 9.1. *There is a unique family of functors* $H^q(G, -) : G$*-mod* $\to \mathbb{Z}$*-mod,* $q \geq 0$ *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*

$$\begin{tikzcd}
0 \arrow[r] & H^0(G,A) \arrow[r, "i_*"] & H^0(G,B) \arrow[r, "j_*"] & H^0(G,C) \arrow[dll, rounded corners, "\delta"] \\
 & H^1(G,A) \arrow[r, "i_*"] & H^1(G,B) \arrow[r, "j_*"] & H^1(G,C) \arrow[dll, rounded corners, "\delta"] \\
 & H^2(G,A) \arrow[r] & \dots &
\end{tikzcd}$$

(iii) $H^q(G, A) = 0$ *for* $q \geq 1$ *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

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

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 $q \geq 2$ choose a free module P_q with a surjective map $d_q : P_q \to \ker d_{i-1}$.

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

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

for all q, 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, $K^i = \mathrm{Hom}_G(P_i, A) \cong \mathrm{Hom}_{\mathbb{Z}}(P_i, X)$. Because each P_i is a free $\mathbb{Z}$-module, this sequence is exact and all $H^q(G, A)$ vanish for $q \geq 1$.

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

For base case of $q = 0$, 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 $A^* = \mathrm{Hom}(\mathbb{Z}[G], A)$. 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 $H^{q+1}(A) \cong H^q(A')$ for all $q \geq 1$, so uniqueness follows by induction. □

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

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "i"] \arrow[d, "\phi_A"] & B \arrow[r, "j"] \arrow[d, "\phi_B"] & C \arrow[r] \arrow[d, "\phi_C"] & 0 \\
0 \arrow[r] & A' \arrow[r, "i'"] & B' \arrow[r, "j'"] & C' \arrow[r] & 0
\end{tikzcd}$$

is a morphism of short exact sequences, the diagram

$$\begin{tikzcd}
{} \arrow[r] & H^q(G,A) \arrow[r, "i_*"] \arrow[d, "(\phi_A)_*"] & H^q(G,B) \arrow[r, "j_*"'] \arrow[d, "(\phi_B)_*"] & H^q(G,C) \arrow[r, "\delta"] \arrow[d, "(\phi_C)_*"] & H^{q+1}(G,A) \arrow[r] \arrow[d, "(\phi_A)_*"] & {} \\
{} \arrow[r] & H^q(G,A') \arrow[r, "i'_*"] & H^q(G,B') \arrow[r, "j'_*"'] & H^q(G,C') \arrow[r, "\delta'"] & H^{q+1}(G,A') \arrow[r] & {}
\end{tikzcd}$$

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 $i \geq 1$.

9.3 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 $q+1$-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 $d_i((g_0, \ldots, g_i)) = \sum_j (-1)^j (g_0, \ldots, \hat{g}_j \ldots, g_i)$.

Then $d_i d_{i+1} = 0$. On the other hand, if $d_i(g_0, \ldots, g_i) = 0$ then for any $s \in G$, have also $d_{i+1}(s, g_0, \ldots, g_i) = (g_0, \ldots, g_i)$, so in fact $\ker d_i = \operatorname{im} d_{i+1}$ and hence we have a projective resolution.

(A more homological interpretation: for $s \in G$, the map $h(g_0, \ldots, g_i) = (s, g_0, \ldots, g_i)$ gives a chain homotopy : $dh + hd = 1$, implying exactness.)

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 $\mathrm{Hom}(P_i, A) \cong \tilde{C}^i(G, A)$ 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

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

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

Next time we'll change variables to work with inhomogeneous cochains, which are easier to compute with. For now let's just work out the case of $i = 1$ to see how things go.

Example. We have $\tilde{C}^0(G, A)$ is the set of maps $f : G \to A$ with $f(gg_0) = gf(g_0)$. Any such map is determined by $f(1) = a$, so $\tilde{C}^0(G, A) \cong A$.

Now $\tilde{C}^1(G, A)$ is the set of maps $f : G \times G \to A$ with $f(gg_0, gg_1) = gf(g_0, g_1)$. Any such map is determined by the function $\phi : G \to A$ given by $\phi(g) = f(1, g)$.

We now work out $d^1 : A \cong \tilde{C}^0(G, A) \to \tilde{C}^1(G, A)$. For $a \in A$, $d^1(a)$ is the function $(g_0, g_1) \mapsto g_0(a) - g_1(a)$, and $\tilde{Z}^1(G, A)$ consists of all homogeneous cochains of this form. The corresponding function $\phi : G \to A$ is $g \mapsto a - g(a)$.

On the other side, the map $d^2 : \tilde{C}^1(G, A) \to \tilde{C}^2(G, A)$ sends a homogeneous 1-cochain f to the 2-cochain $d^2 f$ given by

$$d^2 f(g_0, g_1, g_2) = f(g_1, g_2) - f(g_0, g_2) + f(g_0, g_1).$$

The homogeneous cochain f lies in $\tilde{Z}^2(G, A)$ if and only if this is always 0. By homogeneity, it's enough to check this when $g_0 = 1$: we change variables to $(1, g, gh)$. Then our cocycle condition is

$$0 = f(g, gh) - f(1, gh) + f(1, g) = g\phi(h) - \phi(gh) + \phi(g),$$

writing it in terms of the function $\phi(g) = f(1, g)$.

As a result, we see that

$$\begin{aligned} H^1(G, A) \cong & \tilde{Z}^1(G, A)/\tilde{B}^1(G, A) \\ \cong & \big(\text{functions } \phi : G \to A \text{ with } \phi(gh) = \phi(g) + g\phi(h)\big)/ \\ & \quad \big(\text{functions } \phi : G \to A \text{ of the form } \phi(g) = a - g(a)\big). \end{aligned}$$

10 October 3

10.1 Cohomology via inhomogeneous cochains

We generalize the change-of-variables calculation we did to compute H^1 last time.

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

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

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 $d^{i+1} : C^i(G, A) \to C^{i+1}(G, A)$ sends an inhomogeneus i-cochain ϕ to the inhomogeneous $i+1$-cochain $d^{i+1}\phi$ given by

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

(My indices were off by one in class and I called this d^i.)

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* $B_i(G, A) = \operatorname{im}(d^i : C^{i-1}(G, A) \to C^{i+1}(G, A))$. 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-coycles 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.

10.2 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 giving a group G acting on an abelian group A, the semidirect product $G \ltimes A$ is, as a set, $G \times A$, but with the product given by

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

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

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

Additionally, the group 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 a coboundary to ϕ. 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 map of sets, not necessarily a homomorphism. Then we construct a map $\psi : G \times G \to A$ by $s(g)s(h) = \psi(g, h)s(gh)$. Associativity is then equivalent to $\psi \in Z^2(G, A)$, and replacing s by a different map s' adds an element of $B^2(G, A)$ to ψ.

10.3 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". In fact, if we are working just in the context abelian groups with no G-action, then any A-torsor X is isomorphic to A. To give this isomorphism, pick any $x_0 \in X$. Then the map $a \mapsto a + x_0$ is an isomorphism of torsors.

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 $c \in (L^\times)^n$, 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.

Theorem 10.1. *The set of A-torsors is in bijection with $H^1(G, A)$. This bijection sends the trivial A-torsor A to $0 \in H^1(G, A)$.*

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 $c \in C^G$, 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.

10.4 Group homology

We now define group homology functors $H_q(G, A)$ for $q \geq 0$. 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 10.2. *There is a unique family of functors $H_q(G, A)$, $q \geq 0$ with the properties that*

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

b) $H_q(G, A) = 0$ *for* $q \geq 1$ *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*

$$\begin{tikzcd}
\cdots \arrow[r, "i_*"] & H_2(G,B) \arrow[r, "j_*"] & H_2(G,C) \arrow[dll, "\delta"] & \\
H_1(G,A) \arrow[r, "i_*"] & H_1(G,B) \arrow[r, "j_*"] & H_1(G,C) \arrow[dll, "\delta"] & \\
H_0(G,A) \arrow[r, "i_*"] & H_0(G,B) \arrow[r, "j_*"] & H_0(G,C) \arrow[r] & 0
\end{tikzcd}$$

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 $H^q(G, A)$ be the homology of the chain complex $F_i \otimes_G A$. 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.

□

11 October 5

11.1 Group homology, continued

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 11.1. *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}. □

Digression that will be relevant later: Let H be a group that is contained in a larger group G. By the above, $H_1(G, \mathbb{Z}) \cong I_H/(I_H)^2$.

But also, we use the short exact sequence $0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0$, now viewed in the category of H-modules. The $\mathbb{Z}[H]$-module $\mathbb{Z}[G]$ is free, hence induced. The exact sequence is now

$$0 \to H_1(H, \mathbb{Z}) \to I_G/(I_H I_G) \to \mathbb{Z}[G]/I_H\mathbb{Z}[G]$$

so we also have $H_1(H, \mathbb{Z}) \cong \ker : I_G/(I_H I_G) \to \mathbb{Z}[G]/I_H\mathbb{Z}[G] = I_H\mathbb{Z}[G]/I_H I_G$.

Exercise: check directly that $I_H\mathbb{Z}[G]/I_H I_G \cong I_H/I_H^2$.

11.2 Change of group and compatible pairs

So far we've just talked about $H^q(G, A)$ and $H_q(G, A)$ 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 $\lambda(\rho(g')a) = g'a$.

Example. If H is a subgroup of G, then (H, A) and (G, 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, A) and $(G/H, A^H)$ 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 $\rho_* : \mathbb{Z}[(G')^{q+1}] \to \mathbb{Z}[G^{q+1}]$. Recall that the standard resolutions of G' and G respectively are given by $P_q(G') = \mathbb{Z}[(G')^{q+1}]$ and $P_q(G) = \mathbb{Z}[G^{q+1}]$, and ρ_* maps $P_q(G')$ to $P_q(G)$.

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

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

$$\phi'(g_1', \dots, g_q') = \lambda(\phi'(\rho(g_1', \dots, g_q'))).$$

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 $\operatorname{Res} : H^q(G, A) \to H^q(H, A)$ and is called *restriction*. If we work with inhomogeneous cochains, this map is literally restriction: $(\operatorname{Res} \phi)(h_1, \dots, h_q) = \phi(h_1, \dots, h_q)$.

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

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

Note that for any $\phi \in H^q(G, A)$, the inhomogeneous cocycle $\psi = \operatorname{Inf} \circ \operatorname{Res}(\phi)$ 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: $\psi'(h_1, \dots, h_{q-1}) = a$.

(A slicker way of showing $\operatorname{Inf} \circ \operatorname{Res} = 0$ is to make a commutative diagram of induced maps

$$\begin{tikzcd}
H^q(G/H, A^H) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\mathrm{Res}"] & H^q(G, A) \arrow[d, "\mathrm{Res}"] \\
H^q(H/H, A^H) \arrow[r, "\mathrm{Inf}"] & H^q(H, A^H)
\end{tikzcd}$$

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 $H_q(G, A) \to H_q(H, A)$, 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 $\mathrm{id}_A : A \to A$ 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 $A/I^G A \to A/I^H A$; 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 long exact sequence of G-modules, it is also a long exact sequence of H-modules, and the diagrams

$$\begin{tikzcd}
\dots \arrow[r] & H^q(G, A) \arrow[r, "i_*"] \arrow[d, "\mathrm{Res}"] & H^q(G, B) \arrow[r, "j_*"] \arrow[d, "\mathrm{Res}"] & H^q(G, C) \arrow[r, "\delta"] \arrow[d, "\mathrm{Res}"] & H^{q+1}(G, A) \arrow[r] \arrow[d, "\mathrm{Res}"] & \dots \\
\dots \arrow[r] & H^q(H, A) \arrow[r, "i_*"] & H^q(H, B) \arrow[r, "j_*"] & H_q(H, C) \arrow[r, "\delta"] & H^{q+1}(H, A) \arrow[r] & \dots
\end{tikzcd}$$

and

$$\begin{tikzcd}
\dots \arrow[r] & H_q(H, A) \arrow[r, "i_*"] \arrow[d, "\mathrm{Cor}"] & H_q(H, B) \arrow[r, "j_*"] \arrow[d, "\mathrm{Cor}"] & H_q(H, C) \arrow[r, "\delta"] \arrow[d, "\mathrm{Cor}"] & H_{q+1}(H, A) \arrow[r] \arrow[d, "\mathrm{Cor}"] & \dots \\
\dots \arrow[r] & H_q(G, A) \arrow[r, "i_*"] & H_q(G, B) \arrow[r, "j_*"] & H_q(G, C) \arrow[r, "\delta"] & H_{q+1}(G, A) \arrow[r] & \dots
\end{tikzcd}$$

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 $A_H \to A_G$.

11.3 The inflation-restriction exact sequence

Theorem 11.2. *There exists an exact sequence*

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

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 $\phi \in B^1(G/H, A^H)$.

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 cocycle $g \mapsto ga - a$, may assume that $\phi(h) = 0$ for all $h \in H$. Then we have $\phi(gh) = g\phi(h)$ 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 a spectral sequence. However, in a special case, it does hold:

Theorem 11.3. *If $H^i(H, A) = 0$ for $1 \leq i < q$, then there exists an exact sequence*

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

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 $A^* = \mathrm{coInd}^G(A) = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$. 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 $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A)$ is a product of copies of $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[H], A)$, 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 $1 \leq i \leq q - 1$, this gives us $H^i(H, A') = 0$. Therefore, we may apply the inductive hypothesis to A', and we find that

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

For $i = q$, we get that 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, $(A^*)^H = \mathrm{Hom}_{\mathbb{Z}}(G, A)^H = \mathrm{Hom}_{\mathbb{Z}}(G/H, A)$ 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

$$\begin{tikzcd}
0 \arrow[r] & H^{q-1}(G/H,(A')^H) \arrow[r, "\mathrm{Inf}"] \arrow[d, "\delta"] & H^{q-1}(G,A') \arrow[r, "\mathrm{Res}"] \arrow[d, "\delta"] & H^{q-1}(H,A') \arrow[d, "\delta"] \\
0 \arrow[r] & H^q(G/H,A^H) \arrow[r, "\mathrm{Inf}"] & H^q(G,A) \arrow[r, "\mathrm{Res}"] & H^q(H,A)
\end{tikzcd}$$

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

□

12 October 10

12.1 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

$$\begin{tikzcd}
{} \arrow[r] & \hat{H}^{-2}(G,C) \arrow[r] & A_G \arrow[r] \arrow[d, "N_A^*"] & B_G \arrow[r] \arrow[d, "N_B^*"] & C_G \arrow[r] \arrow[d, "N_C^*"] & 0 & \\
& 0 \arrow[r] & A^G \arrow[r] & B^G \arrow[r] & C^G \arrow[r] & \hat{H}^1(G,A) \arrow[r] & {}
\end{tikzcd}$$

to get a doubly infinite long exact sequence

$$\begin{tikzcd}
{} \arrow[r] & \hat{H}^{-2}(G,C) \arrow[r] & \hat{H}^{-1}(G,A) \arrow[r] & \hat{H}^{-1}(G,B) \arrow[r] & \hat{H}^{-1}(G,C) \arrow[dll] & & \\
& & \hat{H}^0(G,A) \arrow[r] & \hat{H}^0(G,B) \arrow[r] & \hat{H}^0(G,C) \arrow[r] & \hat{H}^1(G,A) \arrow[r] & {}
\end{tikzcd}$$

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

Proposition 12.1. *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 $[\sum_{g \in G} gx_g] \mapsto \sum_{g \in G} x_g$ 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 $\mathbb{Z}$-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 $\mathrm{Hom}_G(P_i, A)$, $q \in \mathbb{Z}$.

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

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

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

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 dualize, we get

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

using the isomorphism $\mathbb{Z}[G] \cong \mathrm{Hom}(\mathbb{Z}[G], \mathbb{Z})$ given by sending $1 \in \mathbb{Z}[G]$ to the function $\phi : \mathbb{Z}[G] \to \mathbb{Z}$ given by $\phi(\sum_g c_g g) = c_0$. (In class, I had that the maps were multiplication by $t^{-1} - 1$; that was a mistake and I've corrected it.)

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:

$$\begin{tikzcd}
\cdots \arrow[r] & \mathbb{Z}[G] \arrow[r, "\times(t-1)"] \arrow[d, equal] & \mathbb{Z}[G] \arrow[r, "\times N"] \arrow[d, equal] & \mathbb{Z}[G] \arrow[r, "\times(t-1)"] \arrow[d, equal] & \mathbb{Z}[G] \arrow[r, "\times N"] \arrow[d, equal] & \mathbb{Z}[G] \arrow[r, "\times(t-1)"] \arrow[d, equal] & \mathbb{Z}[G] \arrow[r, "\times N"] \arrow[d, equal] & \mathbb{Z}[G] \arrow[r, "\times(t-1)"] \arrow[d, equal] & \mathbb{Z}[G] \arrow[r] \arrow[d, equal] & \cdots \\
& P_3 & P_2 & P_1 & P_0 & P_{-1} & P_{-2} & P_{-3} & P_{-4} &
\end{tikzcd}$$

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

$$\begin{tikzcd}
\cdots & \mathbb{Z}[G] \arrow[l] \arrow[d, equal] & \mathbb{Z}[G] \arrow[l, "\times N"'] \arrow[d, equal] & \mathbb{Z}[G] \arrow[l, "\times(t-1)"'] \arrow[d, equal] & \mathbb{Z}[G] \arrow[l, "\times N"'] \arrow[d, equal] & \mathbb{Z}[G] \arrow[l, "\times(t-1)"'] \arrow[d, equal] & \cdots \arrow[l] \\
& \mathrm{Hom}(P_2, A) & \mathrm{Hom}(P_1, A) & \mathrm{Hom}(P_0, A) & \mathrm{Hom}(P_{-1}, A) & \mathrm{Hom}(P_{-2}, A) &
\end{tikzcd}$$

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

12.2 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

$$\begin{tikzcd}
\hat{H}^q(G,A) \arrow[r, "\delta", "\sim"'] \arrow[d, "\mathrm{Res}_q"] & \hat{H}^{q+1}(G,A^-) \arrow[d, "\mathrm{Res}_{q+1}"] \\
\hat{H}^q(H,A) \arrow[r, "\delta", "\sim"'] & \hat{H}^{q+1}(H,A^-)
\end{tikzcd}$$

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

$$\begin{tikzcd}
\hat{H}^q(G,C) \arrow[r, "\delta"] \arrow[d, "\mathrm{Res}_q"] & \hat{H}^{q+1}(G,A) \arrow[d, "\mathrm{Res}_{q+1}"] \\
\hat{H}^q(H,C) \arrow[r, "\delta"] & \hat{H}^{q+1}(H,A)
\end{tikzcd}$$

and

$$\begin{tikzcd}
\hat{H}^q(G,C) \arrow[r, "\delta"] & \hat{H}^{q+1}(G,A) \\
\hat{H}^q(H,C) \arrow[r, "\delta"] \arrow[u, "\mathrm{Cor}_q"] & \hat{H}^{q+1}(H,A). \arrow[u, "\mathrm{Cor}_{q+1}"]
\end{tikzcd}$$

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 $\mathrm{Res}_0 : \hat{H}^0(G, A) \to \hat{H}^0(G, A)$ 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 12.2. *The map* $\mathrm{Cor}_0 : \hat{H}^0(H, A) \to \hat{H}^0(G, A)$ *is induced by the map* $N_{G/H} : A^G \to A^H$ *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* $N'_{G/H} : A_H \to A_G$ *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:

$$\begin{tikzcd}
\hat{H}^{-1}(G, C) \arrow[r, "\delta"] \arrow[d, "N'_{G/H}"] & \hat{H}^{0}(G, A) \arrow[d, "\mathrm{Res}_{q+1}"] \\
\hat{H}^{-1}(H, C) \arrow[r, "\delta"] & \hat{H}^{0}(H, A).
\end{tikzcd}$$

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 12.3. *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 12.4. *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 $n : H^q(G, A) \to H^q(G, A)$ factors through $H^q(H, A) = 0$, 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 $\mathrm{Res} \circ \mathrm{Cor}$ 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. □

13 October 12

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

b) Item $p = q = 0$, $\cup : H^0(G, A) \times H^0(G, B) \to H^0(G, A \otimes B)$ 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 $b \in H^p(G, B)$ 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
$$\delta(a \cup b'') = (-1)^p a \cup \delta(b'').$$

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

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

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.

If f and f' are homogeneous cochains, then define $f \cup f'$ by

$$f \cup f'(g_0, \dots, g_{p+q}) = f(g_0, \dots, g_p) \otimes f'(g_p, \dots, g_{p+q}).$$

If ϕ and ϕ' are inhomogeneous cochains, define $\phi \cup \phi'$ by

$$\phi \cup \phi'(g_1, \dots, g_{p+q}) = \phi(g_1, \dots, g_p) \otimes g_1 \dots g_p \phi'(g_{p+1}, \dots, g_q).$$

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, for 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 $g = 0$.

13.2 Our plan

Notation: Let L/K be a finite Galois extension. If A is a $\mathrm{Gal}(L/K)$-module, write $H^q(L/K, A)$ for $H^q(\mathrm{Gal}(L/K, A)$, this is called the *Galois cohomology* of A.

For any finite Galois extension L/K, we'll construct an isomorphism

$$\mathrm{inv}_{L/K} : H^2(L/K, L^\times) \cong (\frac{1}{n}\mathbb{Z}/\mathbb{Z}).$$

This map is known as the *invariant map*, and gives a canonical generator $u_{L/K} = \mathrm{inv}^{-1}(1/n) \in H^2(L/K, L^\times)$.

We'll then show that cup product $\cup u_{L/K} : H^{-2}(L/K, \mathbb{Z}) \to H^0(L/K, L^\times)$ is an isomorphism. Since $H^{-2}(L/K, \mathbb{Z}) \cong \mathrm{Gal}(L/K)^{ab}$ and $H^0(L/K, L^\times) \cong K^\times/NL^\times$, this will give us an isomorphism $K^\times/NL^\times \cong \mathrm{Gal}(L/K)^{ab}$.

(This is actually a bit more than I've previously promised: when I stated the main theorem of local class field theory before, I restricted to the case of L/K abelian, in which case you get an isomorphism $\mathrm{Gal}(L/K) \cong K^\times/NL^\times$.)

We'll need two main ingredients for this; first we'll need to understand the Galois cohomology of $L^\times$. Then we'll need a purely cohomological result (Tate's theorem) that will guarantee for us that $\cup u_{L/K}$ is an isomorphism.

13.3 Hilbert's Theorem 90

Now we're going to do some Galois cohomology. Before doing Galois cohomology of $L^\times$, I want to say something about why L^+ doesn't have any interesting Galois cohomology.

Proposition 13.1. *L^+ is a coinduced G-module.*

This is a consequence of the Normal Basis Theorem, which we won't prove here. It says that there exists $a \in L$ such that $\{ga \mid g \in G\}$ forms a basis of L. Hence $L^+ = \oplus_{g \in G} g(aK^+)$.

Corollary 13.2. *$\hat{H}^q(L/K, L^+) = 0$ 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 13.3 (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 13.4 (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.

13.4 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 13.5. *Let* G *be a topological group. TFAE:*

a) G *is profinite*

b) G *is compact 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:

$$H^1(K, \bar{K}^\times) = \varprojlim_{L/K \text{ finite}} H^1(L/K, L^\times) = \varprojlim_{L/K \text{ finite}} 1 = 1$$

Which parts of Galois 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 compatibile in the right way).

Cup products still work.

14 October 17

14.1 Clarification from last time

The way I defined $H^q(K, A)$ last time is not quite correct in the case when K has positive characteristic.

Instead, let K^{sep} denote the separable closure of K. We have $K^{\text{sep}} = \bar{K}$ when $\operatorname{char} K = 0$ or more generally when K is perfect (eg $K = \mathbb{F}_p$), but in general K^{sep} is the subfield of $\bar{K}$ which is the union of all finite Galois extensions of K (since Galois implies separable).

Then, for any K and any $\operatorname{Gal}(K^{\text{sep}}/K)$-module A, define $H^q(K, A) = H^q(\operatorname{Gal}(K^{\text{sep}}/K), A)$.

Then the profinite version of Hilbert's theorem 90 is:

Theorem 14.1 (Profinite Hilbert 90)**.** *If K is a field, then $H^1(K, (K^{\text{sep}})^\times) = 0$.*

14.2 Application to Kummer theory

Let K be any field, and let n be a natural number with $(n, \operatorname{char} K) = 1$.

The short exact sequence of $\operatorname{Gal}(K^{\text{sep}}/K)$-modules

$$1 \to \mu_n \to (K^{\text{sep}})^\times \to (K^{\text{sep}})^\times \to 1.$$

yields the long exact sequence in cohomology:

$$1 \to \mu_n(K) \to K^\times \to K^\times \to H^1(K, \mu_n) \to H^1(K, (K^{\text{sep}})^\times) = 0.$$

Hence the connecting homomorphism $\delta : K^\times \to H^1(K, \mu_n)$ induces an isomorphism

$$K^\times/(K^\times)^n \cong H^1(K, \mu_n)$$

Suppose $\mu_n \subset K$, so μ_n has trivial $\operatorname{Gal}(K^{\text{sep}}/K)$ action. Then $H^1(K, \mu_n)$ is the set of continuous homomorphisms $\phi : \operatorname{Gal}(\overline{K}/K) \to \mu_n$: these must factor through the kernel, which will be $\operatorname{Gal}(L/K)$ for some L, so this is the set of fields L/K along with an inclusion $\operatorname{Gal}(L/K) \hookrightarrow \mu_n$.

We can compute the connecting homomorphism δ: for $a \in K^\times$, $\delta(a)$ is the cocycle ϕ_a given by $\phi_a(g) \mapsto \frac{g\sqrt[n]{a}}{\sqrt[n]{a}}$, with kernel field $K[\sqrt[n]{a}]$.

From this we can get the classical statement of Kummer theory: if $K \supset \mu_n$ and L/K is a cyclic extension of degree n, then take an isomorphism $\phi : \operatorname{Gal}(L/K) \to \mu_n$, so $\phi \in H^1(K, \mu_n)$. The inflation $\inf \phi$ is then an element of $H^1(K^{\text{sep}}/K, \mu_n)$, and is equal to $\delta(a)$ for some $a \in K^\times$. Hence $\operatorname{Gal}(K^{\text{sep}}/L) = \ker \inf \phi = \ker(\delta(a)) = \operatorname{Gal}(K^{\text{sep}}/K(\sqrt[n]{a}))$. By the Galois correspondence, we deduce $L = K(\sqrt[n]{a})$ is generated by the nth root of an element of K.

14.3 $H^2(L/K, L^\times)$ 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.)

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 14.2. $\hat{H}^q(L/K, \mathcal{O}_L^\times) = 0$ *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 $q = 1$, use LES

$$0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{\nu_L} \mathbb{Z} \to 0$$

get

$$K^\times \xrightarrow{\nu_L} \mathbb{Z} \to H^1(L/K, \mathcal{O}_L^\times) \to H^1(L/K, L^\times).$$

On the one side, L/K is unramified, so $\nu_L : K^\times \to \mathbb{Z}$ is surjective. On the other side $H^1(L/K, L^\times) = 0$. Hence $H^1(L/K, \mathcal{O}_L^\times) = 0$. □

Using the long exact sequence coming from the short exact sequence

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

and applying the lemma above, we see that the map $\nu_* : H^2(L/K, L^\times) \to H^2(L/K, \mathbb{Z})$ 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

$$H^2(L/K, L^\times) \xrightarrow{\nu_*} H^2(L/K, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(L/K, \mathbb{Q}/\mathbb{Z}) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

We now wish to determine

$$H^2(K^{\mathrm{unr}}/K,(K^{\mathrm{unr}})^\times) = \varinjlim_{L/K \text{ finite unram}} H^2(L/K,L^\times) = \varinjlim_{n} H^2(K_n/K,K_n^\times)$$

where K_n/K is the unique ramified 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

$$\begin{tikzcd}
H^2(K_n/K,K_n^\times) \arrow[r, "\nu_*"] \arrow[d, "\mathrm{Inf}"] & H^2(K_n/K,\mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "\mathrm{Inf}"] & H^1(K_n/K,\mathbb{Q}/\mathbb{Z}) \arrow[r] \arrow[d, "\mathrm{Inf}"] & \frac{1}{n}\mathbb{Z}/\mathbb{Z} \arrow[d, hook] \\
H^2(K_N/K,K_N^\times) \arrow[r, "\nu_*"] & H^2(K_N/K,\mathbb{Z}) \arrow[r, "\delta^{-1}"] & H^1(K_N/K,\mathbb{Q}/\mathbb{Z}) \arrow[r] & \frac{1}{N}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

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

$$H^2(K^{\mathrm{unr}}/K,(K^{\mathrm{unr}})^\times) \cong \varinjlim_{n} H^2(K_n/K,K_n^\times) \cong \varinjlim_{n} \frac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}.$$

As in the finite case, we denote the isomorphism $H^2(K^{\mathrm{unr}}/K,(K^{\mathrm{unr}})^\times) \to \mathbb{Q}/\mathbb{Z}$ by inv_K. For any L/K finite we can view $H^2(L/K,L^\times)$ as a subgroup of $H^2(K^{\mathrm{unr}}/K,(K^{\mathrm{unr}})^\times)$, and then the restriction of inv_K to $H^2(K^{\mathrm{unr}}/K,(K^{\mathrm{unr}})^\times)$ that we've defined above is $\mathrm{inv}_{L/K}$.

Now, suppose L/K is a finite extension of degree n; don't need to assume unramified or Galois. Then $L^{\mathrm{unr}} = L \cdot K^{\mathrm{unr}}$, since $K^{\mathrm{unr}} = \bigcup_{(r,p)=1} K(\zeta_r)$ (p the residue characteristic) and likewise $L^{\mathrm{unr}} = \bigcup_{(r,p)=1} L(\zeta_r)$. It follows that the natural map $\mathrm{Gal}(L^{\mathrm{unr}}/L) \to \mathrm{Gal}(K^{\mathrm{unr}}/K)$ is injective.

Hence we can make a restriction map:
$\mathrm{Res} : H^2(K^{\mathrm{unr}}/K,(K^{\mathrm{unr}})^\times) \to H^2(L^{\mathrm{unr}}/L,(L^{\mathrm{unr}})^\times)$.

Proposition 14.3. $\mathrm{inv}_L \circ \mathrm{Res} = n \cdot \mathrm{inv}_K$.

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:

$$\begin{tikzcd}
H^2(K^{\mathrm{unr}}/K,(K^{\mathrm{unr}})^\times) \arrow[r, "e\cdot(\nu_K)_*"] \arrow[d, "\mathrm{Res}"] & H^2(K^{\mathrm{unr}}/K,\mathbb{Z}) \arrow[r, "\delta^{-1}"] \arrow[d, "\mathrm{Res}"] & H^1(K^{\mathrm{unr}}/K,\mathbb{Q}/\mathbb{Z}) \arrow[r, "f\cdot\mathrm{eval}_{\mathrm{Frob}_K}"] \arrow[d, "\mathrm{Res}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, equal] \\
H^2(L^{\mathrm{unr}}/L,(L^{\mathrm{unr}})^\times) \arrow[r, "(\nu_L)_*"] & H^2(L^{\mathrm{unr}}/L,\mathbb{Z}) \arrow[r, "\delta^{-1}"] & H^1(L^{\mathrm{unr}}/L,\mathbb{Q}/\mathbb{Z}) \arrow[r, "\mathrm{eval}_{\mathrm{Frob}_L}"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

The first square commutes because

$$\begin{tikzcd}
(K^{\mathrm{unr}})^\times \arrow[r, "e\cdot\nu_K"] \arrow[d, hook] & \mathbb{Z} \arrow[d, equal] \\
(L^{\mathrm{unr}})^\times \arrow[r, "\nu_L"] & \mathbb{Z}
\end{tikzcd}$$

commutes (defintion 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 $\bar{k}/k$. □

14.4 What's next

We now want to construct for any Galois extension L/K of local fields of degree n, possibly ramified, an isomorphism $\mathrm{inv}_{L/K} : H^2(L/K, L^\times) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. Equivalently, we want to find a generator $u_{L/K} \in H^2(L/K, L^\times)$ of order n (if we know $\mathrm{inv}_{L/K}$ we will let $u_{L/K} = \mathrm{inv}_{L/K}^{-1}(\frac{1}{n})$).

Our plan for this will first be to construct an element $u_{L/K} \in H^2(L/K, L^\times)$ of order n. Then we will show by independent methods that $|H^2(L/K, L^\times)| \le n$. Putting these two facts together, we must have equality and $u_{L/K}$ must generate.

To construct $u_{L/K}$, we apply the unramified case and diagram-chase. Let K_n/K be the unramified extension of degree n, and let $L_n = K_nL$. We define $u_{K_n/K} = \mathrm{inv}_{K_n/K}^{-1}(\frac{1}{n})$. We have inflation maps $\mathrm{Inf}_{K_n} : H^2(K_n/K, K_n^\times) \to H^2(L_n/K, L_n^\times)$ and $\mathrm{Inf}_L : H^2(L/K, K_n^\times) \to H^2(L_n/K, K_n^\times)$. We then will define

$$u_{K_n/K} = (\mathrm{Inf}_L)^{-1}\,\mathrm{Inf}_{K_n}(u_{K_n/K}).$$

On the other side, to bound the order $|H^2(L/K, L^\times)|$ we'll use induction. One corollary of the whole ramification group setup is that if L/K is a Galois extension of local fields then $\mathrm{Gal}(L/K)$ is solvable. So it'll be enough to check cyclic extensions and induct.

15 October 19

15.1 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 $u_n = u_{K_n/K} \in H^2(K_n/K)$ be the element such that $\mathrm{inv}_{K_n/K}(u_n) = \frac{1}{n}$. Then we have a diagram

$$\begin{tikzcd}
H^2(L_n/L, L_n^\times) \arrow[r, hook] & H^2(L^{\mathrm{unr}}/L, (L^{\mathrm{unr}})^\times) \arrow[r, "\mathrm{inv}_L"] & \mathbb{Q}/\mathbb{Z} \\
H^2(K_n/K, K_n^\times) \arrow[r, hook] \arrow[u, "\mathrm{Res}"] & H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times) \arrow[r, "n\cdot\mathrm{inv}_K"] \arrow[u, "\mathrm{Res}"] & \mathbb{Q}/\mathbb{Z}. \arrow[u, equal]
\end{tikzcd}$$

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

$$\begin{tikzcd}
& H^2(L_n/L, L_n^\times) & & H^2(L_n/K_n, K^\times) & \\
& & H^2(L_n/K, L_n^\times) \arrow[ul, "\mathrm{Res}_L"'] \arrow[ur, "\mathrm{Res}_{K_n}"] & & \\
& H^2(K_n/K, K_n^\times) \arrow[uu, "\mathrm{Res}"] \arrow[ur, "\mathrm{Inf}_{K_n}"] & & H^2(L/K, L^\times) \arrow[ul, "\mathrm{Inf}_L"'] & \\
0 \arrow[ur] & & & & 0 \arrow[ul]
\end{tikzcd}$$

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 $|H^2(L/K, L^\times)| \le n$, so in fact we have equality and $u_{L/K}$ generates.

15.2 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 15.1. *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 15.2. *The Herbrand quotient* $h(\mathcal{O}_L^\times) = 1$.

Proof. Use short exact sequence $0 \to V \to \mathcal{O}_L^\times \to \mathcal{O}_L^\times / V$ to0. 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 15.3. *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 15.4. *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 alerady 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

$$0 \to H^2(M/K, M^\times) \to H^2(L/K, L^\times) \to H^2(L/M, M^\times)$$

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 15.5. *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 15.6. *If K is a local field, then the inflation map*

$$H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times) \to H^2(K^{\mathrm{sep}}/K, (K^{\mathrm{sep}})^\times) = \mathrm{Br}(K)$$

is an isomorphism.

Hence have isomorphism $\mathrm{inv}_K : \mathrm{Br}(K) \to \mathbb{Q}/\mathbb{Z}$.

Proof. We alrady know that inflation is injective. To prove surjectivity: any element of $H^2(K^{\mathrm{sep}}/K, (K^{\mathrm{sep}})^\times)$ 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 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 15.7. *if L/K is a finite extension of local fields, of degree n, then the diagram*

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\mathrm{inv}_K"] \arrow[d, "\mathrm{Res}"] & \mathbb{Q}/\mathbb{Z} \arrow[d, "n\cdot"] \\
\mathrm{Br}(L) \arrow[r, "\mathrm{inv}_L"] & \mathbb{Q}/\mathbb{Z}
\end{tikzcd}$$

commutes (where the map on the right is multiplication by n).

Proof. Immediate consequence of Theorem 15.6 and Proposition 14.3. □

Proposition 15.8. *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. □

Likewies, if $E/L/K$ is a tower with E/K and L/K both Galois, $\mathrm{Inf}(u_{E/K}) = [L : K] \cdot u_{L/K})$.

15.3 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 15.9 (Tate)**.** *If G is a finite group and A 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 15.5.

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.

16 October 24

16.1 Proof of Tate's theorem

Last time we stated

Theorem 16.1 (Tate)**.** *If G is a finite group and A 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:

$$\begin{tikzcd}
\hat{H}^q(G,\mathbb{Z}) \arrow[r, "-\cup a"] \arrow[dr, "-\cup b"'] & H^{q+2}(G,A) \arrow[d, "\wr"] \\
 & \hat{H}^q(G,B)
\end{tikzcd}$$

So it's enough to show that if $H^{-1}(H,B) = 0$ for all $H \subset G$ and $H^2(H,B)$ 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 $n \mapsto nb$. The problem is that the map $n \mapsto nb$ is not necessarily injective. To fix this, we'll replace B to 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 $i(n) = (nb, nN)$ (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

$$\begin{tikzcd}
\hat{H}^q(H,\mathbb{Z}) \arrow[r, "i_*"] \arrow[dr, "\cup b"'] & \hat{H}^q(H,B) \arrow[d, "\wr"] \\
 & \hat{H}^q(H,B')
\end{tikzcd}$$

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 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. □

16.2 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 recirpocity map:

Proposition 16.2. *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 current homework, 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 16.3. *Let $E/L/K$ be a tower of local fields with E/K and L/K Galois. Let $\pi_{E/L}$ be the canonical surjection $\mathrm{Gal}(E/K) \to \mathrm{Gal}(L/K)$ For any $a \in K^\times$ we have*

$$\pi_{E/L}(\theta_{E/K}([a])) = \theta_{L/K}([a])$$

Proof. By the characterization we've just proved it's enough to show that

$$\chi(\pi_{E/L}(\theta_{E/K}([a]))) = \mathrm{inv}_{L/K}([a] \cup \delta\chi).$$

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 $\chi' = \chi \circ \pi_{E/L}$. Note that $\chi' = \mathrm{Inf}\,\chi \in H^1(E/K, \mathbb{Q}/\mathbb{Z})$,

Then

$$\begin{aligned}\chi(\pi_{E/L}(\theta_{E/K}([a]))) &= \chi'(\theta_{E/K}([a])) = \mathrm{inv}_{E/K}([a] \cup \delta\chi') \\ &= \mathrm{inv}_{E/K}([a] \cup \delta(\mathrm{Inf}_{E/L}\,\chi)) \\ &= \mathrm{inv}_{E/K}(\mathrm{Inf}_{E/L}([a] \cup \delta\chi)) \\ &= \mathrm{inv}_{L/K}([a] \cup \delta\chi)\end{aligned}$$

by compatibility of inv with inflation. □

We can restate this proposition as saying that we have a commutative diagram:

$$\begin{tikzcd}
K^\times \arrow[r, "\theta_{E/K}"] \arrow[dr, "\theta_{L/K}"'] & \mathrm{Gal}(E/K)^{ab} \arrow[d, "\pi_{E/L}"] \\
 & \mathrm{Gal}(L/K)^{ab}
\end{tikzcd}$$

Hence the maps $\theta_{L/K}$ for L/K finite Galois combine to give a map

$$\theta_{/K} : K^\times \to \varinjlim_{L/K \text{ finite Galois}} \mathrm{Gal}(L/K)^{\mathrm{ab}} \cong \mathrm{Gal}(K^{\mathrm{ab}})/K.$$

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

$$\begin{tikzcd}
K^\times \arrow[r, "\theta_{/K}"] \arrow[d, "\nu"] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[d] \\
\mathbb{Z} \arrow[r, hook] & \hat{\mathbb{Z}} \cong \mathrm{Gal}(K^{\mathrm{unr}}/K).
\end{tikzcd}$$

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 $\theta_{/K}$.

16.3 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 $|\mathrm{Gal}(L/K)|^{\mathrm{ab}}$. (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, $(K^\times)^n \cap U_r = U_{r+\nu(n)}$), so finite index subgroups are open.

17 October 26

17.1 Existence

Proposition 17.1. *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

$$[L:K] = |\operatorname{Gal}(L/K)| = |K^\times/NL^\times| = [K^\times : NL^\times]$$

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 $\theta_{/K}(A) \subset \operatorname{Gal}(K^{ab}/K)$.

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

$$[(K^{ab})^{\theta_{/K}(NL^\times)} : K] = [\operatorname{Gal}(K^{ab}/K) : \theta_{/K}(NL^\times)] = [\theta_{/K}K^\times : \theta_{/K}NL^\times] = [K^\times : NL^\times] = [L:K]$$

since the kernel of $\theta_{/K}$ is contained in $NL^\times$. Hence we have equality. □

Proposition 17.2. *If* A *is normic any* $B \supset A$ *is normic. If* A *and* B *are normic, so is* $A \cap B$.

Proof. Suppose $A = NL^\times$, so $\operatorname{Gal}(L/K) \cong K^\times/A$. Then for any $B \supset A$ take M to be the fixed field of $\theta_{L/K}(B/A)$. Have diagram

$$\begin{tikzcd}
K^\times/NL^\times \arrow[r, "\theta_{L/K}"] & \operatorname{Gal}(L/K) \\
K^\times/NM^\times \arrow[r, "\theta_{M/K}"] & \operatorname{Gal}(M/K)
\end{tikzcd}$$

where the vertical maps are the natural projections and the horizontal maps are isomorphisms. Then $\theta_{L/K}(B/A) = \operatorname{Gal}(M/L)$ is the kernel of the projection $\operatorname{Gal}(L/K) \to \operatorname{Gal}(M/K)$, 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 $\theta_{M/K}(a) = 1 \in \operatorname{Gal}(M/K)$ and $\theta_{L/K}(a) = 1 \in \operatorname{Gal}(L/K)$, so $\theta_{LM/K}(a) = 1$ in $\operatorname{Gal}(LM/K)$. □

(Eg normic subgroups form a neighborhood base at 1 for a topology on $K^\times$.)

To show that every finite index subgroup of $K^\times$ is normic, it's enough to show that

Proposition 17.3. *Assume K has characteristic 0. Then 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. □

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. Instead we'll prove existence again later using formal groups, and that argument will work in all characteristics.

17.2 Reciprocity map and ramification

Theorem 17.4. *Let L/K be a finite unramified extension of local fields (automatically Galois and abelian). Then $\theta_{L/K}([a]) = \mathrm{Frob}_{L/K}^{\nu(a)}$.*

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:

$$H^2(L/K, L^\times) \xrightarrow{\nu_*} H^2(L/K, \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(L/K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\mathrm{eval}_{\mathrm{Frob}}} \frac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

So

$$[a] \cup \delta\chi \mapsto \nu_p(a) \cdot \delta\chi \mapsto \nu_p(a)\chi \mapsto \chi(\mathrm{Frob}_p^{\nu(a)}).$$

□

Proposition 17.5. *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 $f \mid \nu_K(a)$. Then let $b = a \cdot N(\pi_L)^{-\nu_K(a)/f}$. □

17.3 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 $\{x \mid \nu_p(x) \text{ even}\}$ (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 $a \in \mathbb{Z}$, $a > 0$, $(a, 2p) = 1$.

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 $(a, K_w/\mathbb{Q}_p) = (-1)^{\nu_p(a)}$; either way

$$(a, K_w/\mathbb{Q}_p) = \left(\frac{\ell^*}{p}\right)^{\nu_p(a)}.$$

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 $v = \infty$ so $\mathbb{Q}_v = \mathbb{R}$. 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.

18 October 31

18.1 The big picture for $\mathbb{Q}_p$

For any local field K and any uniformizer $\pi \in K$, have $\operatorname{Gal}(K^{ab}/K) \cong (\mathcal{O}_K)^\times \times \pi^{\hat{\mathbb{Z}}}$.

Let K^{unr} be the fixed field of $\mathcal{O}_K^\times$, 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 $\hat{\mathbb{Z}} \cong \operatorname{Gal}(K^{unr}/K)$ and $\mathcal{O}_K^\times \cong \operatorname{Gal}(K^\pi/K)$.

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 $\mathbb{Q}_p^\pi = \mathbb{Q}_p(\zeta_{p^\infty})$.

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 $\theta_{\mathbb{Q}(\zeta_{p^m}/\mathbb{Q}} : \mathbb{A}_\mathbb{Q} \to \operatorname{Gal}(\mathbb{Q}(\zeta_{p^m}/\mathbb{Q}))$, 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.

18.2 Some broader context: group schemes

Lubin-Tate theory is a generalization of the theory of cyclotomic fields: to do this we'll first understand what's so special about cyclotomic fields. For this we'll talk about affine group schemes.

Motivating question of affine group schemes. Let A be a ring; in this context all A-algebras are assumed to be commutative. For which A-algebras R is $\mathrm{Hom}(R, B)$ naturally a group for any A-algebra B? More precisely: we want $G(B) = \mathrm{Hom}(R, B)$ to be a functor from A-algebras to groups; G is referred to as the *affine group scheme* coming from A.

Example. $R = A[t]$, then $\mathrm{Hom}(R, B) \leftrightarrow B$ is a group under addition. We denote this group scheme by $\mathbb{G}_a$, so $\mathbb{G}_a(B) = B^+$.

Example. $R = A[t, t^{-1}]$, $\mathrm{Hom}(R, B) \leftrightarrow \mathbb{G}_m(B) = B^\times$.

Example. The group scheme μ_n: here $R = A[t, t^{-1}]/t^n = A[t]/t^n$, $\mathrm{Hom}(R, B) \leftrightarrow \mu_n(B)$. Note that $\mu_n(B)$ is naturally a subgroup of $B^\times$, so μ_n is a sub-group scheme of $\mathbb{G}_m$.

Example. The group scheme GL_n: let $R = A[t_{ij,1\le i,j\le n}, \det^{-1}]$, where $\det \in A[t_{ij,1\le i,j\le n}]$ is the determinant of the matrix $[t_{ij}]$. Then $GL_n(B) \leftrightarrow \mathrm{Hom}(R, B)$.

Answer to motivating question: A necessary (and in fact sufficent) condition is that R is a *Hopf algebra* over A.

Definition. A (commutative) *Hopf algebra* over A is a commutative A-algebra R with the following extra structure

- a map $\Delta : A \to A \otimes A$ called *comultiplication*
- a map $S : A \to A$ called *coinversion*
- a map $\epsilon : A \to R$ called the *counit*

(all tensor products taken over A) such that the following diagrams commute:

$$\begin{tikzcd}
R \arrow[r, "\Delta"] \arrow[d, "\Delta"'] & R \otimes R \arrow[d, "\mathrm{id} \otimes \Delta"] \\
R \otimes R \arrow[r, "\Delta \otimes \mathrm{id}"] & R \otimes R \otimes R
\end{tikzcd}
\quad
\begin{tikzcd}
R \arrow[r, "\Delta"] \arrow[dr, "\mathrm{id}"] & R \otimes R \arrow[d, "\epsilon \otimes \mathrm{id}"] \\
 & R
\end{tikzcd}
\quad
\begin{tikzcd}
R \arrow[r, "\Delta"] \arrow[dr, "\mathrm{id}"] & R \otimes R \arrow[d, "\mathrm{id} \otimes \epsilon"] \\
 & R
\end{tikzcd}
\quad
\begin{tikzcd}
R \arrow[r, "\Delta"] \arrow[d, "\epsilon"] & R \otimes R \arrow[r, "S \otimes \mathrm{id}"] & R \otimes R \arrow[d, "m"] \\
A \arrow[rr, "i"] & & R
\end{tikzcd}$$

where in the last diagram the map $m : R \otimes R \to R$ is defined by $m(x \otimes y) = xy$.

If R is a Hopf algebra, we obtain a group law on $\mathrm{Hom}(R, B)$ by the composition

$$\mathrm{Hom}(R, B) \times \mathrm{Hom}(R, B) \cong \mathrm{Hom}(R \otimes R, B) \xrightarrow{\Delta^*} \mathrm{Hom}(R, B)$$

where the first map sends ϕ_1, ϕ_2 to ϕ given by $\phi(r_1 \otimes r_2) = \phi_1(r_1)\phi_2(r_2)$, and the second one sends ϕ to $\phi \circ \Delta$.

Applying the functor $\mathrm{Hom}(-, B)$ to the diagram above gives proofs of the group law axioms on $\mathrm{Hom}(R, B)$.

Also, $G(B) = \mathrm{Hom}(R, B)$ will be abelian for all B if and only if the diagram

$$\begin{tikzcd}
 & R \arrow[dl, "\Delta"'] \arrow[dr, "\Delta"] & \\
R \otimes R \arrow[rr, "x\otimes y \mapsto y \otimes x"'] & & R \otimes R
\end{tikzcd}$$

commutes, in which case we say that the group scheme G is abelian.

Example. If $G = \mathbb{G}_a$, $R = A[t]$, the map $\Delta : A[t] \to A[t] \otimes A[t]$ is determined by $\Delta(t) = 1 \otimes t + t \otimes 1$, S is determined by $S(t) = -t$ and ϵ by $\epsilon(t) = 0$. Can check that

$$(\Delta \otimes 1)(\Delta(t)) = (1 \otimes \Delta)(\Delta(t)) = t \otimes 1 \otimes 1 + 1 \otimes t \otimes 1 + 1 \otimes 1 \otimes t.$$

and likewise that the other axioms are satisfied.

Also, can check that the group law is as stated.

Example. If $G = \mathbb{G}_m$, $R = A[t, t^{-1}]$, $\Delta : A[t, t^{-1}] \to A[t, t^{-1}] \otimes A[t, t^{-1}]$ is given by $\Delta(t) = t \otimes t$ and $\Delta(t^{-1}) = t^{-1} \otimes t^{-1}$ while S is given by $S(t) = t^{-1}$ and $S(t^{-1}) = t$ and ϵ is given by $\epsilon(t) = \epsilon(t^{-1}) = 1$.

Example. If $G = \mu_n$, $R = A[t]/(t^n) = A[t, t^{-1}]/(t^n)$, the Hopf algebra structure is induced from that on $A[t, t^{-1}]$, so $\Delta(t) = t \otimes t$, $S(t) = t^{-1} = t^{n-1}$, and $\epsilon(t) = 0$.

Application to constructing Galois representations and abelian extensions: Suppose that $A = K$ is a field, and G is an abelian affine group scheme over K such that the corresponding Hopf algebra A is a finite separable K-algebra. Then $G(K^{\mathrm{sep}}) = \mathrm{Hom}(A, K^{\mathrm{sep}})$ is a finite group, and $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acts on $G(K^{\mathrm{sep}})$ by group automorphisms, so we get a homomorphism $\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(G(K^{\mathrm{sep}}))$, which factors through some injection $\mathrm{Gal}(L/K) \hookrightarrow \mathrm{Aut}(G(K^{\mathrm{sep}}))$.

For example: $G = \mu_n$, where $\operatorname{char} K$ does not divide n. Then $\mu_n(K^{\mathrm{sep}})$ is cyclic of order n, and $\mathrm{Aut}(G(K^{\mathrm{sep}})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. Note that these group schemes μ_n are all subschemes of the group scheme $\mathbb{G}_m$: in particular, μ_n is the kernel of the nth power map, which is an endomorphism of $\mathbb{G}_m$.

We would like to generalize this setup. There are a couple issues. One is that there aren't actually that many abelian affine group schemes over a field. For instance, the only abelian group schemes defined over an algebraically closed field of characteric 0 are isomorphic to products of copies of $\mathbb{G}_m$, $\mathbb{G}_a$ and μ_n. (There are more over a non-algebraically closed field K, but here our program has the potential to get a bit circular, as they are easier to construct if you've already constructed abelian extensions of K. Characteristic p is another story, and an interesting one.)

There are two ways of dealing with this restriction. One is to drop the "affine" condition and look at projective varieties that are also algebraic groups: this gets into the theory of elliptic curves and abelian varieties. This has the advantage that it works over any field K, and we'll mention this in the context of global fields next semester.

The other is to work with complete rings like the ring of power series $\mathcal{O}_K[[x]]$, as we'll do shortly, in the theory of Lubin-Tate formal groups. We'll be able to make $\mathcal{O}_K[[x]]$ into "something like a Hopf algebra", and in fact this will let us construct quotients of $\mathcal{O}_K[[]x]]$ that are honestly finite-dimensional Hopf algebras over $\mathcal{O}_K$, and so give abelian extensions as above.

The second, orthogonal issue with this setup is that $\mathrm{Aut}(G(K^{\mathrm{sep}}))$ is often not an abelian group, and so this process might give us a non-abelian extension. For this reason, we won't be able to take arbitrary elliptic curves or formal groups, but only ones with extra rigidity ("complex multiplication") which forces the image of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ to lie in some commutative subgroup of $\mathrm{Aut}(G(K^{\mathrm{sep}}))$.

18.3 Definition of formal groups

As mentioned above, the goal here is to make to make $\mathcal{O}_K[[X]]$ into "something like a Hopf algebra". Instead of having comultiplication go from $\mathcal{O}_K[[X]]$ to $\mathcal{O}_K[[X]] \otimes \mathcal{O}_K[[X]]$, however, we'll instead ask that our comultiplication be a map

$$\Delta : \mathcal{O}_K[[X]] \to \mathcal{O}_K[[X_1, X_2]].$$

(There is a natural inclusion $\mathcal{O}_K[[X]] \otimes \mathcal{O}_K[[X]] \hookrightarrow \mathcal{O}_K[[X_1, X_2]]$ sending $X \otimes 1 \to X_1$ and $1 \otimes X \to X_2$, but it's not an isomorphism), and furthermore that it be continuous. Here the topology we use on the ring of formal power series $\mathcal{O}_K[[X_1, \dots, X_n]]$ is the one with neighborhood basis at the origin given by $(X_1, \dots, X_n)^k$ for $k \in \mathbb{Z}$. (In particular, this has nothing to do with the topology on $\mathcal{O}_K$.)

The reason for this, is that for any finite extension L/K, $\mathrm{Hom}_{\mathrm{cts}}(\mathcal{O}_K[[X]], L)$ is canonically in bijection with $\pi_L \mathcal{O}_L$, via the map $\phi \mapsto \phi(X)$. Likewise, $\mathrm{Hom}_{\mathrm{cts}}(\mathcal{O}_K[[X, Y]], L)$ is canonically in bijection with $\pi_L \mathcal{O}_L \times \pi_L \mathcal{O}_L$ via the map $\phi \mapsto (\phi(X), \phi(Y))$.

Thus any such Δ allows us to put a group structure on $\pi_L \mathcal{O}_L$. Since the $\mathcal{O}_K$-algebra Δ is topologically generated by X, in order to know Δ we just need to know $F(X_1, X_2) = \Delta(X)$. We can then unpack what the Hopf algebra axioms say: they will be functional equations satisfied by F. This then motivates:

Definition. A one-parameter commutative formal group law 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 $F(X, i_A(X)) = 0$ (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 $a, b \mapsto F(a, b)$.

Example. The Hopf algebra structure on $A[X]$ that gives the additive group scheme can be extended to $A[[X]]$. We get the additive formal group law $F(X, Y) = X + Y$, with $i_F(X) = -X$.

Example. We can also get a formal group law for the multiplicative group, but we have to change variables, since formal groups are required to have 0 as identity. However, we do have an inclusion $A[T, T^{-1}] \hookrightarrow A[[X]]$ given by $T \mapsto 1 + X$ and $T^{-1} \mapsto 1 - X + X^2 - X^3 + X^4 - \cdots$.

This gives a formal group law $F(X, Y) = X + Y + XY$, with inverse map $i_F(X) = -X + X^2 - X^3 + X^4 - \cdots$. This formal group is denoted the *multiplicative formal group* $\hat{\mathbb{G}}_m$.

19 November 2

19.1 More on Formal Groups

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 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 group law 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 to the analogous construction for infinite extensions. E.g. let K^{sep} be the separable closure of K, with ring of integers $\mathcal{O}_{K^{\mathrm{sep}}}$ and maximal ideal $\pi_{K^{\mathrm{sep}}}$ Then define $F(\mathfrak{p}_{K^{\mathrm{sep}}})$ to be $\mathfrak{p}_{K^{\mathrm{sep}}}$ 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 $F(\mathfrak{p}_{K^{\mathrm{sep}}}) \to G(\mathfrak{p}_{K^{\mathrm{sep}}})$.

Example. Let $A = \mathbb{Q}_p$, $F(X, Y) = \hat{\mathbb{G}}_a(X, Y) = X + Y$, $G(X, Y) = \hat{\mathbb{G}}_m(X, Y) = X + Y + XY$.

Then $f(X) = \exp_p(X) - 1$ is an isomorphism $\hat{\mathbb{G}}_m \to \hat{\mathbb{G}}_a$, with inverse $f^{-1}(X) = \log_p(1 + X)$.

However, as formal groups over $\mathbb{Z}_p$, $\hat{\mathbb{G}}_a$ and $\hat{\mathbb{G}}_m$ are not isomorphic. This is because $\hat{\mathbb{G}}_a(\pi_L \mathcal{O}_L) = \pi_L \mathcal{O}_L^+$ is always a torsion-free group for any finite extension L of $\mathbb{Z}_p$, while $\hat{\mathbb{G}}_m(\pi_L \mathcal{O}_L)$ may contain p-torsion. (E.g. if $L = \mathbb{Q}_p(\zeta_p)$, the element $\zeta_p - 1 \in \mathbb{G}_m(\pi_L \mathcal{O}_L)$ is p-torsion.)

Example. Let $A = \mathbb{Z}_p$, $F = G = \hat{\mathbb{G}}_m$, and let

$$h_n(X) = (X+1)^n - 1 = \sum_{k \geq 1} \binom{n}{k} X^k.$$

for $n \in \mathbb{Z}$. Then $h_n \in \operatorname{End}(\hat{\mathbb{G}}_m)$. In fact, h_n makes sense even if $n \in \mathbb{Z}_p$, since we can define write

$$\binom{n}{k} = \frac{n(n-1)\cdots(n-k+1)}{k!} \in \mathbb{Z}_p$$

for any $n \in \mathbb{Z}_p$.

The map $\mathbb{Z}_p \to \operatorname{End}(\hat{\mathbb{G}}_m)$ is a ring homomorphism (in fact an isomorphism as we'll see later). As a consequence, if $n \in \mathcal{O}_p^\times$, then $h_{n^{-1}}(h_n(X)) = X$ and h_n is an isomorphism.

Let F and G be formal groups over $\mathcal{O}_K$, and let $h \in \operatorname{Hom}(F, G)$. Then we can try to make sense of the kernel of h. First we can look at the kernel of the group homomorphism $F(\mathfrak{p}_{K^{\mathrm{sep}}}) \to G(\mathfrak{p}_{K^{\mathrm{sep}}})$. This is

$$\{a \in \mathfrak{p}_{K^{\mathrm{sep}}} \mid h(a) = 0\},$$

that is, the set of solutions of $h(a) = 0$ in $\mathfrak{p}_{K_{\mathrm{sep}}}$. Note that this kernel is acted on by $\operatorname{Gal}(K^{\mathrm{sep}}/K)$.

We can also look at the ring quotient $\mathcal{O}_K[[X]]/h(X)$. In some cases, such as when $h(X)$ is a monic polynomial, this will be a finite $\mathcal{O}_K$-algebra, and then will be a Hopf algebra.

For instance, in the previous example, with $K = \mathbb{Q}_p$, $F = G = \hat{\mathbb{G}}_m$ and $h_p(X) = (X+1)^p - 1$, we have

$$\mathcal{O}_K[[X]]/h_p(X) \cong \mathcal{O}_K[X]/((X+1)^p - 1)$$

which is a Hopf algebra isomorphic to $\mu_p(\mathcal{O}_K)$.

Note though that if $\ell \neq p$, and we consider $h_\ell(X) = (X+1)^\ell - 1$ we have

$$\mathcal{O}_K[[X]]/h_\ell(X) \cong \mathcal{O}_K[X]/X.$$

since $\frac{(X+1)^\ell - 1}{X}$ is a unit in $\mathcal{O}_K[[X]]$ (the constant term is a unit). This is related to the fact that $h_\ell : \mathbb{G}_m(\mathfrak{p}_{\mathbb{Q}_p^{\mathrm{sep}}}) \to \mathbb{G}_m(\mathfrak{p}_{\mathbb{Q}_p^{\mathrm{sep}}})$ is an injection (there are no nontrivial ℓth roots of unity in $1 + \mathfrak{p}_{\mathbb{Q}_p^{\mathrm{sep}}}$.)

19.2 Lubin-Tate formal groups

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 $\operatorname{Gal}(K^{\mathrm{sep}}/K)$, 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, $f(X) = X^p + \pi X$.

Theorem 19.1. *For any $f \in \mathcal{F}_p$ 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 $[a]_f \equiv a \pmod{\deg 2}$. 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 isomorphism of rings.*

Any two Lubin-Tate group laws are isomorphic over $\mathcal{O}_K$.

The following "workhorse lemma" will let us prove everything in the theorem.

Lemma 19.2. *For $f, g \in \mathcal{F}_\pi$, and any linear polynomial $\Phi_1 \in \mathcal{O}_K[X_1, \ldots, X_r]$. the equation*

$$f(\Phi(X_1, \ldots, X_r)) = \Phi(g(X_1), g(X_2), \ldots, g(X_r)))$$

has a unique solution $\Phi \in \mathcal{O}_K[[X_1, \ldots, X_r]]$ such that $\Phi \equiv \Phi_1 \pmod{\deg 2}$.

Proof. We induct on the following statement:

There is a unique Φ_k in $\mathcal{O}_K[[X_1, \ldots X_r]]$ such that

$$f(\Phi_k(X_1, \ldots, X_r)) \equiv \Phi_k(g(X_1), g(X_2), \ldots, g(X_r))) \pmod{\deg k+1}. \tag{11}$$

and $\Phi_k \equiv \Phi_1 \pmod{\deg}2$.

For $k = 1$ we just need to check that Φ_1 satisfies (11): indeed, the linear terms of both sides are $\pi\Phi_1(X_1, \ldots, X_r)$.

Now assume that we have shown that there is a unique $\Phi_k \equiv \Phi_1 \pmod{\deg}2$ of degree k satisfying (11).

Then any Φ_{k+1} with the desired property will have to reduce to Φ_k modulo $\deg k+1$, so can write $\Phi_{k+1} = \Phi_k + Q$, where Q is homogeneous of degree $k+1$.

Have

$$f(\Phi_{k+1}(X_1, \ldots, X_r)) \equiv f(\Phi_k(X_1, \ldots, X_r)) + \pi Q(X_1, \ldots, X_r) \pmod{\deg k+2}$$

because f has linear term πX, and all higher-order terms involving Q have degree $\geq k+2$.

Also

$$\begin{aligned}\Phi_{k+1}(f(X_1), \ldots, F(X_r)) &= \Phi_k(X_1, \ldots, X_r) + Q(f(X_1), \ldots, f(X_r))\\ &\equiv \Phi_k(f(X_1), \ldots, f(X_r)) + Q(\pi X_1, \ldots, \pi X_r) \pmod{\deg k+2}\\ &= \Phi_k(f(X_1), \ldots, f(X_r)) + \pi^{k+1} Q(X_1, \ldots, X_r)\end{aligned}$$

Setting these equal and solving, we get

$$Q(X_1, \ldots, X_r) = \frac{f(\Phi_k(X_1, \ldots, X_r)) - \Phi_{k+1}(f(X_1), \ldots, f(X_r))}{\pi^{r+1} - \pi}.$$

Hence we must show that the numerator is divisible by $\pi^{r+1} - \pi$, or equivalently by π, since $\pi^r - 1$ is a unit.

For this, use the fact that $f(X) \equiv X^q \pmod{\pi}$, so

$$f(\Phi_k(X_1, \dots, X_r)) \equiv \Phi_k(X_1, \dots, X_r)^q \equiv \Phi_k(X_1^q, \dots, X_r^q) \equiv \Phi_k(f(X_1), \dots, f(X_r)) \pmod{\pi}$$

where $\Phi_k(X_1, \dots, X_r)^q \equiv \Phi_k(X_1^q, \dots, X_r^q) \mod \pi$ because the Frobenius map

$$F \mapsto F^q : \mathcal{O}_K/\pi[[X_1, \dots, X_r]] \to \mathcal{O}_K/\pi[[X_1, \dots, X_r]]$$

is an $\mathcal{O}_K/\pi$-algebra homomorphism. □

We now use the lemma to show that there's a unique formal group F_f for which f is an endomorphism. First we apply the 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 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 $F(F(X, Y), Z)$ and $F(X, F(Y, Z))$. Likewise 0 is a left identity because the power series $F(X, 0)$ and X both commute with f, and a right identity for the same reason.

Existence of an inverse follows from the other axioms (as previous 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.

20 November 7

20.1 Lubin-Tate formal groups, continued

For $f, g \in \mathcal{F}_\pi$ define $[a]_{g,f} \in \mathcal{O}_K[[X]]$ to be the unique power series satisfying

$$[a]_{g,f} \circ f = g \circ [a]_{g,f},$$

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 $\mathrm{End}(f)$ 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 $[a^{-1}]_{f,g}$.

This proves Theorem 19.1.

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 $[a]_{F_f} = [a]_f$.

Note that if F is a formal $\mathcal{O}_K$-module, then $F(\mathfrak{p}_{K^{\mathrm{sep}}})$ 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.

20.2 The field $K^{\pi,n}$ generated by π^n-torsion of F_f

Let $E_{f,n}$ the set of $\{x \in \mathfrak{p}_{K^{\mathrm{sep}}} \mid [\pi^n]_f(x) = 0\}$ all π^n torsion of F_f. Then $E_{f,n}$ 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 $E_{f,n}$.

Proposition 20.1. *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.*

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 $E_{f,\pi_n} \to E^{g,\pi^n}$. By definition of $[1]_{g,f}$ this is an isomorphism of $\mathcal{O}_K$-modules, and clearly $[1]_{f,g}$ is the inverse map.

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 20.2. *$E_{f,n}$ 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.

Now we observe that for all $k \geq 1$, $\frac{[\pi]_f^k}{[\pi]_f^{k-1}}$ is an Eisenstein polynomial of degree $q^k - q^{k-1}$, with constant term π. Hence it has exactly $q^k - q^{k-1}$ roots in $\mathfrak{p}_{K^{\mathrm{sep}}}$.

Conclude that $|E_{f,n}| = q^k$. 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 $E_{f,n}$ is equal to $E_{f,1}$, which has order q. It follows that $m = 1$ and $d_1 = n$.

□

Although this isomorphism is not canonical, the isomorphism $\mathrm{Aut}(E_{f,n}) \to (\mathcal{O}_K/(\pi^n\mathcal{O}_K))^\times$ is canonical, and the inverse map is given by $a \mapsto [a]_f$.

Corollary 20.3. $E_f = \bigcup E_{f,n} \cong K/\mathcal{O}_K$. *This isomorphism is not canonical.*

Proof. For each $n \geq 1$, choose $\alpha_n \in E_{f,n}$ such that α_1 generates $E_{f,1}$ and $[\pi]_f\alpha_n = \alpha_{n+1}$. The annihilator in $\mathcal{O}_K$ of α_n is π^n, so α_n generates $E_{f,n}$.

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 20.4. *The map* $\mathrm{Gal}(K^{\pi,n}/K) \to \mathrm{End}_{\mathcal{O}_K}(E_{f,n})$ *is an isomorphism.*

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 the Eisenstein polynomial $\frac{[\pi]_f^n}{[\pi]_f^{n-1}}$. Hence $|\mathrm{Gal}(K^{\pi,n}/K)| = [K^{\pi,n} : K] = q^n - q^{n-1}$.

On the other hand, we already have $|\mathrm{End}_{\mathcal{O}_K}(E_{f,n})| = |\mathcal{O}_K/(\pi^n)|^\times = q^n - q^{n-1}$.

□

Corollary 20.5. *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 ultimately prove that these two constructions give the same field. The first step towards this is:

Proposition 20.6. $\pi \in N_{K^{\pi,n}/K}(K^{\pi,n})^\times$.

Proof. Proof: $N(\alpha_n) = (-1)^{q^n - q^{n-1}}\pi = \pi$ unless q is even and $n = 1$. In that case, $N(-\alpha_n) = -N(\alpha_n) = \pi$. □

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 abiliity to prove this.

20.3 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 $r_\pi(\pi)|K^\pi = \mathrm{id}$.

Goal: $L^\pi = K^{ab}$ and $r_\pi = \theta_{/K}$ is the Artin map.

Strategy: we'll show that L^π and r_π don't depend on our choice of π. Once we know that it won't take much work to show $r_\pi = \theta_{/K}$, and we'll then be able to get $L^\pi = K^{ab}$.

21 November 9

21.1 Characterization of the Artin Map

Theorem 21.1. *Let K be a field. Assume that the field $L = L^\pi = K^{unr}K^\pi$ is independent of the choice of uniformizer π of K.*

If $r : K^\times \to \mathrm{Gal}(L/K)$ is a homomorphism such that

- *the composition*

$$K^\times \xrightarrow{r} \mathrm{Gal}(L/K) \to \mathrm{Gal}(K^{unr}/K)$$

  is given by $a \mapsto \mathrm{Frob}^{v_K(a)}$.

- *For any uniformizer $\pi \in K$, $r(\pi)$ is the identity on K^π.*

  Then $r = \theta_{L/K}$.

Proof. 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

$$r(\pi)|_{K^{unr}} = \mathrm{Frob} = \theta_{L/K}(\pi)|_{K^{unr}}$$

We saw last time that $\pi \in (NK^{\pi,n})^\times$ for any n, so

$$\theta_{L/K}(\pi)|_{K^\pi} = \mathrm{id}|_{K^\pi} = \theta_{L/K}(\pi)|_{K^\pi}$$

and we're done since $L = K^\pi K^{\mathrm{unr}}$. $\square$

Our plan for this and the next lecture is to show that in fact the candidate field $L^\pi = K^\pi K^{\mathrm{unr}}$ is independent of π, and that the candidate reciprocity map $r_\pi : K^\times \to \mathrm{Gal}(L^\pi/K)$ is also independent of π. Then we'll be able to use the theorem above to get $\theta_{L^\pi/K} = r_\pi$.

However, before we do that, we'll derive some consequences from $\theta_{L^\pi/K} = r_\pi$.

First, we can compute the subgroup

$$N(K^{\pi,n})^\times = \ker(\theta_{K^{\pi,n}/K}) = \ker r_\pi : K^\times \to \mathrm{Gal}(K^{\pi,n}/K)$$

For this, let $\pi^r u$ be an arbitrary element of $K^\times$, where $u \in \mathcal{O}_K^\times$. Let f be a Lubin-Tate series, so that $K^{\pi,n} = K(E_{f,n})$ is generated by π^n-torsion of the formal group F_f, and let $x \in E_{f,n}$ be arbitrary. Have

$$r_\pi(\pi^r u)(x) = r_\pi(u)(x) = [u^{-1}]_f(x).$$

Hence $r_\pi(\pi^r u)$ acts on the $\mathcal{O}_K$-module $E_{f,n}$ as multiplication by u^{-1}. Since $E_{f,n} \cong \mathcal{O}_K/\pi^n$ as $\mathcal{O}_K$-modules, $r_\pi(\pi^r u)$ is the identity on $K^{\pi,n}$ if and only if u^{-1} is $1 \pmod{\pi}^n$ if and only if u is $1 \pmod{\pi}^n$.

We conclude that

$$N(K^{\pi,n})^\times = U_n \cdot \pi^{\mathbb{Z}}$$

where $U_n = \{a \in \mathcal{O}_K \pmod{a} \equiv 1 \pmod{\pi^n}\}$.

As a consequence, we obtain

Theorem 21.2. *Any finite abelian extension* L *of* K *is contained in* $K^\pi K^{\mathrm{unr}}$. *Hence* $K^\pi K^{\mathrm{unr}} = K^{\mathrm{ab}}$.

Proof. Look at the group $NL^\times$, which by class field theory we know has finite index in $K^\times$. Hence $NL^\times$ contains π^f for some f. Also, $NL^\times$ is open in $K^\times$, so must contain U_n for some n. Hence

$$\begin{aligned} NL^\times &\supset (U_n \cdot \pi^{\mathbb{Z}}) \cap \{x \in K^\times \mid \nu_K(x) \equiv 0 \pmod{f}\} \\ &= N(K^{\pi,n})^\times \cap N(K^{\mathrm{unr},f})^\times \\ &= N(K^{\pi,n} \cdot K^{\mathrm{unr},f})^\times \end{aligned}$$

where $K^{\mathrm{unr},f}$ is the unique unramified extension of K of degree f. Hence $L \subset K^{\pi,n} \cdot K^{\mathrm{unr},f} \subset K^\pi \cdot K^{\mathrm{unr}}$, as desired. $\square$

21.2 Completions of infinite algebraic extensions of local fields

Now we'll do the groundwork to show that L^π and r_π are independent of π. Let π, ω be uniformizers, and let $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\omega$ be Lubin-Tate series with formal group laws F_f, G_g.

We need a way of relating the formal groups F_f and G_g. However, these formal groups are not isomorphic over $\mathcal{O}_K$: if they were we would have $K^\pi = K^\omega$, which will not be the case. We want to find a larger ring over which F_f and G_g are isomorphic as formal groups: the ring of integers of K^{unr} seems like a possible choice, since we are hoping to show $K^{unr}K^\pi = K^{unr}K^\omega$. Unfortunately, the problem is that K^{unr} is not a complete field (can construct Cauchy sequences that don't converge), so instead we will have to work with the completion $\widehat{K^{unr}}$ and its ring of integers $\widehat{\mathcal{O}^{unr}}$.

We'll now make a couple general comments about completions of local fields. If L is an infinite algebraic extension of K, then L is not complete, but we form take the completion $\hat{L}$.

Example. (Not to be used here, but for general context) $K = \mathbb{Q}_p$, $L = \overline{\mathbb{Q}_p}$, $\hat{L}$ is known as the "p-adic complex numbers" $\mathbb{C}_p$ and is algebraically closed.

If $g \in \mathrm{Gal}(L/K)$, we can extend g by continuity to a unique element $\hat{g} \in \mathrm{Aut}(\hat{L}/K)$ (we don't call this a Galois group, because $\hat{L}$ is a transcendental extension). For example, get Frobenius element $\mathrm{Frob} \in \mathrm{Aut}(O^{\hat{unr}})$. We'll write a^ϕ as shorthand for $\mathrm{Frob}(a)$.

Proposition 21.3. *K is a local field, L/K an algebraic extension, then any $x \in \hat{L}$ which is separable over L must actually lie in L.*

Proof. (Fixed from class.) Let L^{sep} be the separable closure of L, which has a topology coming from the absolute value on L^{sep}. Choose an embedding $L(x)$ into L^{sep}: under this embedding x lies in the topological closure L' of L^{sep}.

So it's enough to show that $L' = L$. For this we use Galois theory. Suppose $g \in \mathrm{Gal}(L^{sep}/L)$. Because g is continuous, g must also fix the closure L'. Hence $\mathrm{Gal}(L^{sep}/L) = \mathrm{Gal}(L^{sep}/L')$. By the Galois correspondence for infinite extensions this gives $L' = L$.

□

21.3 Proof that any two Lubin-Tate group laws are isomorphic over $\mathcal{O}^{\hat{unr}}$

Notation as before: Let π, ω be uniformizers, and let $f \in \mathcal{F}_\pi$ and $g \in \mathcal{F}_\omega$ be Lubin-Tate series with formal group laws F_f, G_g. Also, we use the notation a^ϕ for $\mathrm{Frob}(a)$ (or, if $\alpha = \sum a_n X^n \in \mathcal{O}^{unr}[[X]]$, $\alpha^\phi = \sum a_n^\phi X^n$).

Lemma 21.4. *There exists a power series $\alpha(X) \in \widehat{\mathcal{O}^{unr}}[[X]]$ such that*

a) $\alpha^\phi = \alpha \circ [u]_f$

b) $\alpha^\phi \circ f = g \circ \alpha$.

c) α *is a formal group homomorphism* $F_f \to G_g$ *(*$G_g \circ (\alpha \times \alpha) = \alpha \circ F_f$*)*

d) $\alpha \circ [a]_f = [a]_g \circ \alpha$ *for all* $a \in \mathcal{O}_K$

Proof. (following Milne) By HW, choose $\epsilon \in (\mathcal{O}^{\mathrm{unr}})^\times$ such that $\mathrm{Frob}(\epsilon)/\epsilon = u$.

First show that an α exists with $\mathrm{Frob}(\alpha) = \alpha \circ [u]_f$. Write α^ϕ as shorthand for $\mathrm{Frob}(\alpha)$.

We induct on n, show that there exist polynomials α_n of degree n such that

$$\alpha_n^\phi = \alpha_n \circ [u]_f \pmod{\deg} n+1.$$

For $n = 1$, $\alpha_n(X) = \epsilon X$ works.

Write $\alpha_{n+1} = \alpha_n + cX^{n+1}$.

Then $(\alpha_{n+1})^\phi(X) = \alpha_n^\phi(X) + c^\phi X^{n+1} \pmod{\deg n+2}$.

While $\alpha_{n+1} \circ [u]_f(X) = \alpha_n \circ [u]_f(X) + cu^{n+1}X^{n+1} \pmod{\deg n+2}$

Must then solve equation of form $cu^{n+1} - c^\phi = d$ in $\mathcal{O}^{\mathrm{unr}}$.

Change variables to $c = b\epsilon^{n+1}$ to get $b - b^\phi = d'$, which we know has a solution by HW.

Now, we let $g' = \alpha^\phi \circ f \circ \alpha^{-1} = \alpha \circ [u]_f \circ f \circ \alpha^{-1}$.

First, we note that $g' \in \mathcal{O}_K[[X]]$: for this, enough to show $(g')^\phi = g$.

We have

$$g^\phi = \alpha^\phi \circ [u]_f \circ f \circ (\alpha^\phi)^{-1} = \alpha \circ [u]_f \circ [u]_f \circ f \circ [u]_f^{-1} \circ \alpha^{-1} = \alpha^\phi \circ [u]_f \circ f \circ \alpha^{-1}.$$

also, modulo ω,

$$g^\phi = \alpha^\phi \circ X^q \circ \alpha^{-1} = \alpha^\phi \circ (\alpha^{-1})^q = \alpha^\phi \circ (\alpha^{-1}(X^q))^\phi = X^q.$$

So $g' \in \mathcal{F}_\omega$. Hence there is a power series $[1]_{g,g'}$ with $[1]_{g,g'} \circ g' \circ [1]_{g,g'}^{-1} = g$.

Modify α to $\alpha' = [1]_{g,g'} \circ \alpha$, so $g = (\alpha')^\phi \circ f \circ (\alpha')^{-1}$. Still have $(\alpha')^\phi = (\alpha') \circ [u]_f$ because $[1]_{g,g'}^\phi = 1_{g,g'}$.

So α' satisfies a) and b): by homework this implies c) and d). □

22 November 14

22.1 Proof of Independence of uniformizer

Now we're ready to prove

Theorem 22.1. *For all* π *and* ω, $L^\pi = L^\omega$

Proof. We have previous seem that the power series α is an isomorphism of formal groups $F_f \to G_g$ over $\mathcal{O}^{unr}$. Hence the map $x \mapsto \alpha(x)$ is an isomorphism of the π^n torsion modules $E_{f,n} \to E_{g,n}$, with inverse $x \mapsto \alpha^{-1}(x)$.

It follows that $\widehat{K}^{unr}K^{\pi,n} = \widehat{K}^{unr}K^{\omega,n}$.

Taking the union, get $\widehat{K}^{unr}K^{\omega} = \widehat{K}^{unr}K^{\pi}$. Completing both sides it follows that $\widehat{K^{unr}K^{\omega}} = \widehat{K^{unr}K^{\pi}}$. Taking the separable closure of K in both sides and applying the lemma get $K^{unr}K^{\omega} = K^{unr}K^{\pi}$. □

Proving that the reciprocity map is independent of π is a little more work:

Theorem 22.2. $r_\pi = r_\omega$.

Proof. Need to show that $r_\pi(y) = r_\omega(y)$ for all $y \in K^\times$. Since uniformizers generate $K^\times$, enough to show this when y is a uniformizer.

We already have that $r_\pi(y)|_{K^{unr}} = r_\omega(y)|_{K^{unr}}$. So it's enough to show that $r_\pi(y)|_{K^\omega} = r_\omega(y)|_{K^\omega}$. We'll do this by showing that both are equal to $r_y(y)|_{K^\omega}$.

After relabeling, need to check that

$$r_\pi(\omega)(x) = r_\omega(\omega)(x)$$

for all $x \in E_g$ and all uniformizers π, ω of K. (As usual, write $\pi = u\omega$.

By definition, $r_\omega(\omega)(x) = x$.

Write $x = \alpha(x')$ for $x' \in E_f$. Get

$$r_\pi(\omega)(\alpha(x')) = r_\pi(\omega)(\alpha(x')) = r_\pi(\omega)(\alpha)\left(r_{u\omega}(x')\right) = \alpha^\phi([u^{-1}]_f(x')) = \alpha(x')x.$$

as desired. □

We've now determined that L^π and r_π are independent of choice of π, so by what we did last time, we have $L^\pi = K^{ab}$ and $r_\pi = \theta_{/K}$.

22.2 Artin map and Ramification filtration

We conclude the discussion of Lubin-Tate theory with one application to local fields.

Let L/K be a finite extension. Have surjection $\mathcal{O}_K^\times \to I(L/K)$. Both sides have natural filtrations

$$U_{K,m} = \{u \mid u \equiv 1 \pmod{\pi_K^m}\}$$

and

$$G_i(L/K) = \{g \in G \mid g(\pi_L) \equiv \pi_L \pmod{\pi_L^i}\}$$

for $n \geq 1$.

Want to compare them.

First we do this for the case $L = K^{\pi,n}$, where the reciprocity map $\theta_{L/K}$ induces an isomorphism $\mathcal{O}_K^\times/U_{K,n} \to \mathrm{Gal}(L/K)$ you will show on problem set that

$$G_i(L/K) = \begin{cases} \mathrm{Gal}(L/K) & \text{if } i < 1 \\ \theta_{L/K}(U_{K,m}) & \text{if } q^{m-1} \leq i \leq q^m \text{ and } 1 \leq m \leq n-1 \\ 1 & \text{if } q^{n-1} \leq i. \end{cases} \tag{12}$$

Actually we can combine the last two cases, as $\theta_{L/K}(U_{K,m}) = 1$ if $m \geq n$.

Hence for all $i \geq 1$

$$G_i(K^{\pi,n}/K) = \theta_{K^{\pi,n}/K}(U_{K,m}) \text{ if } q^{m-1} \leq i \leq q^m. \tag{13}$$

Recall there's also an upper numbering filtration: $G^m(L/K)$, defined by

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

where $\phi(x) = \int_0^x \frac{1}{[G_0:G_t]} dt$.

For the case $L = K^{\pi,n}$ we can compute $\phi(q^{m-1}) = m$ for $i = 1, 2, \ldots, n+1$.

Combining this with (13), we get

$$G^m(K^{\pi,n}/K) = \theta_{K^{\pi,n}/K}(U_{K,m}).$$

We can also extend this result to the infinite field K^π. For this, we use the fact (which we haven't proved: see e.g. Neukirch for a proof) that if $E/L/K$ is a tower, $G^m(E/K)$ surjects onto $G^m(L/K)$. Hence, for an infinite extension L/K we may define

$$G^m(L/K) = \varprojlim_{L'} \mathrm{Gal}(L'/K)$$

where L' runs over all finite subextentions of L/K.

We then immediately get

$$G^m(K^\pi/K) = \theta_{K^\pi/K}(U_{K,m}).$$

Hence can define $G^m(K^\pi/K)$ and $G^m(K^{ab}/K)$.

for $L = K^{\pi,n}$ have

$$G^m(L/K) = \theta_{L/K}(U_{K,m}).$$

for all $i \geq 1$.

Hence $G^i(K^\pi/K) = \theta_{K^\pi/K}(U_{K,m})$

Can get that also $G^i(K^{ab}/K) = \theta_{K^\pi/K}(U_{K,m})$: so for any L/K abelian $G^m(L/K) = \theta_{L/K}(U_{K,m})$ for each i.

Note that we have $\mathrm{Gal}(K^\pi/K) \cong \mathcal{O}_K^\times$, so we have in this case $\theta_{K^\pi/K} : U_{K,m} \to G^m(K^\pi/K)$ is an isomorphism.

Now we consider extensions that are not totally ramified, starting with K^{ab}/K. We have

$$\begin{tikzcd}
\mathcal{O}_K^\times \arrow[r, "\theta_{K^{ab}/K}"] \arrow[rrr, bend right, "\theta_{K^\pi/K}"'] & I(K^{ab}/K) \arrow[r] & I(K^\pi/K) \arrow[r, equal] & \mathrm{Gal}(K^\pi/K)
\end{tikzcd}$$

Hence we have $I(K^{ab}/K) \cong I(K^\pi/K)$, and induced isomorphisms $G^m(K^{ab}/K) \cong G^m(K^\pi/K)$. As a result, we have also that also

$$G^m(K^{ab}/K) = \theta_{/K}(U_{K,m}).$$

Applying the surjection $G^m(K^{ab}/K)$ to $G^m(L/K)$ for any abelian extension $\mathrm{Gal}(L/K)$, we get

$$G^m(L/K) = \theta_{L/K}(U_{K,m})$$

in general for any finite extension L/K.

22.3 Introduction to Brauer Group from the point of view of Central Simple Algebras

Take a base field K. We'll be interested in non-commutative algebras over K, e.g. the algebra $M_n(K)$ of $n \times n$ matrices

As another example of a non-commutative algebra, take the $\mathbb{R}$-algebra of Hamilton's quaternions $\mathbb{H} = \mathbb{R}\langle i, j\rangle/(i^2 = j^2 = -1, ij = -ji)$, which is spanned over $\mathbb{R}$ by $1, i, j$ and $k = ij = -ji$. This is a division algebra (every nonzero element has an inverse).

Note that if we try to construct the quaternions over $\mathbb{C}$, would get

$$\mathbb{H}_{\mathbb{C}} = \mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}\langle i, j\rangle/(i^2 = j^2 = -1, ij = -ji)$$

which is isomorphic to $M_2(\mathbb{C})$ via the map

$$i \mapsto \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right), \quad j \mapsto \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right).$$

We can say then that $\mathbb{H}$ is a *twist* or *form* of $M_2(\mathbb{R})$, since $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{R}) \otimes_{\mathbb{R}} (\mathbb{C})$.

Generally, for a field K, we will be interested in *twists* of $M_n(K)$, that is, K-algebras A such that $A \otimes_K K^{sep} \cong M_n(K^{sep})$. One thing we'll see is that these twists are classified by elements of a non-abelian Galois cohomology set (no longer a group!) $H^1(K, PGL_n(K^{sep}))$ which we haven't defined yet. We'll get a connecting homomorphism $H^1(K, PGL_n(K^{sep}) \to H^2(K, (K^{sep})^\times) = \mathrm{Br}(K)$, which explains how the Brauer group comes into things.

There's another class of noncommutative K-algebras that can be defined in an unrelated way, but turns out to give exactly those K-algebras that are twists of $M_n(K)$ for some n. We'll do that now.

Definition. A K-algebra A is *simple* if A has no nonzero proper two-sided ideals. We say that A is a *central simple algebra* over K if A is a simple algebra and the center $Z(A) = K$.

Example. The algebra of $n \times n$ matrices $M_n(K)$ is central simple; we'll do this at the start of next time.

Example. For $a, b \in K^\times$, define a *generalized quaternion algebra* $H(a, b)$ over K by

$$H(a, b) = K\langle i, j\rangle/(i^2 = a, j^2 = b, ij = -ji).$$

As in the case of ordinary quaternions, $H(a, b)$ has basis $1, i, j, k = ij$.

You'll prove on HW that $H(a, b)$ is central simple.

23 November 16

(Reference for all this material is Milne's CFT notes: `http://www.jmilne.org/math/CourseNotes/CFT.pdf`, chapter 4)

23.1 Definition of Brauer Group in terms of Central Simple Algebras

K is a field, A is a K-algebra. Recall:

Definition. A is simple if and only if there are no nontrivial 2-sided ideals of A.

A is central if and only if $Z(A) = K$

Observe that A is simple if every homomorphism from A to a nonzero K-algebra B is injective.

Example. $M_n(K)$ is simple

Proof. Let I be a nonzero 2-sided ideal of $M_n(K)$. Choose $x \in I$ nonzero, so $x_{ij} \neq 0$ for some i, j. By rescaling may assume $x_{ij} = 1$. Then I also contains the matrix $e_{ij} = e_{ii}xe_{jj}$. By multiplying by permutation matrices on both sides, get that I contains e_{kl} for all k, l in range, so $I = M_n(K)$. □

Also $M_n(K)$ is central.

If D is a division algebra over K, then D is simple.

Saw quaternions last time. One more example of a central simple algebra (proofs deferred, probably until problem set.)

Example. $\mathrm{Gal}(L/K)$ cyclic, generator g of order n ($\mathrm{char}\, K \nmid n$), $a \in K^\times$.

Then define A_a to be generated over L by an element γ with relations $\gamma^n = a$, and $\gamma b = (gb)\gamma$ for all $b \in L$. Can show that A_a is n^2-dimensional as a K-vector space.

If $a = 1$ have isomorphism $A \cong \mathrm{End}_K(L)$. The isomorphism sends $b \in L$ to the multiplication-by-b map $m_b \in \mathrm{End}_K(L)$, and sends γ to $g \in \mathrm{End}_K(L)$.

If $a'/a \in NL^\times$ then $A_a \cong A_{a'}$. To show this choose $b \in L^\times$ with $a'/a = Nb$, and take the isomorphism $A_{a'} \to A_a$ that is the identity on L and the generator $\gamma_{a'}$ of $A_{a'}$ to the element $b\gamma_a$ of A_a.

This is central simple, but we won't show it here; we may return later, or put in on the problem set.

Proposition 23.1. *If $A \otimes_K L$ is a simple K-algebra, then so is A.*

Proof. If I is an ideal of A, then $I \otimes_K L$ is an ideal of $A \otimes_K L$. □

The converse is not true, e.g. $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \oplus \mathbb{C}$, is not simple. More generally $L \otimes_K L$.

However, if A is central simple then $A \otimes_K L$ is simple over L. More generally:

Proposition 23.2. *A, B are K-algebras, A central simple, B simple implies $A \otimes_K B$ simple.*

Proof. Let I be an ideal of B and let $\sum_{i=1}^n a_i \otimes b_i$ be a nonzero element of I with n minimal.

The ideal Aa_1A is equal to all of A, so wlog can assume that $a_1 = 1$. Take commutator with arbitrary element $a \otimes 1$, minimality gives that a commutes with a_i for each i. So $a_i \in K$, and get $\sum_{i=1}^n a_i \otimes b_i$ in $K \otimes_K B$ can be written as $1 \otimes b$. Now use that B is simple, to get that I contains $K \otimes_K B$, hence contains $A \otimes_K B$. □

Also, if we let $Z(A)$ denote the center of a K-algebra A,

Proposition 23.3. *Have $Z(A \otimes B) = Z(A) \otimes_K Z(B)$*

Proof. Exercise. □

It follows from the previous two problems that the set of central simple algebras $/K$ forms a monoid under tensor product.

From now on, we are going to require that all central simple algebras over K are finite-dimensional.

The monoid of central simple algebras over K has a submonoid consisting of the matrix algebras $M_n(K)$ for $n \in \mathbb{Z}$. We will define the Brauer group as the quotient of the monoid of central simple algebras over K by the submonoid of matrix algebras. We need to show that this is a group.

Definition. For a K-algebra A, define A^{op} to be the K-algebra which is equal to A as a K-vector space but has the opposite multiplication: $a * b = ba$.

Note that A^{op} is central / simple if and only if A is.

Proposition 23.4. *If A is a central simple algebra of dimension n as a K-vector space, then $A \otimes_K A^{op} \cong \mathrm{End}_K(A) \cong M_n(K)$.*

Proof. We define a homomorphism $\phi : A \otimes_K A^{op} \to \mathrm{End}_K(A)$ as follows.

Let $\phi(a \otimes 1) = \ell_a$, where ℓ_a is the left multiplication map by a: $\ell_a(b) = ab$.

Let $\phi(1 \otimes a) = r_a$, where r_a is the right multiplication map by a: $r_a(b) = ba$.

Because $A \otimes_K A^{op}$ is a central simple algebra, ϕ is injective. However, $\mathrm{End}_K(A) \cong M_n(K)$ and $A \otimes_K A^{op}$ are both K-vector spaces of the same dimension n^2, so ϕ must be an isomorphism. □

Hence we may now give the original definition of the Brauer group:

Definition. The Brauer group $\mathrm{Br}(K)$ is the quotient of the monoid of central simple algebras over K by the monoid of matrix algebras.

We have defined this but we aren't yet ready to compute it in any cases, that will take more theory.

23.2 Classification of Central Simple Algebras

In this section we'll show that any central simple algebra is of the form $M_n(D) = M_n(K) \otimes_K D$ where D is a division algebra with center K.

First we need some facts about modules over non-commutative algebras.

Definition. If M is a (finitely generated) module over a K-algebra A, we say that

- M is *simple* if M has no nonzero proper A-submodules.
- M is *semisimple* if M is the direct sum of simple A-modules.
- M is *indecomposable* if M cannot be written as $M_1 \oplus M_2$ with $M_1, M_2 \neq 0$.

Lemma 23.5. *(Schur) If M is a simple A-module, then $\mathrm{End}_A(M)$ is a division algebra.*

Proof. We need to show that any nonzero $\phi \in \mathrm{End}_A(M)$ is a unit. Note that $\ker \phi$ must equal either 0 or M, but can't be M, so must be 0. Likewise, $\mathrm{im}\, \phi$ is either 0 or M, but can't be 0, so must be M. Hence ϕ is an invertible linear transformation, and $\phi^{-1} \in \mathrm{End}_A(M)$, so ϕ is a unit in $\mathrm{End}_A(M)$. □

Proposition 23.6. *If D is a division algebra, then any f.g. D-module M is isomorphic to D^n for a unique n. Any set of n linearly independent vectors of D^n spans.*

Proof. Same as for D a field. □

For V a K-vector space and A a (*simple*: this was not stated in class) subalgebra of $\mathrm{End}_K(V)$, let $C(A)$ denote the centralizer of A in $\mathrm{End}_K(V)$. Observe that $C(A) = \mathrm{End}_A(V)$.

Theorem 23.7 (Double Centralizer). $C(C(A)) = A$ *in* $\mathrm{End}_K(V)$.

Proof. Skipped: See Milne. □

${}_AA$ denotes A considered as left A-module. Note that $\text{End}_A({}_AA) \cong A^{\text{op}}$, and more generally, if V is a free A-module of rank n, $\text{End}_A(V) \cong M_n(A^{\text{op}})$.

Theorem 23.8. *Any central simple algebra over K is isomorphic to $M_n(D)$ for D a division algebra.*

Proof. Choose a nonzero simple A-module S (eg a minimal nonzero left ideal of A).

Then A embeds in $\text{End}_K(S)$. Let B be the centralizer of A in $\text{End}_K(S)$: B is a division algebra by Schur. Then $A = \text{End}_B(S)$ by the double centralizer theorem. Since B is a division algebra, $S \cong B^n$ for some n, and then $A = \text{End}_B(S) \cong M_n(B^{\text{op}})$ as desired. □

24 November 21

24.1 Classification results for CSAs and modules over CSAs

Last time we showed that any CSA A over K is isomorphic to $M_n(D)$ for some division algebra D with center K. Now we'll show that D, and hence n, are uniquely determined by A, giving a precise classification of central simple algebras.

Note that in our construction of D, there was exactly one choice that we had to make: we had to pick a simple A-module S. We'll now show that there is only one simple A-module up to isomorphism, which will imply that D is uniquely determined by A.

Proposition 24.1. *Let A be a central simple algebra over K (or generally, a simple algebra.)*

Up to isomorphism there's a unique simple module S over A. Every finitely generated A module is semisimple and isomorphic to S^n for some n, so are classified by dimension.

Proof. By classification, $A = M_n(D)$. Then $S = D^n$ is an A-module; easily seen to be simple.

First, we decompose ${}_AA$ (A viewed as a (left) A-module) as a sum of simple A-modules as follows:

$$ {}_AA = \oplus_i S_i, $$

where S_i is the set of all matrices which are 0 outside of the ith row. Each $S_i \cong S$, so is simple.

Now let M be any simple A-module, and $m \in M$ be a nonzero element. Then define a map $\text{ phi} : A \to M$ by $\phi(a) = am$. For some i the restriction $\phi|_{S_i}$ must be nonzero, and since both M and S_i are simple, this implies that ϕ is an isomorphism $S \to M$.

We'll only sketch the proof of the second part: if M is a finite-dimensional A-module, we have a surjection $\phi \cong A^m = S^{mn} \to M$ for some m. By a similar but more involved argument, we can show that we can restrict the domain of ϕ to obtain an isomorphism $S^k \to M$ for some k. □

By the argument before the statement of Proposition 24.1, we can now deduce:

Proposition 24.2. *Any CSA A over K is isomorphic to $M_n(D)$ for some division algebra D. The division algebra D and integer n are uniquely determined by A.*

Corollary 24.3. *There is a bijection between the set of division algebras D with center K and $\mathrm{Br}(K)$ given by sending D to the class $[D]$ of D in the Brauer group.*

Corollary 24.4. $\mathrm{Br}(K) = 0$ *if K is algebraically closed.*

Proof. Follows from the fact that any finite-dimensional division algebra over K is equal to K (if $x \in D$, $K(x)$ is a an algebraic field extension of K, so $x \in K$). □

Wedderburn's theorem says that every finite division algebra is a field: hence $\mathrm{Br}(\mathbb{F}_q) = 0$. (We'll see other ways of proving this later.)

Likewise, the classification of finite-dimensional division algebras over $\mathbb{R}$ gives $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, where the nonzero element is the class $[\mathbb{H}]$ of the quaternions..

24.2 Extension of base field:

If A is a CSA over K, and L/K is any field extension, we've previously seen that $A \otimes_K L$ is a CSA / L. Hence we have a homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(L)$.

Proposition 24.5. *If A is a CSA / K, then $[A : K] = \dim_K A$ is a square.*

Proof. We have $A \otimes_K \overline{K} \cong M_n(K)$ for some n, so $\dim_K A = \dim_{\overline{K}} A \otimes_K \overline{K} = n^2$. □

For L/K any field extension, let $\mathrm{Br}(L/K)$ be the kernel of the natural map $\mathrm{Br}(K) \to \mathrm{Br}(L)$. We say that a CSA A/K is split by L if $A \otimes_K L$ is a matrix algebra: this is equivalent to $[A] \in \mathrm{Br}(K)$.

(One implication of this is clear: for the other direction, we need to check that whether $A \otimes_K L$ is a matrix algebra depends only on $[A] \in \mathrm{Br}(K)$. Write $A = M_n(D)$, where D is a division algebra. If $D \otimes_K L = M_m(D')$, $A \otimes_K L \cong M_n(D \otimes_K L) \cong M_{mn}(D')$, which is a matrix algebra if and only if $D' = K$. This condition depends only on D, so depends only on the class $[A] \in \mathrm{Br}(K)$.)

Proposition 24.6. $\mathrm{Br}(K) = \bigcup_{L/K \textit{ finite}} \mathrm{Br}(L/K)$

Proof. Let $A \in \mathrm{Br}(K)$ be arbitrary. We already know that we have an isomorphism $\phi : M_n(\overline{K}) \to A \otimes_K \overline{K}$. Take L large enough that $\phi(e_{ij})$ lies in $A \otimes_K L$: then ϕ restricts to an isomorphism $M_n(L) \to A \otimes_K L$. □

Our goal now is to to show that for L/K Galois, $\mathrm{Br}(L/K) \cong H^2(L/K, L^\times)$.

24.3 Maximal Subfields of CSAs

First we'll ask a more basic question: if A is a CSA over K, how to tell which extensions L of K split A?

Example. $K = \mathbb{Q}$, $A = H(-1,-1)$ is the quaternion algebra with generators i, j, k and relations $i^2 = j^2 = k^2 = -1$ and $ij = -ji = k$.

Then for any extension L of $\mathbb{Q}$, the algebra $A \otimes_{\mathbb{Q}} L = H_L(-1,-1)$ is a quaternion algebra over L. By your last HW, A is split by L if and only if either one of the following two equivalent conditions holds:

- $x^2 + y^2 + z^2 = 0$ has a nonzero solution in L^3.
- $x^2 + y^2 + z^2 + w^2 = 0$ has a nonzero solution in L^4

Consider the case where $L = \mathbb{Q}(\sqrt{D})$ is a quadratic extension of $\mathbb{Q}$, D a squarefree integer. First of all, if $D > 0$, then L embeds in $\mathbb{R}$: since the quadratic forms above are positive definite, we conclude that A is not split by L.

If D is congruent to $1 \pmod 8$, then $\mathbb{Q}(\sqrt{D})$ embeds in $\mathbb{Q}_2$. Again, we can check that the quadratic form $x^2 + y^2 + z^2 = 0$ has only trivial solutions in $\mathbb{Q}_2$ (WLOG $x, y, z \in \mathbb{Z}_2$ are relatively prime, and work mod 4), so it has no solutions in $\mathbb{Q}(\sqrt{D})$.

In any other case, we can use Legendre's three squares theorem to write $-D = a^2 + b^2 + c^2$, for $a, b, c \in \mathbb{Z}$ and then $(a, b, c, \sqrt{D})$ is a solution to $x^2 + y^2 + z^2 + w^2 = 0$, so A is split by L.

In short, $\mathbb{Q}(\sqrt{D})$ splits A iff D is positive and $1 \pmod 8$ iff $-D$ is the sum of three rational cubes.

Another equivalent condition is the following: $\mathbb{Q}(\sqrt{D})$ embeds in A. To see this, note that if $a = w + xi + yj + zk$, $w, x, y, z \in \mathbb{Q}$, is an arbitrary element of A, $a^2 = D$ iff $w = 0$ and $x^2 + y^2 + z^2 = -D$. This condition is one we'll be able to generalize.

First we need the following algebraic fact, which we will state without proof:

Theorem 24.7. *Double centralizer theorem for central simple algebras: if A is a CSA, $B \subset A$ simple, and $C = C(B)$, then C is simple, $B = C(C)$ and $[A : K] = [B : K][C : K]$. (As with field extensions, $[A : K]$ denotes the dimension of A as a K-vector space.)*

Proof. (See Milne) □

Corollary 24.8. *If $Z(B) = K$ then $Z(C) = K$ and $A \cong B \otimes_K C$.*

Proof. For the first part, $Z(B) = B \cap C = Z(C)$. For the second part, since both B and C are central simple over K, so is $B \otimes_K C$, and the natural map $B \otimes_K C \to A$ must be injective. By dimension counting it's an isomorphism. □

Corollary 24.9. *For A a CSA/K and $L \subset A$ a field. TFAE:*

a) $\mathsf{L} = \mathsf{C}(\mathsf{L})$

b) $[\mathsf{L} : \mathsf{K}]^2 = [\mathsf{A} : \mathsf{K}]$

c) L *is a maximal commutative* K*-subalgebra.*

d) L *is a maximal commutative subfield*

Proof. a) implies b) by double centralizer. b)implies c) : if L' is a comm K-subalg of A, then $[\mathsf{L}' : \mathsf{K}]^2 \leq [\mathsf{L}' : \mathsf{K}][\mathsf{C}(\mathsf{L}') : \mathsf{K}] = [\mathsf{A} : \mathsf{K}] = [\mathsf{L} : \mathsf{K}]^2$, so $[\mathsf{L}' : \mathsf{K}] \leq [\mathsf{L} : \mathsf{K}]$, hence L is maximal. c) implies a) : if $x \in \mathsf{C}(\mathsf{L}) \setminus \mathsf{L}$ then $\mathsf{L}[x]$ is commutative. □

Corollary 24.10. *If* D *is a division algebra, the maximal commutative subfields of* D *all have dimension* $[\mathsf{L} : \mathsf{K}] = \sqrt{[\mathsf{D} : \mathsf{K}]}$.

Proposition 24.11. L *splits* A *if and only if there is an algebra* $\mathsf{B} \sim \mathsf{A}$ *containing a subfield isomorphic to* L *such that* $[\mathsf{B} : \mathsf{K}] = [\mathsf{L} : \mathsf{K}]^2$.

(done correctly in next lecture)

25 November 28

25.1 Condition for L to Split A

Last time we were proving:

Proposition 25.1. L *splits* A *if and only if there is an algebra* $\mathsf{B} \sim \mathsf{A}$ *containing a subfield isomorphic to* L *such that* $[\mathsf{B} : \mathsf{K}] = [\mathsf{L} : \mathsf{K}]^2$.

Let's correct the proof of the ⇒ direction, and give a proof of ⇐:

Proof. ⇒: L splits A, so also A^{op}, so $\mathsf{A}^{\mathrm{op}} \otimes_{\mathsf{K}} \mathsf{L} \cong \mathrm{End}_{\mathsf{L}}(\mathsf{V})$ for some L-vector space V with $\dim_{\mathsf{L}}(\mathsf{V}) = \sqrt{[\mathsf{A} : \mathsf{K}]}$.

Take B to be the centralizer of A^{op} in $\mathrm{End}_{\mathsf{K}}(\mathsf{V})$. By Corollary 24.8 we have $\mathsf{B} \otimes \mathsf{A}^{\mathrm{op}} \cong \mathrm{End}_{\mathsf{K}}(\mathsf{V})$, so $[\mathsf{B}] = [\mathsf{A}]$ in $\mathrm{Br}(\mathsf{K})$. Also, $1 \otimes \mathsf{L} \subset \mathsf{B}$ since $\mathsf{A}^{\mathrm{op}} \otimes 1$ commutes with $1 \otimes \mathsf{L}$. Finally,

$$[\mathsf{B} : \mathsf{K}] = \frac{[\mathrm{End}_{\mathsf{K}}(\mathsf{V}) : \mathsf{K}]}{[\mathsf{A}^{\mathrm{op}} : \mathsf{K}]} = \frac{\dim_{\mathsf{K}}(\mathsf{V})^2}{[\mathsf{A} : \mathsf{K}]} = [\mathsf{L} : \mathsf{K}]^2 \frac{\dim_{\mathsf{L}}(\mathsf{V})^2}{[\mathsf{A} : \mathsf{K}]} = [\mathsf{L} : \mathsf{K}]^2.$$

For other direction, enough to show that L splits B. Say $[\mathsf{L} : \mathsf{K}] = n$ so $[\mathsf{B} : \mathsf{K}] = [\mathsf{L} : \mathsf{K}]^2$. We need a vector space V such that $\mathsf{B} \otimes_{\mathsf{K}} \mathsf{L} \cong \mathrm{End}_{\mathsf{L}}(\mathsf{V})$: since $\mathsf{B} \otimes_{\mathsf{K}} \mathsf{L}$ is of dimension n^2 over L, we need V to be an n-dimesional L-vector space.

The obvious choice is $\mathsf{V} = \mathsf{B}$: however, since B is non-commutative, we'll take the L-vector space structure on B to have L acting by right multiplication. (Alternatively we could take $V = B^{op}$ with L acting by left multiplication, but this will be notationally simpler.)

Then we can map $B \otimes_K L \to \mathrm{End}_L(V)$ by $b \otimes 1 \mapsto \ell_b$ (where ℓ_b is the left multiplication by B map) and $1 \otimes \ell \mapsto r_\ell$ (where r_ℓ is left multiplication by ℓ.) This map is an injection because $B \otimes_K L$ is simple, and is surjective by dimension count.

□

Corollary 25.2. *Suppose* $[L : K] = \sqrt{[D : K]}$. *Then* L *splits* D *iff* L *embeds in* D*; that is, all maximal subfields of* D *split* D.

25.2 Noether-Skolem

Theorem 25.3 (Noether-Skolem). *If* A, B *are* K*-algebras,* A *simple,* B *central simple, then any two homs* $f, g : A \to B$ *are conjugate: related by* $g = bfb^{-1}$.

Example. $K = \mathbb{R}$, $f, g : \mathbb{C} \to \mathbb{H}$ given by $f(i) = i$, $g(i) = j$, take $b = \frac{1}{\sqrt{2}}(1 + k)$, $b^{-1} = \frac{1}{\sqrt{2}}(1 - k)$,

$$bib^{-1} = \frac{1}{2}(1 + k)i(1 - k) = \frac{1}{2}(i + ki - ik - kik) = j.$$

We give the important corollaries first.

Corollary 25.4. *If* A *is a simple algebra, all automorphisms of* A *are inner.*

Corollary 25.5. *If* A *is a central simple algebra over* K*, and* L *is a field, then any two embeddings* $i_1, i_2 : L \hookrightarrow A$ *are conjugate to each other by some element of* A *(*$i_2 = ai_1a^{-1}$ *for some* $a \in A$*).*

Proof. We case of $B = M_n(K)$ first. We put two different two A-module structures on K^n exetending the K-vector space structure.

Let $M_1 = K^n$ with A-module structure $a *_1 v = f(a)v$, and let $M_2 = K^n$ with A-module structure $a *_2 v = g(a)v$.

Since A-modules are classified by dimension, there is an A-module isomorphism $\phi : M_1 \to M_2$. Since ϕ is a K-linear map, it can be viewed as a matrix $\phi \in M_n(K)$.

Then $\phi(f(a)v) = g(a)(\phi v)$ for all $v \in K^n$, so $\phi f(a) = g(a)\phi \in M_n(K)$, hence f and g are conjugate as desired.

Now let B be a general central simple algebra over K. We use the fact $B \otimes B^{op}$ is a matrix algebra, and apply the first part to get that $f \otimes 1$ is conjugate to $g \otimes 1$ in $B \otimes K^{op}$. That is, there is some $x \in B \otimes B^{op}$ with

$$x(f(a) \otimes b')x^{-1} = (g(a) \otimes b')$$

for all $b' \in B^{op}$. In particular, setting $a = 1$ get that x commutes with $1 \otimes B^{op}$: implies that $x = b \otimes 1$ for some $b \in B$. This b has the desired property. □

25.3 Bijection between Central Simple Algebras and Cocycles

Suppose L/K Galois, and $G = \mathrm{Gal}(L/K)$.

Then

Definition. $\mathcal{A}(L/K)$ is the set of CSAs A of degree $[L:K]^2$ split by L

By Proposition 24.11, the map $\mathcal{A}(L/K) \to \mathrm{Br}(L/K)$ that sends $A \mapsto [A]$ is a bijection.

We'll now put $\mathcal{A}_{L/K}$ in bijection with $H^2(L/K, L^\times)$.

Recall that $H^2(L/K, L^\times)$ can be described using inhomogeneous cocycles as $Z^2(G, L^\times)/B^2(G, L^\times)$, where

$$Z^2(G, L^\times) = \{\phi : G \times G \to L^\times \mid g_1\phi(g_2, g_3) \cdot \phi(g_1, g_2g_3) = \phi(g_1g_2, g_3) \cdot \phi(g_1, g_2)\}$$

$$B^2(G, L^\times) = \{\phi : G \times G \to L^\times \mid \phi(g_1, g_2) = \frac{g_1\psi(g_2) \cdot \psi(g_1)}{\psi(g_1g_2)} \text{ for some } \psi : G \to L^\times\}.$$

We first describe the map $\mathcal{A}(L/K) \to H^2(G, L^\times)$.

Suppose $A \in \mathcal{A}(L/K)$, and fix an embedding $i : L \hookrightarrow A$ (by Noether-Skolem, i is unique up to inner automorphisms with A.) Identify L with $i(L) \subset A$.

Take any $g \in \mathrm{Gal}(L/K)$. By Noether-Skolem applied to $i, i \otimes g : L \to A$ there exists $a_g \in A^\times$ such that $g(x) = a_g x a_g^{-1}$ for all $x \in L$. Here a_g is well defined up to left multiplication by elements of $C(L) = L$, since if

$$g(x) = a_g x a_g^{-1} = b_g x b_g^{-1}$$

for all $x \in L$ we have that $a_g b_g^{-1}$ commutes with $g(x)$ for all $x \in L$.

(Alternatively, a_g is well-defined up to right multiplication by elements of $C(L) = L$, since $a_g^{-1} b_g$ commutes with all $x \in L$. But these come down to the same thing since $a_g \ell = g(\ell) a_g$ for all $ell \in L$.)

Now note that for $g, h \in G$ $(a_g a_h) x (a_g a_h)^{-1} = g(h(x))$, so $a_g a_h$ must equal $\phi(g, h)$ for some $\phi(g, h) \in L$.

This $\phi = \phi_A$ will give our desired cohomology class in $H^2(G, L^\times)$. To check that ϕ is a cocycle, expand$(a_{g_1} a_{g_2}) a_{g_3} = a_{g_1}(a_{g_2} a_{g_3})$ and cancel the unit $a_{g_1 g_2 g_3}$ from both sides.

Now, the elements a_g are only defined up to multiplication by elements of L. If we choose a different set of elements $a'_g = \psi(g) a_g$, then the new cocyle ϕ' is given by

$$\phi'(g, h) = \frac{\psi(g, h)}{\psi(g) \cdot g\psi(h)} \phi(g, h)$$

so represents the same class in $H^2(G, L^\times)$.

We now give the inverse map.

Let $[\phi] \in H^2(G, L^\times)$ be arbitrary represented by a cocycle ϕ.

Definition. $A_\phi = \oplus_{g \in G} L e_g$, where the multiplication structure is determined by $e_g x = g(\ell) e_g$ for all $g \in G$, $x \in L$ and $e_g e_h = \phi(g, h) e_{gh}$.

The multiplicative identity 1 in A_ϕ is given by $\frac{e_1}{\phi(1,1)}$, and so we have a canonically embedded copy of L inside A given by $Le_1 = L \cdot 1$.

(One can choose the representative cocycle ϕ so that $\phi(1, 1) = 1$, and then e_1 is the identity.)

It follows from the cocycle conditions that A is an associative K-algebra. Also $[A : K] = |G|[L : K] = [L : K]^2$.

Proposition 25.6. *A_ϕ is central simple over* K.

Proof. Central: If $a \in Z(A)$ then a commutes with L so $a \in L = Le_1$, but also a commutes with all e_g so a is in the fixed field of $\mathrm{Gal}(L/K)$ namely K.

Simple: Let I be a nonzero proper ideal of A. Take an element $a = c_1 e_{g_k} + \cdots + c_n e_{g_k} \in I$ with $c_1, \ldots, c_k \in L$, k minimal. WLOG $g_1 = 1$. Since I is not all of A, $k \geq 2$

Take $x \in L$ such that $g_2(x) \neq x$. Then $xa - ax \in I$ but

$$xa - ax = (xc_1 - c_1 x)e_1 + (xc_2 - c_2 g_2(x))e_{g_2} + \cdots = (x - g_2(x))c_2(x)e_{g_2} + \cdots$$

contradicts minimality of k. □

We've now defined maps $A \to \phi_A : \mathcal{A}(L/K) \to H^2(G, L^\times)$, and $\phi \to A_\phi : H^2(G, L^\times) \to \mathcal{A}(L/K)$. It's clear that $\phi_{A_\phi} = \phi$, since we can take $a_g = e_g$. The other direction is only slightly harder. If $\phi = \phi_A$, then there's a natural homomorphism $A_\phi \to A$ sending L to L and e_g to a_g. This homomorphism is injective because A is central simple, and is surjective by dimension count.

Hence we've established a bijection $\mathcal{A}(L/K) \to H^2(G, L^\times)$, and have already established a bijection $\mathrm{Br}(L/K) \to \mathcal{A}(L/K)$, so composing the two gives a bijection $\mathrm{Br}(L/K) \to H^2(G, L^\times)$.

26 November 30

26.1 Conclusion from Last time

Let L/K be a finite Galois extension of arbitrary fields. Last time we gave a bijection $\mathrm{Br}(L/K) \leftrightarrow H^2(L/K, L^\times)$. One can show that this bijection is indeed a group homomorphism ($A_\phi \otimes_K A_{\phi'} \cong A_{\phi+\phi'} \otimes M_n(K)$), but we won't do it here.

As well, the following diagrams commute (though we won't check them either)

$$\begin{tikzcd}
\mathrm{Br}(L/K) \arrow[r, hook] \arrow[d, "\sim"] & \mathrm{Br}(E/K) \arrow[d, "\sim"] \\
H^2(L/K, K^\times) \arrow[r, "\mathrm{inf}"] & H^2(E/K, E^\times)
\end{tikzcd}$$

where $E \subset L$ is a field with E/K finite Galois.

and

$$\begin{tikzcd}
\mathrm{Br}(L/K) \arrow[r, "A \mapsto A \otimes_K L"] \arrow[d, "\sim"] & \mathrm{Br}(E/K) \arrow[d, "\sim"] \\
H^2(L/K, K^\times) \arrow[r, "\mathrm{Res}"] & H^2(E/K, E^\times)
\end{tikzcd}$$

where M is any intermediate field.

As a consequence of the first diagram above we get an isomorphism

$$\mathrm{Br}(K) = \bigcup_{L/K} \mathrm{Br}(L/K) = \varinjlim_{L} \mathrm{Br}(L/K) = \varinjlim_{L} H^2(L/K, L^\times) = H^2(K, (K^{\mathrm{sep}})^\times)$$

(where L runs through all finite Galois extensions of K), justifying the terminology $\mathrm{Br}(K)$ used previously in this class.

Corollary 26.1. *If* $[L : K] = n$, $\mathrm{Br}(L/K)$ *is an* n*-torsion group.* $\mathrm{Br}(K)$ *is a torsion group.*

26.2 Examples of fields with trivial Brauer groups:

We've previously seen that $\mathrm{Br}(K) = 0$ if K is algebraically closed or if K is finite. (We know how to prove these both on the CSA side and on the Galois cohomology side!)

We'll now develop a tool for studying division algebras that will let us show that a wider range of fields have trivial Brauer group.

Let A be a central algebra over K with $[A : K] = n^2$. Let L be any field that splits A, and pick an L-algebra isomorphism $\phi : A \otimes_K L \to M_n(L)$. (By Noether-Skolem, ϕ is unique up to conjugation.)

Then, define

$$\mathrm{Nrd}(a) = \det(\phi(a \otimes 1)).$$

A priori, $\mathrm{Nrd}(a) \in L^\times$.

However, we claim

Claim: $\mathrm{Nrd}(a)$ is fixed by $\mathrm{Gal}(L/K)$, hence lies in $K^\times$.

Proof. For $g \in \mathrm{Gal}(L/K)$ be arbitrary. By Skolem Noether: the two L-algebra maps $\phi, \phi' : A \otimes_K L \to M_n(L)$ given by $\phi'(a \otimes x) = g\phi(a \otimes g^{-1})x$ are conjugate. Taking determinants of both sides, $\det \phi(a \otimes 1) = g \det(\phi a \otimes 1)$, as desired. □

Now suppose that $A = D$ is a division algebra. Because Nrd is multiplicative, it maps $D^\times \to K^\times$: in other words, it is a function on D which is only zero at $d = 0$.

However, Nrd is a polynomial function, in the sense that if $v_1, \dots, v_{n^2}$ form a basis for D, then

$$\mathrm{Nrd}(\sum_i x_i v_i) \in K[x_1, \dots, x_{n^2}]$$

is a homogeneous polynomial of degree n. So we have a polynomial in $K[x_1, \dots, x_{n^2}]$, homogeneous of degree only n, with no roots in $K^n \setminus 0$. There are a number of fields over which this is impossible.

Definition. K is quasi-algebraically closed (QAC) if any homogeneous degree d polynomial $f \in K[x_1, \dots, x_N]$ with $d < N$ has a nonzero solution in K^n.

We now automatically get

Theorem 26.2. *If K is QAC, then $\mathrm{Br}(K) = H^2(K, (K^{\mathrm{sep}})^\times) = 0$*

Proof. By the above discussion, if D is a division algebra over K with $[D : K] = n^2$, we must have $n^2 \leq n$, so $n = 1$ and $D = K$. □

Example. If K is algebraically closed then K is QAC.

Example. If $K = \mathbb{F}_q$ is a finite field, then the *Chevalley-Warning theorem* says K is QAC. More specifically, it shows that the number of solutions of f in K^n is a multiple of p, where $p = \operatorname{char} K$, and therefore 0 cannot be the only solution. The proof is a matter of evaluating $\sum_{\nu \in \mathbb{F}_q^n} (1 - f(\nu)^{q-1})$ in two different ways.

Example. Tsen's theorem: $\mathbb{C}[t]$ is quasi-algebraically closed. (More generally, function fields in one variable over $\mathbb{C}$.

Example. (Lang: any complete DVR with alg closed residue field, eg, $\mathbb{C}[[t]]$ or the completion $\widehat{K^{\mathrm{unr}}}$ of the maximal unramified extension of a local field.

Example. The maximal unramified extension K^{unr} of a local field is also itself quasi-algebraically closed.

Also:

Theorem 26.3 (Lang)**.** *If K is QAC, then any finite extension of K is also QAC.*

One consequence of Lang's theorem plus the fact that the Brauer group of any QAC field is trivial is the following: If K is QAC, then for any $L/K'/K$ $H^1(L/K', L^\times) = H^2(L/K', L^\times) = 0$. It follows (by an old HW), that all $\hat{H}^i(L/K', L^\times) = 0$. In particular, for any finite extension L/K, every element of K is a norm from L.

26.3 Brauer Groups of Local Fields

First we deal with archimedean local fields. $\mathrm{Br}(\mathbb{C}) = 0$ because $\mathbb{C}$ is algebraically closed. For $\mathbb{R}$ we can compute via cohomology: $\mathrm{Br}(\mathbb{R}) = H^2(\mathbb{R}, \mathbb{C}^\times) \cong \hat{H}^0(\mathbb{R}, \mathbb{C}^\times) = \mathbb{R}^\times / N\mathbb{C}^\times$ is cyclic of order 2.

If K is an archimedean local field: we have already constructed an isomorphism $\mathrm{inv} : \mathrm{Br}(K) \cong H^2(K, (K^{\mathrm{sep}})^\times \to \mathbb{Q}/\mathbb{Z}$.

We also know that if L/K has degree n, the following diagram commutes

$$\begin{tikzcd}
\mathrm{Br}(K) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}"] & \mathrm{Br}(L) \arrow[d, "\mathrm{inv}"] \\
\mathbb{Q}/\mathbb{Z} \arrow[r, "\times n"] & \mathbb{Q}/\mathbb{Z}.
\end{tikzcd}$$

Hence if $x \in \mathrm{Br}(K)$ has $\mathrm{inv}(x) \in \frac{1}{n}\mathbb{Z}$, then x is split by any extension L with $[L : K] = n$. In particular, x is split by the unramified extension K_n of K of degree n. Now, K_n/K is cyclic, so any element of $\mathrm{Br}(K_n/K)$ is of the form A_a for some $a \in K^\times/NL^\times$ (see problem 2 on current problem set).

However, there's also a way of seeing all this from the point of view of central simple algebras.

Let D be central division algebra over K with $[D : K] = n^2$. Let L be a maximal subfield, so L splits D.

We can extend the absolute value $||_K$ on to D, in a similar manner to how we extend absolute value to field extensions. Define $|a|_D = |\mathrm{Nrd}(a)|_K^{\frac{1}{n}}$. This is certainly multiplicative, and a similar argument to the commutative case shows that it is a non-archimedean absolute value. (First check that it is a non-archimedean absolute value when restricted to any subfield of D.)

Likewise we can extend the valuation $v = v_K : K^\times \to \mathbb{Z}$ to a valuation $v : D^\times \to \frac{1}{n}\mathbb{Z}$ by $v(a) = \frac{1}{n}v(\mathrm{Nrd}(a))$. We can define a ramification index $e = e_{D/K}$ to be the index of $v(D^\times)$ in $v(K^\times) = \mathbb{Z}$. Note that e must divide n.

Also, we say that a *uniformizer* of D is an $\pi_D \in D^\times$ with the smallest positive absolute value (namely $1/e$.)

(For once I am breaking with my convention that valuations always have integer values. There's a reason for this which you'll see later when we define $\mathrm{inv}([D])$.)

We can then define a "ring of integers" (often called an "order" because of non-commutativity)

$$\mathcal{O}_D = \{x \in D \mid v(x) \geq 0\}$$

which has a maximal two-sided ideal

$$\mathfrak{p}_D = \{x \in D \mid v(x) > 0\}.$$

Here $\mathfrak{p}_D = \pi_D\mathcal{O}_D = \mathcal{O}_D\pi_D$ for any uniformizer π_D. Extend $v : K^\times \to \mathbb{Z}$ to $v : D^\times \to 1/n\mathbb{Z}$.

Then $\mathcal{O}_D/\mathfrak{p}_D$ is a division algebra over $\mathcal{O}_K/\mathfrak{p}_K = \mathbb{F}_q$, so it must be a field. Any primitive element $\bar{a}$ of $\mathcal{O}_D/\mathfrak{p}_D$ lifts to an element $a \in \mathcal{O}_D$, and $[K(a) : K] \geq f$. Since the maximal subfields of L all have degree n over K, we conclde that $f \leq n$.

Exactly the same argument as in the commutative case shows that $ef = [D : K] = n^2$. But we've bounded both e and f above by n! So $e = n$, $f = n$.

In particular, the subfield $K(a) \subset D$ is unramified of degree n, so $K_n \cong K(a)$ embeds in D.

Now, there exists some element $b \in D^{\times}$ such that $bxb^{-1} = \mathrm{Frob}(x)$ for all $x \in b$. The element b is defined up to left multiplication by elements of K_n, so the image of $\nu(b)$ in $\mathbb{Q}/\mathbb{Z}$ is well defined. We define $\mathrm{inv}_K([D]) = \nu(b) \pmod{\mathbb{Z}}$.

26.4 Global Fields

If K is a Global field, the Brauer group of K is also known. The important theorem is

Theorem 26.4 (Albert-Brauer-Hasse Noether)**.** *There exists a short exact sequence $0 \to \mathrm{Br}(K) \mapsto \oplus_\nu \mathrm{Br}(K_\nu) \to \mathbb{Q}/\mathbb{Z} \to 0$.*

Proof will follow from what we do next semester.

Example. $K = \mathbb{Q}$, $A = H(a, b)$ is a quaternion algebra. Then ABHN says that $H(a, b)$ is non-split at an even number of places e.g. $\prod_\nu (a, b)_\nu$ is 1. And conversely, given an set S of places with even cardinality, we can produce a quaternion algebra that it split exactly at those places (this is a little stronger than ABHN).

Specialize to case of $a = p, b = q$ positive primes. Then $\prod_\nu (p, q)_\nu = 1$. $(p, q)_\infty = 1$, also $(p, q)_p$ is $\left(\frac{q}{p}\right)$, and $(p, q)_q$ is $\left(\frac{p}{q}\right)$, and $(p, q)_2 = (-1)^{(p-1)(q-1)/2}$. Hence in this case we get quadratic reciprocity again!