Math 223a - Algebraic Number Theory

Taught by Alison Beth Miller
Notes by Dongryul Kim

Fall 2017

This course was taught by Alison Beth Miller. The lectures were on Tuesdays and Thursdays at 11:30–1, and the main textbook was *Algebraic number theory* by Cassels and Frölich. There were weekly problem sets and a final paper, and there were 15 students enrolled. The course assistant was Lin Chen. Lecture notes can be found online on the course website.

Contents

1 August 31, 2017 **4**
1.1 Historic perspective: class fields 4
1.2 Frobenius elements 5
1.3 Infinite field extensions and their Galois groups 5

2 September 5, 2017 **7**
2.1 Overview of global class field theory 7
2.2 Overview of local class field theory 8
2.3 Local field: evaluations 9
2.4 Completion 10

3 September 7, 2017 **11**
3.1 Hensel's lemma 11
3.2 Extending absolute values 13

4 September 12, 2017 **14**
4.1 Ramification and inertia 14
4.2 Extending absolute values II 14
4.3 Local fields 16

5 September 14, 2017 **17**
5.1 Multiplicative group of local fields 17
5.2 Exponential and logarithm 18
5.3 Unramified extensions 19

6 September 19, 2017 **21**
6.1 Artin map for unramified extensions 22
6.2 Decomposition group 23
6.3 Inertia group 24

7 September 21, 2017 **25**
7.1 Totally ramified extensions of local fields 25
7.2 Ramification groups 26
7.3 Tamely ramified extensions 27

8 September 26, 2017 **29**
8.1 Category of G-modules 29

9 September 28, 2017 **33**
9.1 Group cohomology 33
9.2 Standard bar resolution 34

10 October 3, 2017 **36**
10.1 Explicit descriptions of cohomology 36
10.2 The first cohomology and torsors 37
10.3 Group homology 39

11 October 5, 2017 **40**
11.1 Changing the group 41
11.2 Inflation-restriction exact sequence 42

12 October 10, 2017 **44**
12.1 Tate cohomology 44
12.2 Restriction and corestriction 46

13 October 12, 2017 **48**
13.1 Cup products 48
13.2 Galois cohomology 49
13.3 Cohomology of profinite groups 50

14 October 17, 2017 **52**
14.1 Kummer theory 52
14.2 Second Galois cohomology of unramified extensions 53
14.3 Some diagrams 54

15 October 19, 2017 **56**
15.1 Second Galois cohomology of finite extensions 56
15.2 Estimating the size 57
15.3 Brauer group of a local field 58
15.4 Tate's theorem 59

16 October 24, 2017 **61**
16.1 Reciprocity map 62
16.2 Group of universal norms 64

17 October 26, 2017 **65**
17.1 Normic subgroups 65
17.2 Quadratic reciprocity 66
17.3 Reciprocity map on units 68

18 October 31, 2017 **69**
18.1 Affine group schemes 69
18.2 Formal groups 71

19 November 2, 2017 **73**
19.1 Morphisms between formal groups 73
19.2 Lubin–Tate theory 74

20 November 7, 2017 **76**
20.1 Torsion points in a formal group 76
20.2 Field obtained by adjoining torsion points 78

21 November 9, 2017 **80**
21.1 Characterization of the Artin map 80
21.2 Independence on the uniformizers 81

22 November 14, 2017 **83**
22.1 Artin map and the ramification filtration 84
22.2 Brauer group and central simple algebras 86

23 November 16, 2017 **87**
23.1 Tensor product of central simple algebras 88
23.2 Structure theorem for central simple algebras 89

24 November 21, 2017 **91**
24.1 Modules over simple algebras 91
24.2 Extension of base fields 92

25 November 28, 2017 **95**
25.1 Noether–Skolem theorem 95
25.2 Classification of central simple algebras 96

26 November 30, 2017 **98**
26.1 Fields with trivial Brauer group 98
26.2 Brauer groups of local fields 100

1 August 31, 2017

In 223a we will be studying local class field theory and in 223b global class field theory. For local class field theory, we are going to be proving stuff about $\mathbb{Q}_p$ and their finite extensions. There is another local field, $\mathbb{F}_p((t))$, which may be more comfortable depending on your background. The main tool we will use to analyze these is Galois cohomology.

An example of a global field is $\mathbb{Q}$, and we will of course look at their finite extensions, which are also called number fields. The polynomials $\mathbb{F}_p(t)$ is also a global field. The rings $\mathbb{Z}$ or $\mathbb{F}_p[t]$ have many prime ideals, while $\mathbb{Z}_p$ and $\mathbb{F}_p[[t]]$ have few primes.

The textbook we are going to use is Cassels–Fröhlich, which is actually a set of conference notes. This also includes Tate's thesis. The book has a few errors and there is an errata online. Other recommended books are Neukirch's *Algebraic Number Theory* and *Class Field Theory*.

1.1 Historic perspective: class fields

Suppose we have a finite Galois extension $L/\mathbb{Q}$. In $\mathbb{Q}$ there is a natural ring $\mathbb{Z}$ and in L there is also a natural ring $\mathcal{O}_L$. One thing people were interested in was to take (p), lift it to $p\mathcal{O}_L$, and see how this ideal factorizes. In the case of a Galois extension, this becomes

$$p\mathcal{O}_l = \mathfrak{p}_1^e \cdots \mathfrak{p}_r^e$$

and $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the set $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$.

One thing you should know is that $e = 1$ except for finitely many p. (These are called ramified primes.) For p unramified, the data of r is called the "splitting type of p".

Example 1.1. Suppose $L = \mathbb{Q}[\sqrt{n}]$ is quadratic. There can be two splitting types, and either $p\mathcal{O}_L = \mathfrak{p}_1$ or $p\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. How can you tell which case you are in?

For simplicity assume that $n \not\equiv 1 \pmod 4$. We are trying to check whether $p\mathbb{Z}[\sqrt{n}]$ is prime in $\mathbb{Z}[\sqrt{n}]$, or equivalently, whether $(\mathbb{Z}/p)[\sqrt{n}]$ is an integral domain. Quadratic reciprocity then tells us that this only depends on p modulo $4n$.

Definition 1.2. A Galois number field $L/\mathbb{Q}$ is a **class field** if there exists on N such that the splitting type of p depends only on p modulo N.

For example, quadratic extensions are class fields, but general cubic extensions are not. If $\mathcal{O}_L = \mathbb{Z}[\alpha]$, where the minimal polynomial of α is $f(x)$, then the splitting type of p in L is given by the number of irreducible factors of f in $(\mathbb{Z}/p\mathbb{Z})[x]$.

Example 1.3. If $L = \mathbb{Q}(\zeta_n)$, then $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$ so the splitting type is related to the factorization of $\Phi_n(x)$ over $\mathbb{Z}/p\mathbb{Z}$. You can use this to show that this is a class field.

Here is the big main theorem people proved in class field theory over $\mathbb{Q}$.

Theorem 1.4. *The following are equivalent for a Galois extension $L/\mathbb{Q}$:*

- *L is a class field.*
- *$L/\mathbb{Q}$ is abelian.*
- *L is contained in some $\mathbb{Q}(\zeta_n)$.*

The equivalence of the second and third is also called the Kronecker–Weber theorem. The reason this is not the end of the story is that we want to generalize this to general number fields or function fields.

1.2 Frobenius elements

We want to build something called an Artin map over $\mathbb{Q}$. Return to $p\mathcal{O}_L = \mathfrak{p}_1 \cdots \mathfrak{p}_r$ for an unramified prime p, and let $\mathfrak{p} = \mathfrak{p}_1$. We define the **decomposition group**

$$D_{\mathfrak{p}} = \text{stabilzer of } \mathfrak{p} \subseteq \mathrm{Gal}(L/\mathbb{Q}).$$

By transitivity of the action, we will know $|D_{\mathfrak{p}}| = [L : \mathbb{Q}]/r$.

Let $\ell = \mathcal{O}_L/\mathfrak{p}$ be the finite extension of $\mathbb{Z}/p$. We have a homomorphism

$$\varphi : D_{\mathfrak{p}} \to \mathrm{Gal}(\ell/\mathbb{F}_p)$$

Theorem 1.5. *The map φ is injective if and only if p is unframified. The map φ is always surjective.*

Note that $\mathrm{Gal}(\ell/\mathbb{F}_p)$ is always cyclic and so is generated by $F : a \mapsto a^p$. So F has a unique lift to a **Frobenius element** $\mathrm{Frob}_{\mathfrak{p}} \in D_{\mathfrak{p}}$. If I had chosen some other $\mathfrak{p}' = g\mathfrak{p}$ for $g \in \mathrm{Gal}(L/\mathbb{Q})$, then $\mathrm{Frob}_{\mathfrak{p}'} = g \,\mathrm{Frob}_{\mathfrak{p}}\, g^{-1}$. This means that Frob is well-defined a conjugacy class. In particular, if $L/\mathbb{Q}$ is abelian, we can just write $\mathrm{Frob}_p \in \mathrm{Gal}(L/\mathbb{Q})$.

Example 1.6. Let $L = \mathbb{Q}(\zeta_n)$ and $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$. Take any $p \in \mathbb{Z}$ that is unramified (in this case, relatively prime to $2n$). There is an isomorphism

$$\mathrm{Gal}(L/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})^\times; \quad g \mapsto a \text{ such that } g(\zeta_n) = \zeta_n^a.$$

Now there is going to be a Frobenius element $\mathrm{Frob}_{\mathfrak{p}}(\zeta) \equiv \zeta^p \pmod{\mathfrak{p}}$. Then it has to be $\mathrm{Frob}_{\mathfrak{p}} = p \in (\mathbb{Z}/n\mathbb{Z})^\times$.

1.3 Infinite field extensions and their Galois groups

We can state the Kronecker–Weber theorem in an alternative form as

$$\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}[\zeta_\infty] = \bigcup_{n \geq 1} \mathbb{Q}[\zeta_n].$$

Here, $\mathbb{Q}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathbb{Q}$.

We can try to look at the Galois group $\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$, which is an infinite group. But these are related to finite Galois groups by restriction maps

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

So we can understand this group by considering the map

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \hookrightarrow \prod_n \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Injectivity comes from the fact that $\mathbb{Q}(\zeta_n)$ fills $\mathbb{Q}^{\mathrm{ab}}$. But this is not surjective because $g_n \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ has to restrict to $g_{n'} \in \mathrm{Gal}(\mathbb{Q}(\zeta_{n'})/\mathbb{Q})$ if $n' \mid n$. So this Galois group is the inverse limit

$$\mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q}) \cong \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times \cong \hat{\mathbb{Z}}^\times,$$

where $\hat{\mathbb{Z}} = \varprojlim_n (\mathbb{Z}/n\mathbb{Z})$. Actually these are topological groups and topological rings, but we'll get there.

Definition 1.7. The ***p*-adic integers** $\mathbb{Z}_p$ is defined as

$$\mathbb{Z}_p = \varprojlim_i (\mathbb{Z}/p^i\mathbb{Z}).$$

These are sort of like infinite series $c_0 + c_1 p + c_2 p^2 + \cdots$. The following proposition follows from the Chinese remainder theorem.

Proposition 1.8. $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$.

Thus

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

This is not true for other general fields. So we are going to define a crazy ring called the **adele ring**. This is

$$\mathbb{A}_{\mathbb{Q},\mathrm{fin}} = \left\{ (a_p) \in \prod_p \mathbb{Q}_p : \text{all but finitely many } a_p \text{ are in } \mathbb{Z}_p \right\}, \quad \mathbb{A}_{\mathbb{Q}} = \mathbb{A}_{\mathbb{Q},\mathrm{fin}} \times \mathbb{R}.$$

We can extend the isomorphism to

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

This is called the **Artin map**.

2 September 5, 2017

2.1 Overview of global class field theory

At the end of last class, we computed the Galois group of the maximal abelian extension of $\mathbb{Q}$:

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

Here

$$\mathbb{A}_{\mathbb{Q}} = \{(x_p)_p, (x_\infty) : x_p \in \mathbb{Z}_p \text{ for all but finitely } p\}.$$

The group $\mathbb{A}_{\mathbb{Q}}^\times$ is actually a topological group, with basis

$$\prod_{p_1,\dots,p_r} U_{p_i} \times \prod_{\text{all other } p} \mathbb{Z}_p^\times \times U_{\mathbb{R}},$$

where $U_{p_i} \subseteq \mathbb{Q}_{p_i}^\times$ and $U_{\mathbb{R}} \subseteq \mathbb{R}^\times$ are open sets. The fact that $\theta : \mathbb{A}_{\mathbb{Q}}^\times \to \mathrm{Gal}(\mathbb{Q}^{\mathrm{ab}}/\mathbb{Q})$ contains $\mathbb{Q}^\times$ in the kernel is called Artin reciprocity, and implies quadratic reciprocity.

For K a number field and a prime $\mathfrak{p} \subseteq \mathcal{O}_K$, there is the completion $K_{\mathfrak{p}}$. In general, we define

$$\begin{aligned}\mathbb{A}_{K,\mathrm{fin}}^\times &= \{(x_{\mathfrak{p}}) \in \prod_{\mathfrak{p}} K_{\mathfrak{p}}^\times : x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^\times \text{ for all but finitely } \mathfrak{p}\},\\ \mathbb{A}_{K,\mathrm{inf}}^\times &= \prod_{K\hookrightarrow\mathbb{R}} \mathbb{R}^\times \times \prod_{K\hookrightarrow\mathbb{C}} \mathbb{C}^\times,\\ \mathbb{A}_K^\times &= \mathbb{A}_{K,\mathrm{fin}}^\times \times \mathbb{A}_{K,\mathrm{inf}}^\times.\end{aligned}$$

Again, you can prove that

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \mathbb{A}_K^\times / K^\times \cdot (\mathbb{A}_K)_0,$$

where $(\mathbb{A}_K)_0$ is the connected component of the identity, and the connected component of 1 of $\prod \mathbb{R}^{>0} \times \prod \mathbb{C}^\times$. This isomorphism is the main theorem of global class field theory. If we define the **adelic class group** as $C_k = \mathbb{A}_K^\times/K^\times$, then this is also isomorphic to $C_K/(C_K)_0$.

For finite extensions L/K, there is a reciprocity map

$$\theta_{L/K} : C_K/NC_L \xrightarrow{\cong} \mathrm{Gal}(L/K),$$

where NC_L is the norm of C_L. Then finite abelian extensions L/K corresponds to open finite index subgroups of C_K, with L mapping to NC_L.

So in global class field theory, we are going to construct the Artin map $\theta : \mathbb{A}_K \to \mathrm{Gal}(L/K)$. Then we will show Artin reciprocity, and show the map is surjective. At the end of the semester, we are going to know how to construct the Artin map.

2.2 Overview of local class field theory

Let K be a local field, e.g., $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$. Then there exists a local Artin map

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

This is not an isomorphism, but it is very close to; it is an injection with dense image. As with the global case, if L/K is a finite abelian extension,

$$\theta_{L/K} : K^\times/NL^\times \xrightarrow{\cong} \mathrm{Gal}(L/K)$$

is now an isomorphism. So again we have the correspondence between finite abelian extensions L/K and finite index subgroups of $K^\times$, which is given by $LN^\times$.

Suppose K is a number field, and take a prime $\mathfrak{p} \subseteq \mathcal{O}_K$. Then $K_\mathfrak{p}$ is a local field and so we have the local Artin map

$$\theta_{K_\mathfrak{p}} : K_\mathfrak{p}^\times \to \mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ab}}/K_\mathfrak{p}).$$

On the other hand, we have the global Artin map

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

If L/K is abelian, then we pick a prime $\mathfrak{p}' \subseteq L$ lying over $\mathfrak{p}$, and then $L_{\mathfrak{p}'}/K_\mathfrak{p}$ is an extension and we get a map

$$\mathrm{Gal}(L_{\mathfrak{p}'}/K_\mathfrak{p}) \hookrightarrow \mathrm{Gal}(L/K),$$

which is actually an isomorphism onto the decomposition group $D_{\mathfrak{p}'}$. Putting these together, we get an injection

$$\mathrm{Gal}(K_\mathfrak{p}^{\mathrm{ab}}/K_\mathfrak{p}) \hookrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K),$$

where the image is a decomposition group.

As we hope, the diagram

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

commutes. Because $K_\mathfrak{p}^\times$ generates $\mathbb{A}_K^\times$ topologically, we will be able to use this to construct θ_K.

In this course, we will cover

- basics of local fields
- ramification
- Galois cohomology
- proofs of local class field theory
- Lubi–Tate theory (explicit local class field theory)
- the Brauer group
- applications to global class field theory

2.3 Local field: evaluations

Now I want to do this from scratch. The motivation is that I want to generalize $\mathbb{Q}_p$, $\mathbb{F}_p((t))$. So we want to give a definition of local fields so that all local fields are finite extensions of $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$.

Definition 2.1. A **valuation** on a field K is a map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that

(a) $v(0) = \infty$,

(b) $v : K^\times \to \mathbb{Z}$ is a group homomorphism,

(c) $v(x + y) \geq \min(v(x), v(y))$.

Example 2.2. On $\mathbb{Q}$, define $v_p(x)$ as the power of p in the prime factorization of x. This is valuation.

Example 2.3. Let $\mathcal{O}$ be a Dedekind domain, i.e., an integral domain with unique factorization of ideals. For $\mathfrak{p}$ a prime ideal, define $v_\mathfrak{p}(x)$ to be the power of p in the prime factorization of (x) as a fractional ideal.

Definition 2.4. An **absolute value** on K is a map $|-| : K \to \mathbb{R}^{\geq 0}$ such that

(a) $|0| = 0$,

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

(c) $|x + y| \leq |x| + |y|$.

If v is a valuation, then $|x|_v = a^{v(x)}$ for $a < 1$ is an absolute value. This in fact satisfies

(c′) $|x + y| \leq \max(|x|, |y|)$.

These are called **non-archemedian absolute values**.

Note that any embedding $i : K \hookrightarrow \mathbb{R}$ or $i : K \hookrightarrow \mathbb{C}$ will give an absolute value $|x| = |i(x)|$. The nice thing that happens is that it is possible to classify all absolute values.

Theorem 2.5 (Ostrowski). *Any absolute value of $\mathbb{Q}$ is equivalent to $|-|_p$ for some p or to $|-|_\mathbb{R}$ coming from the embedding $\mathbb{Q} \hookrightarrow \mathbb{R}$.*

Here, we say that $|-|_1 \sim |-|_2$ if $|-|_1 = |-|_2^a$ for some $a \in \mathbb{R}^{>0}$.

Sketch of proof. If $|-|_1$ is an absolute value, consider the set

$$\{x \in \mathbb{Z} : |x| < 1\},$$

which turns out to be a prime ideal. Either it is (0), in which case the valuation is $|-|_\mathbb{R}$, or (p), in which case the valuation is equivalent to $|-|_p$. □

Example 2.6. Consider $\mathbb{F}_p(t)$. Here there are choices for the ring of integers in this field, but I'm arbitrarily going to pick $\mathcal{O} = \mathbb{F}_p[t]$. Now every prime ideal $\mathcal{O}$ gives a valuation, and also $f(t) \mapsto -\deg(f(t))$ is another valuation. There is an analogue Ostrowski's theorem, which says that these are all the valuations, and you can exponentiate them to get all absolute values.

Definition 2.7. A **discrete valuation ring**, or DVR for short, is a local PID that is not a field.

If v is a (surjective) valuation of K, the set

$$\mathcal{O}_v = \{x \in K : v(x) \geq 0\}$$

is a discrete valuation ring with maximal ideal $\mathfrak{p}_v = \{x \in k : v(x) \geq 1\} = (\pi)$ for any π with $v(\pi) = 1$. Conversely, if $\mathcal{O}$ is a discrete valuation ring with maximal ideal $\mathfrak{p}$, then $v_{\mathfrak{p}}$ on $K = \operatorname{Frac}(\mathcal{O})$ is going to give $\mathcal{O}$.

2.4 Completion

If K is a field with absolute value $|-|$, then define the **completion** $\hat{K}$ as the topological completion of K as a metric space. (If $|-|$ comes from a valuation v, then we write this as K_v.) Then $\hat{K}$ is a complete topological field.

Definition 2.8. A **place** of K is an equivalence class of absolute values of K: "finite places" come from valuations and "infinite places" come from embeddings into $\mathbb{R}$ or $\mathbb{C}$. We use the notation v for a place, and then write K_v for the completion at the place v.

Using this, we can formally define

$$\mathbb{A}_K = \left\{ (x_v) \in \prod_{v \text{ places}} K_v : (x_v) \in \mathcal{O}_v^\times \text{ for all but finite } v \right\}.$$

3 September 7, 2017

We finished by talking about absolute values and valuations, and making the field complete. Now we are going to talk about fields that are complete.

First let us talk about non-archemedian absolute values, i.e., absolute values with

$$|x+y| \leq \max\{|x|,|y|\}.$$

Theorem 3.1. *If K is complete with respect to an archemedian absolute value, then $K \cong \mathbb{R}$ or $K \cong \mathbb{C}$.*

Now let's assume that K is a field complete with respect to a discrete absolute value, that is, $\operatorname{im}|-|$ is a discrete subgroup of $\mathbb{R}^{>0}$. Because of the previous theorem, $|-|$ is non-archemedian, and this must come from exponentiating a valuation. That is, $|x| = c^{-v(x)}$ for some $c > 1$.

Now the subring

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

is a DVR, and it is both open and closed in K. The maximal ideal is

$$\mathfrak{p} = \pi\mathcal{O} = \{a \in K : |a| < 1\},$$

and we can cover $\mathcal{O}$ by cosets of $\mathfrak{p}$. We can do the same thing inside the cosets of $\mathfrak{p}$, and write $\mathfrak{p}$ as the disjoint union $\mathfrak{p} + a = \coprod_b(\mathfrak{p}^2 + b)$. The upshot of this is that

$$\mathcal{O} = \varprojlim_n \mathcal{O}/\mathfrak{p}^n\mathcal{O} = \varprojlim_n \mathcal{O}/\pi^n\mathcal{O},$$

by completeness of K.

Generally, let $\mathcal{O}$ be any Dedekind domain, $\mathfrak{p} \subseteq \mathcal{O}$ be a prime. Let $K = \operatorname{Frac}\mathcal{O}$ and $\hat{K}$ be the completion with respect to $v_{\mathfrak{p}}$. If $\hat{\mathcal{O}}$ and $\hat{\mathfrak{p}}$ are the completed ring and prime ideal, then $\mathcal{O}/\mathfrak{p}^i \cong \hat{\mathcal{O}}/\hat{\mathfrak{p}}^i$. We can thus write

$$\hat{\mathcal{O}} = \varprojlim \hat{\mathcal{O}}/\hat{\mathfrak{p}}^i = \varprojlim \hat{\mathcal{O}}/\mathfrak{p}^i.$$

3.1 Hensel's lemma

Let K be complete with respect to a discrete absolute value, and L/K be a finite extension. Is it always possible to extend $|-|_K$ to L? Is it unique, and does this make L complete? The answer to all three questions is yes.

Lemma 3.2 (Hensel)**.** *Let $\mathcal{O}$ be a complete DVR with prime $\mathfrak{p} = (\pi)$ and $k = \mathcal{O}/\mathfrak{p}$. Suppose $f \in \mathcal{O}[x]$ and let $\bar{f} \in k[x]$ be the reduction. If $\bar{f}$ factors as $\bar{f} = \bar{g}\bar{h}$, with $\bar{g}$ and $\bar{h}$ relatively prime, then there exists a factorization $f = gh$ such that g reduces to $\bar{g}$ and h reduces to $\bar{h}$.*

Without the relatively prime condition, a counterexample is $x^2 - p$ in $\mathbb{Q}_p[x]$.

Proof. The idea is to use $\mathcal{O} = \varprojlim \mathcal{O}/\pi^r$. It suffices to find $g_r, h_r \in (\mathcal{O}/\pi^r)[x]$ such that $g_r h_r = f \pmod{\pi^r}$, and $g_{r'}$ reduces to g_r for $r' > r$. Actually we also need degree conditions $\deg g_r = d_g = \deg \bar{g}$ and $\deg h_r \leq d_h = \deg f - \deg \bar{g}$, because the degree might blow up.

We induct on r. If $r = 1$, we can just take $\bar{g} = g_1$ and $\bar{h} = h_1$. Assume we have $g_r, h_r \in (\mathcal{O}/\pi^r)[x]$ which works. Choose arbitrary lifts g'_{r+1} and h'_{r+1}. We want to correct this by writing

$$g_{r+1} = g'_{r+1} + \pi^r a, \quad h_{r+1} = h'_{r+1} + \pi^r b.$$

Then what we need is

$$a h'_{r+1} + b g'_{r+1} = \frac{g'_{r+1} h'_{r+1} - f}{\pi^r} \pmod{\pi}.$$

We are now working in $k[x]$, and we are trying to solve

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

for some $c \in k[x]$. This we can do by linear algebra. Let P_m be the space of polynomials of degree at most m in $k[x]$. Then the map

$$P_{d_g} \times P_{d_h} \to P_{d_g + d_h} = P_{\deg f}; \quad (a, b) \mapsto a\bar{h} + b\bar{g}.$$

The kernel is generated by $(\bar{g}, -\bar{h})$, and so has dimension 1. This shows that the map is surjective. □

As an exercise, try to show that the polynomials g and h are unique up to multiplication by elements of $\mathcal{O}^\times$.

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

Proof. Use Hensel's lemma on $\bar{f} = (x - a)\bar{g}$. □

Example 3.4. Let $K = \mathbb{Q}_p$ and $\mathcal{O} = \mathbb{Z}_p$. Take $f(x) = x^{p-1} - 1$ so that $\bar{f}(x) = (x-1)\cdots(x-p+1)$. Then $x^{p-1} - 1$ has $p - 1$ roots in $\mathbb{Z}_p^\times$, and these are distinct mod p.

Example 3.5. Let $K = \mathbb{Q}_p$ and $\mathcal{O} = \mathbb{Z}_p$ with p odd. Take $f(x) = x^2 - a$ where $a \in \mathbb{Z}_p^\times$. If a is not a square mod p, then $f(x)$ is irreducible, and if a is a square mod p, then $f(x)$ has two distinct solutions. Therefore, $a \in \mathbb{Z}_p^\times$ is a square if and only if $\bar{a}$ is square in $\mathbb{F}_p$.

More generally, if $a \in \mathbb{Q}_p^\times$ and $a = p^i u$ where $u \in \mathbb{Z}_p^\times$, a is a square if and only if i is even and $\bar{u}$ is a square in $\mathbb{F}_p$.

Lemma 3.6. *Let K be a field complete with respect to a valuation v. If $f = a_n x^n + \cdots + a_0 x^0 \in K[x]$ is irreducible, then* $\min_{0 \leq i \leq n} v(a_i) = \min(v(a_n), v(a_0))$.

Proof. By rescaling, we may assume that $\min_{0\leq i\leq n} v(a_i) = 0$ so that $f \in \mathcal{O}[x]$.

Let m be the maximal number with $v(a_m) = 0$, so that $\deg \bar{f} = m$. Apply Hensel to the factorization $\bar{f} = \bar{f} \cdot 1$, so that we have a factorization of f into a degree m and a degree $n - m$ polynomial. Then $m = 0$ or $m = n$. □

This generalizes to the theory of Newton polygons. Here you apply the theorem to stuff like $f(\pi^k x)$.

3.2 Extending absolute values

Theorem 3.7. *Let K be a field complete respect to a discrete absolute valuation $|-|_K$. If L/K is finite with $[L : K] = n$, then there exists a unique extension of $|-|_K$ to an absolute value $|-|_L$, given by*

$$|a|_L = \sqrt[n]{|N_{L/K}a|_K}.$$

Furthermore, L is complete with respect to $|a|_L$.

Before I prove this I want to say a couple of things about norms. Here we are not assuming L/K is Galois, so we can't just multiply the Galois conjugates.

Definition 3.8. If L/K is a finite extension, $a \in L$, then $N_{L/K} = \det_K(m_a : L \to L)$.

In practice, what you use is

Proposition 3.9. *If a has minimal polynomial $x^m+c_{m-1}x^{m-1}+\cdots+c_0 \in K[x]$, then $\chi_{m_a} = f(x)^{n/m}$ and $N_{L/K}(a) = c_0^{n/m}$.*

Proof of Theorem 3.7. We first check that $|a+b|_L \leq \max\{|a|_L + |b|_L\}$. Without loss of generality, let max $= |a|_L = 1$. It suffices to show that $|b|_L \leq 1$ implies $|1 + b|_L \leq 1$.

Let $f(x) = x^m + c_{m-1}x^{m-1} + \cdots + c_0 \in \mathcal{O}[x]$ be the minimal polynomial of b. Then $|c_0| = |b|^m \leq 1$, and the previous lemma implies $|c_i| \leq 1$ for all i. Then $f(x) \in \mathcal{O}[x]$, and so the minimal polynomial of $b + 1$ is also in $\mathcal{O}[x]$. That is, $N_{L/K}(b + 1) \in \mathcal{O}$ and $|b + 1|_L \leq 1$.

We now have to check uniqueness and completeness. Suppose I have $|-|_L$ and $|-|'_L$. We can view them as a norms on L as a finite-dimensional vector space K. It is a theorem that any two such norms induce the same topology. Then $|a|_L < 1$ if and only if $\{a^n\} \to 0$ in $|-|_L$ if and only if $\{a^n\} \to 0$ in $|-|'_L$ if and only if $|a|'_L < 1$.

For completeness, we can again use the fact that any norm induce the same topology. Take the max norm on $L \cong K^n$. This topological space is complete, and so L is complete with respect to $|-|_L$. □

4 September 12, 2017

We've just shown that every absolute value extends to an absolute value on a finite extension. Assume that L/K is a finite extension K is complete with respect to $|-|$. We have shown there exists a unique extension of $|-|$ to L, and that L is complete with respect to $|-|$.

4.1 Ramification and inertia

Now let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the discrete valuation rings, with prime ideals $\mathfrak{p}_K = (\pi_K) \subseteq \mathcal{O}_K$ and $\mathfrak{p}_L = (\pi_L) \subseteq \mathcal{O}_L$. Now $\pi_K \mathcal{O}_L \subseteq \mathcal{O}_L$ is an ideal, and it has to be

$$\pi_K \mathcal{O}_L = (\pi_L)^e$$

for some e. This e is called the **ramification index**. This is the index of

$$\operatorname{im}(|-| : K^\times \to \mathbb{R}^{>0}) \subseteq \operatorname{im}(|-| : L^\times \to \mathbb{R}^{>0}),$$

because the images are generated by $|\pi_K|$ and $|\pi_L|$. We can also define the **inertia degree** as

$$f = f_{L/K} = [\mathcal{O}_L/(\pi_L) : \mathcal{O}_K/(\pi_K)].$$

Example 4.1. Let p be odd and $K = \mathbb{Q}_q$. Consider the extension $\mathbb{Q}_p[\sqrt{u}]$ where $u \in \mathbb{Z}_p^\times$ is not a square mod p. Here it is clear that $e = 1$ and $f = 2$, since $p = \pi_K = \pi_L$ and so $\ell = \mathbb{F}_p[\sqrt{u}]$.

Example 4.2. Let p be odd and $K = \mathbb{Q}_q$. Consider the extension $L = \mathbb{Q}_p(\sqrt{p})$, $\mathcal{O}_L = \mathbb{Z}_p[\sqrt{p}]$. Here $\pi_L = \sqrt{p}$ and so $e = 2$. But $\ell = \mathbb{F}_p$ and so $f = 1$.

Theorem 4.3. *If L/K is as above, then $e_{L/K} f_{L/K} = [L : K] = n$.*

Proof. The quotient $\mathcal{O}_L/\pi_K\mathcal{O}_L$ is a vector space over $k = \mathcal{O}_K/\pi_K\mathcal{O}_K$, and we compute its dimension in two different ways.

Firstly, $\mathcal{O}_L$ is a free $\mathcal{O}_K$-module and is of rank $[L : K] = n$. So $\mathcal{O}_L/\pi_K\mathcal{O}_L$ is a free k-module of rank $[L : K]$, and hence $\dim_k \mathcal{O}_L/\pi_K = n$.

Secondly, we have $\pi_K\mathcal{O}_L = \pi_L^e\mathcal{O}_L$ and so

$$\dim_k \mathcal{O}_L/\pi^e\mathcal{O}_L = \dim_k \mathcal{O}_L/\pi_L\mathcal{O}_L + \dim_k \pi_L\mathcal{O}_L/\pi_L^2\mathcal{O}_L + \cdots = e \dim_k \ell = ef.$$

This shows that $n = ef$. □

4.2 Extending absolute values II

Let K be a field with usual discrete non-archemedian absolute value $|-|_K$. But let us not assume that K is complete. Now suppose that L/K is finite. How many ways can we $|-|_K$ extended to $|-|_L$?

Consider the case $K = \operatorname{Frac}\mathcal{O}_K$ where $\mathcal{O}_K$ is a Dedekind domain. Assume that $|-|_K = |-|_\mathfrak{p}$ for some $\mathfrak{p} \subseteq \mathcal{O}_K$. One way of extending $|-|_\mathfrak{p}$ to L is to factor

$\mathfrak{p} \subseteq \mathcal{O}_L$. (Here $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$ in L, and is thus Dedekind.) Let $\mathfrak{p}' \subseteq \mathcal{O}_L$ be a factor of $\mathfrak{p}\mathcal{O}_L$ with exponent e. Then for each $a \in K$, we have

$$v_{\mathfrak{p}'}(a) = ev_{\mathfrak{p}}(a).$$

After appropriate normalization, $|-|_{\mathfrak{p}'}$ extends $|-|_{\mathfrak{p}}$.

Theorem 4.4. *Any absolute value $|-|'$ of L extending $|-|_{\mathfrak{p}}$ is equivalent to $|-|_{\mathfrak{p}'}$ for some $\mathfrak{p}' \mid \mathfrak{p}$.*

Proof. First we will show that $|-|$ is discrete. Look at the completions $\hat{K}$ and $\hat{L}$, where the both valuations will be discrete. This implies that $|-|'$ is discrete and non-archemedian.

Consider

$$\mathcal{O}_{L,v'} = \{a \in L : |a|' \leq 1\}$$

which is a DVR. This ring contains $\mathcal{O}_K$ and so contains $\mathcal{O}_L$. Let

$$\mathfrak{p}' = \mathfrak{p}_{L,v'} \cap \mathcal{O}_L,$$

which is a prime ideal.

Inside L we have $(\mathcal{O}_L)_{\mathfrak{p}'} \subseteq \mathcal{O}_{L,v'}$, both DVRs. But if $A \subseteq B \subsetneq L$ are DVRs, then $A = B$. So $\mathcal{O}_{L,v'} = (\mathcal{O}_L)_{\mathfrak{p}'}$ and the valuations on them must agree. □

Corollary 4.5. *Let K be a number field and $|-|$ an absolute value. Then $|-|$ is equivalent to*

- *an absolute value from $K \hookrightarrow \mathbb{R}$ or $\mathbb{C}$,*
- *or $v_{\mathfrak{p}}$ for some $\mathfrak{p} \subseteq \mathcal{O}_K$.*

Proof. If $|-|$ is archemedian, then its completion $\hat{K}$ is going to be $\mathbb{R}$ or $\mathbb{C}$. Then the embedding $K \to \hat{K}$ gives the valuation.

If it is non-archemedian, then its restriction to $\mathbb{Q}$ gives $|-|_p$ for some p, and so it is $|-|_{\mathfrak{p}}$ for some $\mathfrak{p} \mid p\mathcal{O}_K$. □

Now let K be a field with an absolute value $|-|_v$, and L be a finite separable extensions of K with absolute value $|-|_{v'}$ extending $|-|_v$. Now we have completions

$$\begin{tikzcd} K \arrow[r, hook] \arrow[d, hook] & K_v \arrow[d, hook] \\ L \arrow[r, hook] & L_{v'} \end{tikzcd}$$

and furthermore $L_{v'} = K_v \cdot L$ is the compositum. So $L_{v'}/K_v$ is finite. Conversely, if there exists some L'/K_v finite with $L' = L \cdot K_v$, then we can extend $|-|_v$ on K_v to L' and restricting to L gives an absolute value $|-|_{L'}$ on L. This gives a bijection

$$\left\{\begin{matrix}\text{isom.classes of}\\ \text{fields } L' \text{ with } L' = K_v \cdot L\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}\text{absolute values}\\ \text{of } L \text{ extending } |-|_v\end{matrix}\right\}.$$

Proposition 4.6. $K_v \otimes_K L \cong \prod_{v' \textit{ extending } v} L_{v'}$.

Proof. To get the map, note that we have bilinear maps $K_v \times L \to K_v \cdot L = L_{v'}$ for any v'.

It is a general fact that if L/K is finite separable and K'/K is any extension, then $K' \otimes_K L \cong \prod L_i$ where L_i runs over isomorphism classes of fields L' such that $L' = K' \cdot L$. Using this fact and the previous isomorphism, we get the result. □

Example 4.7. Take $K = \mathbb{Q}$, $K_v = \mathbb{Q}_3$ and $L = \mathbb{Q}[\sqrt{7}]$. By Hensel, 7 is a square in $\mathbb{Q}_3$, and so $x^2 - 7 = (x-a)(x+a)$ in $\mathbb{Q}_3[x]$. Now

$$L \otimes_{\mathbb{Q}} \mathbb{Q}_3 = \mathbb{Q}_3[x]/(x^2-7) \cong \mathbb{Q}_3[x]/(x-a) \times \mathbb{Q}_3[x]/(x+a).$$

So we have two embeddings $L = \mathbb{Q}[\sqrt{7}] \hookrightarrow \mathbb{Q}_3$, and each give different absolute values.

Example 4.8. Let $K = \mathbb{Q}$, $K_v = \mathbb{Q}_3$ and $L = \mathbb{Q}[\sqrt{3}]$. In this case,

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

is a field, and this is the unique extension of the absolute value.

Another example is $L = \mathbb{Q}[\sqrt[3]{2}]$. In this case $L \otimes_{\mathbb{Q}} \mathbb{Q}_3 \cong \mathbb{Q}_3 \times K$ where K is a quadratic extension. This is because $L/\mathbb{Q}$ is not Galois.

4.3 Local fields

Definition 4.9. A **local field** K is a locally compact complete valued field.

If K is a non-archemedian local field, then $\mathcal{O}_K$ is compact. This is because for $a \in \mathcal{O}_K$ with $|a| < 1$, one of the sets $a^n\mathcal{O}_K$ is compact by local compactness. These sets are all homeomorphic to $\mathcal{O}_K$.

This also means that the absolute value on $\mathcal{O}_K$ is discrete. Indeed, $\mathcal{O}_K$ has an open cover $\{a : a < c\}$ for $c < 1$ and so has a finite subcover. Then there no absolute values in $(c, 1)$ for some $c < 1$.

Choose a π with $|\pi| < 1$ maximal. The quotient $\mathcal{O}_K/(\pi)$ is compact and discrete. This implies that this is a finite field. Therefore non-archemedian local fields are field complete with respect to a discrete valuation with with finite residue field. If there is such a K_s, then

$$\mathcal{O}_K = \varprojlim \mathcal{O}_K/(\pi^n)$$

is compact.

Archemedian local fields are either $\mathbb{R}$ or $\mathbb{C}$, and these are actually locally compact.

Definition 4.10. If K is a non-archemedian local field with valuation v and residue field $k = \mathcal{O}/\pi$, the **standard normalization** is given by

$$|a|_K = |k|^{-v(a)}.$$

This works well, if you think K has a Haar measure on it. Multiplication by $|a|$ rescales the measure by $|a|_K$.

5 September 14, 2017

We have been talking about local fields. A field K is a local field, if it is a complete field (with respect to a absolute value) that is locally compact. If the absolute value is discrete, is equivalent to

$$k = \mathcal{O}_K / \pi_K \mathcal{O}_K$$

being finite. For example, $\mathbb{Q}_p$ and $\mathbb{F}_p((t))$ are both local fields, and finite extensions of local fields are local.

Theorem 5.1. *In fact, all local fields are finite extensions of* $\mathbb{Q}_p$ *or* $\mathbb{F}_p((t))$*, or just* $\mathbb{R}$ *or* $\mathbb{C}$

Definition 5.2. K is a **global field** if every completion of K is a local field.

Examples of global fields are $\mathbb{Q}$, which complete to $\mathbb{Q}_p$ or $\mathbb{R}$, and $\mathbb{F}_p(t)$, which complete to $\mathbb{F}_q((t))$ for some q.

Theorem 5.3. *All global fields are finite extensions of either* $\mathbb{Q}$ *or* $\mathbb{F}_p(t)$*.*

If K is a global field, we have the product formula.

Proposition 5.4 (Product formula)**.** *For* $a \in K^\times$*,*

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

where v *runs over normalized absolute values.*

Proof. For $K = \mathbb{Q}$ and $K = \mathbb{F}_p(t)$, we can manually check this. If the product formula holds for K, we want a product formula for L/K a finite extension. This follows from the fact that if v is a place of K, then

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

(This claim follows from what we did last time, that $L \otimes_K K_v \cong \prod L_{v'}$.) □

5.1 Multiplicative group of local fields

Let K be a (non-archemedian) local field, with discrete valuation $K^\times \twoheadrightarrow \mathbb{Z}$. We have an exact sequence

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

This sequence splits, but not canonically, with the choice of a uniformizer π with $v(\pi) = 1$.

Now there is another exact sequence

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

and this splits canonically due to Hensel lifting. There are $q-1$ roots of unity in $\mathcal{O}^\times$. Then we can say that

$$\mathcal{O}^\times \cong U_1 \times \mu_{q-1} \cong U_1 \times k^\times.$$

We can filter down even more. For any n we have

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

and get a decreasing filter $U_1 \supseteq U_2 \supseteq \cdots$.

Proposition 5.5. *For $n \geq 1$, $U_n/U_{n+1} \cong k^+$ non-canonically.*

Proof. Pick a uniformizer π and look at the map

$$k^+ \to U_n/U_{n+1}; \quad a \mapsto [1+\pi^n a].$$

This is an isomorphism and it is not hard to see that it is an isomorphism. □

This means that $U_n^p \subseteq U_{n+1}$. On the other hand, if $(m,p)=1$ then

$$U_n \to U_n; \quad x \mapsto x^m$$

is a bijection.

Proof. To show that this map is injective, take any $a \in U_n$ with $a \neq 1$. Let N be maximal with $a \in U_N - U_{N+1}$. Then $[a] \in U_N/U_{N+1}$ is not equal to 1, and so $[a^m] \in U_N/U_{N+1}$ is not equal to 1. This shows $a^m \neq 1$ and so we have injectivity.

For surjectivity, use Hensel's lemma, or directly prove it using surjectivity of $x \mapsto x^m$ on U_n/U_{n+1}. □

So if we look at the roots of unity with order prime to p, it must have trivial intersection with U_1. It also have to map bijectively to $\mathcal{O}^\times/U_1 = k^\times$. So these are exactly μ_{q-1}, where $k = \mathbb{F}_q$.

On the other hand, if we have a root of unity $a \in \mathcal{O}^\times$ of order p^i, it must be in $a \in U_1$.

5.2 Exponential and logarithm

Let K be a local field of characteristic 0. (So it is a finite extension of $\mathbb{Q}_p$.) Let $p\mathcal{O}_K = (\pi)^e$ for some e.

Definition 5.6. We define the **exponential** as

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

It is an exercise in analysis that this power series converges for $v(x) > e/(p-1)$. The important fact here is that $v_p(n!) = (n - s(n))/(p-1)$ where $s(n)$ is the sum of base-p digits of n.

Definition 5.7. Define the **logarithm** as

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

This converges with $v(z) > 0$, equivalently $1+z \in U_1$.

Theorem 5.8. *For any $n > e/(p-1)$, the maps*

$$\exp_p : (\pi)^n \to U_n, \quad \log_p : U_n \to (\pi)^n$$

are inverse homomorphisms.

Proof. You mainly just need to check that exp sends (π^n) to U_n and vice versa. Then as power series, they are inverses and homomorphisms, as we know from our previous experiences. □

Corollary 5.9. *For $p > 2$, we have $\mathbb{Z}_p^\times = \mu_p \times U_1 \cong (\mathbb{Z}/(p-1)\mathbb{Z})^+ \times \mathbb{Z}_p^+$, and for $p = 2$, we have $\mathbb{Z}_2^\times = \mu_2 \times U_2 \cong (\mathbb{Z}/2\mathbb{Z})^+ \times \mathbb{Z}_2^+$.*

Proof. With p odd, we have $e = 1$ and so $e/(p-1) < 1$. Now apply the theorem. For $p = 2$, we have $e = 1$ and so apply to $2 = n > e/(p-1) = 1$. □

This works out very nicely for $\mathbb{Z}_p^\times$, but in general we won't have something as nice as this. Here, we have some

$$U_n \cong \mathcal{O}^+ \cong \mathbb{Z}_p^{[K:\mathbb{Q}_p]}.$$

Again we have

$$1 \to U_n \to U_1 \to U_1/U_n \to 1,$$

where U_1/U_n is a finite p-group, but it may not split.

5.3 Unramified extensions

Let L/K be a finite extension of complete fields with discrete absolute values. Recall that we have $\mathcal{O}_L$ over $\mathcal{O}_K$ and also have residue fields $\ell = \mathcal{O}_L/\pi_L$ and $k = \mathcal{O}_K/\pi_K$. Then we have the ramification index

$$\pi_K\mathcal{O}_L = (\pi_L\mathcal{O}_L)^{e_{L/K}}$$

and the inertia degree $f_{L/K} = [\ell : k]$. We have proved that $n = [L : K] = e_{L/K}f_{L/K}$.

Definition 5.10. L/K is **unramified** if $e_{L/K} = 1$ and ℓ/k is separable. (This second condition is automatic for local fields.)

Lemma 5.11. *Suppose $L = K(a)/K$ be a finite extension, and K be complete with a discrete valuation. If there exists a monic polynomial $f(x) \in \mathcal{O}_K[x]$ such that $f(a) = 0$ such that $\overline{f}(x) \in k[x]$ is separable, then L/K is unramified and $\mathcal{O}_L = \mathcal{O}_K[a]$.*

Proof. I might as well take f to be the minimal polynomial of a so that f is irreducible. If follows that $\bar{f} \in k[x]$ is also irreducible by Hensel's lemma, since $\bar{f}$ is separable. Now $\bar{a} \in \ell$ have minimal polynomial $\bar{f}$. This means that

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

This means that $[\ell : k] = [L : K]$.

Note that we also have from this, $\ell = k(\bar{a})$. Apply Nakayama to $\mathcal{O}_K[a] \subseteq \mathcal{O}_L$ as $\mathcal{O}_K$-modules. We have that $\mathcal{O}_K[a] + \pi_L \mathcal{O}_L = \mathcal{O}_L$ and so we conclude that $\mathcal{O}_K[a] = \mathcal{O}_L$. □

Let L/K be unramified and let ℓ/k be their residue fields. Choose any prime element $\bar{a} \in \ell$ with $\ell = k(\bar{a})$. Let $\bar{f}$ be the monic minimal polynomial of f. Then we can lift $\bar{f} \in k[x]$ to a $f \in \mathcal{O}_K[x]$. Then we can lift $\bar{a}$ to $a \in \mathcal{O}_K$ with $f(a) = 0$, by Hensel. Then

$$[K(a) : K] = [k(a) : k] = [\ell : k] = [L : K],$$

and so $L = K(a)$ and $\mathcal{O}_L = \mathcal{O}_K[a]$ by our lemma.

Example 5.12. If $L = K(\zeta_n)$ for some n relatively prime to p, then the lemma applies and we have L/K unramified and $\mathcal{O}_L = \mathcal{O}_K[\zeta_n]$.

In particular, let $n = p^m - 1$ and $K = \mathbb{Q}_p$. This extension has degree

$$[\mathbb{Q}_p(\zeta_{p^m-1}) : \mathbb{Q}_p] = [\mathbb{F}_p(\zeta_{p^m-1}) : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_p] = m.$$

So $\mathbb{Q}_p(\zeta_{p^m-1})$ is an unramified extension of degree m.

6 September 19, 2017

Let K be a local field and L/K be unramified. This means that $e_{L/K} = 1$, or equivalently $f_{L/K} = [L : K]$. We showed that any such L is of the form $K(a)$ with $a \in \mathcal{O}_L^\times$, such that the minimal polynomial $f(x)$ of a satisfies $\bar{f}(x) \in k[x]$ is irreducible.

Proposition 6.1. *There is a unique unramified extension L/K of degree n, for every $n \geq 1$.*

Proof. We constructed the extension $L = K(\zeta_{q^n-1})$ where $q = |k|$. For uniqueness, suppose we have L, L' as above. We can write $L' = K(a)$ where $f(x)$ is the minimal polynomial of a. The polynomial f has degree $[L' : K] = n$, and so $\bar{f}(x)$ is irreducible of degree n over k.

The residue field ℓ of L is a extension of k of degree n. Because k is a finite field, $\bar{f}(x) \in k[x]$ splits in ℓ. By Hensel's lemma, $f(x)$ has a root in L. That is, we have an inclusion

$$L' \hookrightarrow L; \quad a \mapsto \text{root}$$

which must be an isomorphism because $[L : K] = [L' : K]$. □

More generally, suppose L and L' are unramified extensions of K with residue fields ℓ and ℓ'. If there is a map $\varphi : \ell \hookrightarrow \ell'$ that fixes k, then the same argument shows that we can lift the map uniquely to

$$\tilde{\varphi} : L \hookrightarrow L'$$

so that $\mathcal{O}_L/\pi_L \to \mathcal{O}_{L'}/\pi_{L'}$ is φ. In fact, we have an equivalence of categories

$$\left\{\begin{matrix}\text{finite extensions} \\ \text{of } k\end{matrix}\right\} \quad \longleftrightarrow \quad \left\{\begin{matrix}\text{finite unramified} \\ \text{extensions of } K\end{matrix}\right\}.$$

There is even a canonical construction called Witt vectors that goes from finite extensions of k to finite unramified extensions of K.

Corollary 6.2. *Every unramified extension of K is equal to $K(\zeta_m)$ for some m.*

The compositum of two unramified extensions of K is unramified. So it is meaningful to talk about the maximal unramified extension K^{unr} of K. This is

$$K^{\text{unr}} = \bigcup (\text{finite unramified extensions}) = \bigcup_{(m,p)=1} K(\zeta_m).$$

This is even an abelian extension.

6.1 Artin map for unramified extensions

Let L/K be a finite extension of local field. Recall that we've conjectured there exists an Artin map

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

We will verify this for unramified extensions by just computing both sides. If $[L:K]=n$, we have the isomorphism

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(\ell/k) \cong (\mathbb{Z}/n\mathbb{Z})^+$$

by what we know about finite fields.

The other side is harder to deal with. We have the valuation map $v : K^\times \to \mathbb{Z}$, and this extends to $v : L^\times \to \mathbb{Z}$. Let's look at what this does on the norm. We have

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

This means that $v : NL^\times \twoheadrightarrow n\mathbb{Z}$. So we have a short exact sequence

$$1 \to \mathcal{O}_K^\times/N\mathcal{O}_L^\times \to K^\times/NL^\times \to (\mathbb{Z}/n\mathbb{Z})^+ \to 0.$$

We need to show that $\mathcal{O}_K^\times = N\mathcal{O}_L^\times$.

We have filtrations

$$\begin{aligned} \mathcal{O}_K^\times &= U_{K,0} \supseteq U_{K,1} \supseteq U_{K,2} \supseteq \cdots \\ \mathcal{O}_L^\times &= U_{L,0} \supseteq U_{L,1} \supseteq U_{L,2} \supseteq \cdots \end{aligned}$$

with $N : U_{L,i} \to U_{K,i}$. My claim is that

$$N : U_{L,i}/U_{L,i+1} \to U_{K,i}/U_{K,i+1}$$

is surjective. If $i=0$, we have

$$N : \mathcal{O}_L^\times/U_{L,1} \cong \ell^\times \to k^\times \cong \mathcal{O}_K^\times/U_{K,1}.$$

This is something about finite fields, and you can check that this is surjective. Something similar happens for $i>0$. There is an identification

$$\ell^+ \cong U_{L,i}/U_{L,i+1}; \quad a \mapsto [1+\pi_L^i a]$$

and a similar identification for K. But note that we can choose $\pi_L = \pi_K$ because L/K is unramified. Then what we are trying to show reduces to showing that

$$\mathrm{tr} : \ell^+ \to k^+$$

is surjective. This also can be checked.

Now we want to show that if $a \in \mathcal{O}_K^\times$ there exists a $b \in \mathcal{O}_L^\times$ with $Nb = a$. First find a $b_1 \in \mathcal{O}_L^\times$ such that

$$Nb_1 \equiv a \pmod{U_{K,1}}.$$

Then there exists a $c_2 \in U^{\times}_{L,1}$ such that $Nc_2 \equiv a(Nb_1)^{-1} \bmod U_{K,2}$ so that

$$N(b_1c_2) \equiv a \pmod{U_{K,2}}.$$

We can keep on going to get b.

Theorem 6.3. *If L/K is a unramified extension of local fields, then there is an isomorphism*

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

with both sides being isomorphic to $(\mathbb{Z}/n\mathbb{Z})^+$.

6.2 Decomposition group

Let L/K be a Galois extension, and $v \in K$ and $v' \in L$ be places with v' extending v. We define **decomposition group**

$$D_{v'} = D_{v'}(L/K) = \{g \in \mathrm{Gal}(L/K) : |ga|_{v'} = |a|_{v'} \text{ for all } a \in L\}.$$

We have shown that if K is complete, then $D_{v'}(L/K) = \mathrm{Gal}(L/K)$.

If $K = \mathrm{Frac}\,\mathcal{O}_K$ with $\mathcal{O}_K$ a Dedekind domain and $v = v_{\mathfrak{p}}$, then we have shown that $v' = v_{\mathfrak{p}'}$ for some $\mathfrak{p}'$ dividing $\mathfrak{p}$. Then

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

If v is archemedian, then complex conjugation is always going to be in the decomposition group.

If K_v and $L_{v'}$ are completions, then

$$D_{v'}(L/K) = D_{v'}(L_{v'}/K_{v'}) = \mathrm{Gal}(L_{v'}/K_{v'}).$$

This is because if g fixes v' then it lifts to the completion, and if it acts on $L_{v'}$ then its restriction to L fixes v'. In this case, let

$$Z = Z(v') = \text{fixed field of } D_{v'}(L/K).$$

We can restrict v' to Z and get a place v_Z on $Z(v')$.

$$\begin{tikzcd}
L \arrow[d, dash] & v' \arrow[d, mapsto] \\
Z(v') \arrow[d, dash] & v_Z \arrow[d, mapsto] \\
K & v
\end{tikzcd}$$

Proposition 6.4. *v' is the only valuation of L extending v_Z.*

Proof. Note that $\mathrm{Gal}(L/Z)$ acts transitively on $\{$valuations of L extending $v_Z\}$. (This is equivalent to the same statement about primes in the non-archemedian case, and can be worked out in the archemedian case.) Because $D_{v'}(L/K)$ fixes v', there is only one valuation extending v_Z. □

We now have

$$\mathrm{Gal}(L/Z) \cong D_{v'} \cong \mathrm{Gal}(L_{v'}/K_v),$$

and this really means that Z embeds in K_v and $Z = K_v \cap L$.

6.3 Inertia group

Suppose I have a Galois extension L/K and v a discrete valuation on K. Suppose v' on L extends v. Define the **inertia group** as

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

In other words, $I_{v'}$ is the kernel of the map

$$D_{v'} \to \mathrm{Gal}(\ell/k).$$

We then have a short exact sequence

$$1 \to I_{v'} \to D_{v'} \to \mathrm{Gal}(\ell/k) \to 1$$

because $D_{v'} \to \mathrm{Gal}(\ell/k)$ is surjective. The proof of surjectivity goes like this.

Proof. By replacing with completions if necessary, we can assume that $D_{v'} = \mathrm{Gal}(L/K)$. Pick some $\bar{a} \in \ell$ and let its minimal polynomial be $\bar{f}(x)$. Lift it to $a \in \mathcal{O}_{v'}$. For

$$h(x) = \prod_{g \in \mathrm{Gal}(L/k)} (x - ga) \in \mathcal{O}_K[x],$$

we will have that $\bar{a}$ is a root of

$$\bar{h}(x) = \prod_{g \in \mathrm{Gal}(L/K)} (x - \overline{ga}) \in k[x].$$

For any $\bar{a}'$ Galois conjugate to $\bar{a}$ in ℓ, there exists a $g \in \mathrm{Gal}(L/K)$ such that $\overline{ga} = \bar{a}'$. □

Corollary 6.5. *If L/K is complete, then $I_{v'}$ has size e.*

Proof. This is because $D_{v'} = \mathrm{Gal}(L/K)$ has size ef and $\mathrm{Gal}(\ell/k)$ has size f. □

Proposition 6.6. *Let $T(v')$ be the fixed field of $I_{v'}$. Then $T(v')$ is the maximal unramified subextension of L/K.*

Proof. Let t be the residue field of T. Then $\mathrm{Gal}(L/T) \twoheadrightarrow \mathrm{Gal}(\ell/t)$ but

$$\begin{tikzcd}
\mathrm{Gal}(L/T) \arrow[r, two heads] \arrow[d, "\cong"] & \mathrm{Gal}(\ell/t) \arrow[d, hook] \\
I(L/K) \arrow[r, "1"] & \mathrm{Gal}(\ell/k).
\end{tikzcd}$$

This implies that $\ell = t$ and $f_{L/T} = 1$. On the other hand, $e_{L/T} = [L : T] = e_{L/K}$. This shows that $e_{T/K} = 1$ and $f_{T/K} = f_{L/K}$. □

7 September 21, 2017

Last time we had L/K a Galois extension of local fields and defined T which corresponds to $I(L/K) \subseteq \mathrm{Gal}(L/K)$. Then

$$e_{L/T} = [L : T], \quad f_{L/T} = 1,$$

and

$$e_{T/K} = 1, \quad f_{L/K} = [L : K].$$

7.1 Totally ramified extensions of local fields

Let L/K be a totally ramified finite extension between local fields, so that $e_{L/K} = [L : K] = n$.

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

Proof. We will show that $1, \pi_L, \dots, \pi_L^{n-1}$ are linearly independent over K. In other words, that

$$\sum_{0 \le i < n} a_i \pi_L^i \neq 0$$

for $a_i \in K$ not all zero. Note that

$$v_L(a_i \pi_L)^i = i + n v_K(a_i),$$

and so

$$v\left(\sum_{0 \le i < n} a_i \pi_L^i \right) = \min_{0 \le i < n} (i + n v_K(a_i)) < \infty.$$

It can also be checked from this formula that $\sum_{0 \le i < n} a_i \pi_L^i$ is in $\mathcal{O}_L$ if and only if $a_i \in \mathcal{O}_K$ for all i. □

The minimal polynomial f of π_L has degree n. Let

$$f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0.$$

Then we get $c_0 = N_{L/K}(\pi_K)$ so $v_L(c_0) = n$. It follows that $v_K(c_0) = 1$. Likewise, we have c_i as a symmetric polynomial of the Galois conjugates of π_K, so $v_K(c_i) > 0$ for $0 \le i \le n-1$. Such a polynomial is called an **Eisenstein polynomial**.

Conversely, if $f(x) \in K[x]$ is any Eisenstein polynomial, i.e., $v_K(c_i) > 0$ and $v_K(c_0) = 1$, then $L = K(a) = K[x]/f(x)$ is totally ramified. This is because $|a|_L = |c_0|_K^{1/n}$.

Example 7.2. Let K be an arbitrary local field and let $L = K(\sqrt[m]{\pi_K})$. Then $\pi_L = \sqrt[m]{\pi_K}$ has minimal polynomial

$$x^m - \pi_K = 0.$$

Example 7.3. Let $K = \mathbb{Q}_p$ and let $L = \mathbb{Q}_p[\zeta_{p^r}]$. This time, $\pi_L = \zeta_{p^r} - 1$, which you can check as an exercise.

7.2 Ramification groups

Let L/K be an arbitrary finite extension, and let v' be a place of L lying over v of K. We have defined the decomposition group $D_{v'}(L/K)$ and the inertia group $I_{v'}(L/K)$. Then L/T is totally ramified and T/Z is entirely inert.

$$\begin{tikzcd}
L \arrow[d, dash, "\text{total ram.}"'] & \{1\} \arrow[d, hook] \\
T \arrow[d, dash, "\text{inert}"'] & I_{v'}(L/K) \arrow[d, hook] \\
Z \arrow[d, dash] & D_{v'}(L/K) \arrow[d, hook] \\
K & \mathrm{Gal}(L/K)
\end{tikzcd}$$

Now we are going to define a filtration

$$I_{v'}(L/K) = G_{0,v'} \supseteq G_{1,v'} \supseteq G_{2,v'} \supset \cdots .$$

Definition 7.4. We define the **ramification groups** as

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

Note that $G_{N,v'} = \{1\}$ for all $N \gg 0$. Also, $g_{i,v'}$ is a subgroup of $D_{v'}$ acting trivially on $\mathcal{O}_{v'}/(\pi_L^{i+1})$. If we complete the field, then

$$G_{i,v'}(L/K) = G_{i,v'}(L_{v'}/K_{v'}).$$

Now let's assume that L, K are non-archemedian local fields, and write $v_L = v'$ and $v_K = v$. We can rewrite

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

If a_0 generates $\mathcal{O}_L/\mathcal{O}_K$, i.e., $\mathcal{O}_L = \mathcal{O}_K[a_0]$, then we can just check for a_0:

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

Proposition 7.5. $G_i(L/K) = \{g \in I(L/K) : v_L(g\pi_L - \pi_L) > i\}$.

Proof. It suffices to show this in the case when L/K is totally ramified. This is because we can replace K by T. Now in this case we have $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, and so take $a_0 = \pi_L$. □

For each $i \geq 0$, we have a map

$$\varphi_i : G_i/G_{i+1} \hookrightarrow U_{i,L}/U_{i+1,L}; \quad g \mapsto [g\pi_L/\pi_L].$$

It can be shown that these maps are group homomorphisms. It turns out that this map is completely canonical, i.e., independent of the choice of π_L. If we replace π_L with $u\pi_L$, then

$$\frac{g(u\pi_L)}{u\pi_L} = \frac{gu}{u}\frac{g\pi_L}{\pi_L}$$

where $gu/u \in U_{i+1,L}$.

Recall that $U_{0,L}/U_{1,L} \cong \ell^\times$ and $U_{i,L}/U_{i+1,L} \cong \ell^+$ for $i \geq 1$. We conclude that G_0/G_1 is cyclic of order relatively prime to $\mathrm{char}(\ell) = p$ and G_i/G_{i+1} is an abelian group of exponent of p. From the fact that the filtration goes down to $\{1\}$, we deduce that G_1 is a p-group. So G_1 is a p-Sylow subgroup of $I(L/K) = G_0$.

We call G_0/G_1 the **tame inertia group** and G_1 the **wild inertia group**. We say that L/K is **tamely ramified** if $G_1 = \{1\}$. This is equivalent for $e_{L/K} = |G_0|$ is relatively prime to p.

Example 7.6. Let $K = \mathbb{Q}_2$ and $L = K[\zeta_8]$. Then $[L : K] = 4 = e_{L/K}$ and we can take the uniformizer as $\pi_L = \zeta_8 - 1$. We have

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

so that $g_i(\zeta_8) = \zeta_8^i$. Let's compute $v_L(g_i\pi_L - \pi_L)$ for each i. We have

$$\begin{aligned}
&v_L(g_1\pi_L - \pi_L) = v_L(0) = \infty,\\
&v_L(g_3\pi_L - \pi_L) = v_L(\zeta_8^3 - \zeta_8) = v_L(\zeta_8(\zeta_8 - 1)(\zeta_8 + 1)) = 2,\\
&v_L(g_5\pi_L - \pi_L) = v_L(\zeta_8^5 - \zeta_8) = v_L(-2\zeta_8) = 4,\\
&v_L(g_7\pi_L - \pi_L) = v_L(\zeta_8^7 - \zeta_8) = v_L(\zeta_8^2(\zeta_8^3 - \zeta_3)) = 2.
\end{aligned}$$

So

$$\{g_1, g_3, g_5, g_7\} = G_0 = G_1 \supsetneq G_2 = \{g_1, g_5\} = G_3 \supsetneq G_4 = \{g_1\} = G_5 = \cdots .$$

7.3 Tamely ramified extensions

Let L/K be a Galois extension of local fields. This is tamely ramified if and only if $(e_{L/K}, p) = 1$. Clearly, unramified extensions are tamely ramified!

Note that we can take the definition of tamely ramified as $(e_{L/K}, p) = 1$, and then we don't need to assume the Galois extension. Here are two facts:

- Compositum of tamely ramified extensions are tamely ramified.
- L/K tamely ramified implies that the Galois closure of L is tamely ramified.

Example 7.7. The field $K[\zeta_m, \sqrt[d]{\pi_K}]$ for $(m, p) = 1$ and $d \mid m$ is a Galois extension of K and is tamely ramified.

Proposition 7.8. *Let L/K be Galois and tamely ramified. Then $L \subseteq K[\zeta_m, \sqrt[d]{\pi_K}]$ for some $(m, p) = 1$ and $d \mid m$.*

Proof. By replacing K with its maximal unramified extension of K in L, we may assume that L/K is totally ramified. Then

$$\mathrm{Gal}(L/K) = G_0(L/K) \cong G_0/G_1,$$

is a cyclic group of order n with $(n,p)=1$. Let $K' = K(\zeta_n)$ and $L' = L(\zeta_n)$. Then there is an inclusion

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

and so $\mathrm{Gal}(L'/K')$ is cyclic of order $d \mid n$.

Since K' contains the n-root of unity, we can use Kummer theory to write

$$L' = K'(\sqrt[d]{a})$$

for some $a \in (K')^\times$. If we write $a = \pi_K^r u$ for $u \in \mathcal{O}_{K'}^\times$, then

$$L \subseteq L' \subseteq K'(\sqrt[d]{u}, \sqrt[d]{\pi_K}) \subseteq K''(\sqrt[d]{\pi_K})$$

for some unramified extension K'' of K. □

Before wrapping up the discussion of ramification, let me give a big picture of local class field theory over $\mathbb{Q}_p$. Over abelian extensions of $\mathbb{Q}_p$, the maximal unramified extension is $\mathbb{Q}_p[\zeta_{\text{prime to } p}]$ and the maximal tamely ramified extension is $\mathbb{Q}_p[\zeta_{\text{prime to } p}, p^{1/(p-1)}]$.

$$\begin{tikzcd}
\mathbb{Q}_p^{\mathrm{ab}} \arrow[d, dash, "\mathbb{Z}_p^+"', "\text{wild}"] \\
\mathbb{Q}_p[\zeta_{\text{prime to } p}, p^{1/(p-1)}] \arrow[d, dash, "\mathbb{F}_p^\times"'] \\
\mathbb{Q}_p[\zeta_{\text{prime to } p}] \arrow[d, dash, "\hat{\mathbb{Z}}^+"'] \\
\mathbb{Q}_p
\end{tikzcd}$$

The Artin map is then

$$\mathbb{Q}_p^\times \to \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p), \quad \mathbb{Z}_p^\times \xrightarrow{\cong} \mathrm{Gal}(\mathbb{Q}_p^{\mathrm{ab}}/\mathbb{Q}_p^{\mathrm{unr}}).$$

Another remark is that the numbering of the ramification group is not the best. For $L'/L/K$, the groups $G_i(L'/K)$ and $G_i(L/K)$ are not going to be related because they are defined in terms of different valuations.

To fix this, there is an **upper numbering**. Define

$$\phi(u) = \int_0^u \frac{dt}{[G_0 : G_t]},$$

and write $G^i = G_{\phi^{-1}(i)}$. Then Herbrard showed that $G^i(L'/K)$ restricts to $G^i(L/K)$, and Hasse–Arf showed that if L/K is abelian then jumps in G^i occur at integer points.

Example 7.9. For the case $\mathbb{Q}_2(\zeta_8)/\mathbb{Q}_2$, we have $G^3 = G_4$ and $G^2 = G_2$.

8 September 26, 2017

I am now going to move on to Galois cohomology. Roughly I will be following Cassels–Frohlich, but it can be a bit terse. Other references include Neukirch, *Class Field Theory—Bonn lectures* or Dummit–Foote.

8.1 Category of G-modules

Let G be a finite group, in most cases, $G = \mathrm{Gal}(L/K)$.

Definition 8.1. A **G-module** A is an abelian group A with an action of G, satisfying $g(a+b) = ga + gb$.

This is like representations, but with abelian groups rather than vector spaces.

Example 8.2. For $G = \mathrm{Gal}(L/K)$, the abelian groups L^+, $L^\times$, $\mathcal{O}_L^\times$, $\mu_n(L)$, $\mathrm{Cl}(\mathcal{O}_L)$, $\mathbb{A}_L^\times/L^\times$ are all G-modules. We are going to be interested in $L^\times$ for L a local field this semester. Next semester we are going to be interested in $\mathbb{A}_L^\times/L^\times$ for L a global field.

Also, for any commutative algebraic group $\mathbb{G}$ over K, you can look at $\mathbb{G}(L)$ as a $\mathrm{Gal}(L/K)$-module. For instance, if E is an elliptic curve over K, then $E(L)$ is a G-module. This is important if you study Selmer groups.

Example 8.3. For G any group and A any abelian group, there is a trivial action $ga = a$ that makes A into a G-module. In many cases we are going to look at $A = \mathbb{Z}$.

A G-module is the same thing as $\mathbb{Z}[G]$-modules, where $\mathbb{Z}[G]$ is the **group ring**, a non-commutative ring of formal linear combinations

$$\sum_{g\in G} a_g g,$$

with multiplication done formally. If $G = C_n = \langle t\rangle$ is a cyclic group, then

$$\mathbb{Z}[G] = \mathbb{Z} \oplus \mathbb{Z}t \oplus \cdots \oplus \mathbb{Z}t^{n-1} = \mathbb{Z}[t]/(t^n - 1).$$

This is *not* the same thing as $\mathbb{Z}[\zeta_n]$.

The ring $\mathbb{Z}[G]$ has an important ideal, called the **augmentation ideal** $I_G = \ker \epsilon$, where

$$\epsilon : \mathbb{Z}[G] \twoheadrightarrow \mathbb{Z}; \quad \sum a_g g \mapsto \sum a_g.$$

As a $\mathbb{Z}$-module, I_G is free and is spanned by $g-1$. In the case $G = C_n$, the ideal I_G is just $(t-1)\mathbb{Z}[G]$.

We can also consider the operator $N = \sum_{g\in G} g$. Then for any G-module A, we have

$$NA = \Big\{ \sum_{g\in G} ga : a \in A \Big\}.$$

If $A = L^\times$, then N becomes the norm and $NA = NL^\times$. If $A = L^+$, then N becomes the trace map.

G-modules form an abelian category, i.e., we can take kernels, cokernels, images, direct sums, etc. If A and B are G-modules, we can take

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

has a natural structure of a G-module. This works by $g \cdot \phi = g\phi(g^{-1}-)$. Likewise we can take tensor products

$$A \otimes B = A \otimes_{\mathbb{Z}} B$$

and the action is $g(a \otimes b) = ga \otimes gb$.

There are also functors $G-\mathsf{Mod} \to \mathbb{Z}-\mathsf{Mod}$. If A is a G-module, we have

$$\begin{aligned} A^G &= \{a \in A : ga = a \text{ for all } g \in G\}, \\ A_G &= A/\langle a - ga \rangle = A/I_G A. \end{aligned}$$

The A^G is called the invariants and A_G is called the coinvariants. It can be checked that these are both functions.

These are actually special cases. If $A, B \in G-\mathsf{Mod}$, then we have $\mathrm{Hom}_G(B, A)$ is an abelian group, but not generally a G-module. If $B = \mathbb{Z}$, then

$$\mathrm{Hom}_G(\mathbb{Z}, A) = A^G.$$

We can also take the tensor product. Generally, $A \otimes_R G$ makes sense if A is a right R-module and B is a left R-module. So in order for us to take $A \otimes_G B$, we need to look at a A as a right $\mathbb{Z}[G]$-module. This is done by looking at the g^{-1} action instead of g. So

$$A \otimes_G B = A \otimes_{\mathbb{Z}} B / \langle g^{-1}a \otimes b - a \otimes gb \rangle.$$

Then $A_G = \mathbb{Z} \otimes_G A$. On the other hand, we have $\mathrm{Hom}_G(B, A) = \mathrm{Hom}(A, B)^G$ and $A \otimes_G B = (A \otimes B)_G$.

Proposition 8.4. *The functor $A \to A^G$ is left exact, i.e., $0 \to A \to B \to C$ exact implies $0 \to A^G \to B^G \to C^G$ exact.*

Proof. Injectivity of $A^G \to B^G$ is clear. If $b \in B^G$ with $\psi(b) = 0$, then by exactness there exists a unique A such that $\varphi(a) = b$. This means that $a = ga$ for any $g \in G$. So $a \in A^G$. □

This is also a special case of the fact that $\mathrm{Hom}(B, -)$ is left exact for any abelian category.

Proposition 8.5. *The functor $A \to A_G$ is right exact, i.e., $A \to B \to C \to 0$ exact implies $A_G \to B_G \to C_G \to 0$ exact.*

This is also a special case of the fact that $B \otimes -$ is right exact. You can use that this is the left adjoint functor to $\mathrm{Hom}(B, -)$ to show this.

Example 8.6. Let $G = C_1 = \{1, t\}$. Consider the $\mathbb{Z}_\chi = \mathbb{Z}$ as an abelian group, but with the G-action by the character $\chi : G \to \{1, -1\}$, $1 \mapsto 1$, $t \mapsto -1$ as $g(a) = \chi(g)a$. We have the exact sequence

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

If we take the invariants, we get

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

If we take the coinvarians, we get

$$\mathbb{Z}/2 \xrightarrow{\cdot 2} \mathbb{Z}/2 \to \mathbb{Z}/2 \to 0.$$

Example 8.7. Let L/K be a totally ramified extension of local fields. To make this simple, let us use a quadratic extension, e.g., $\mathbb{Q}_p(\sqrt{p})/\mathbb{Q}_p$. There is an exact sequence

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

If we take G-invariants,

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

but the image of $K^\times \to \mathbb{Z}$ is now $2\mathbb{Z}$.

We say that a G-module is **free** if F is a direct sum of (possibly infinitely many) copies of $\mathbb{Z}[G]$. If F is free, then $\mathrm{Hom}_G(F, -)$ is exact because $\mathrm{Hom}_G(\mathbb{Z}[G], -)$ is just the identity. Likewise, $F \otimes_G -$ is exact. The fact that $\mathrm{Hom}_G(F, -)$ is exact means that F is projective: there always is a lift

$$\begin{tikzcd} F \arrow[d, dashed, "\tilde{\varphi}"'] \arrow[dr, "\varphi"] & \\ B \arrow[r, "\pi"] & C. \end{tikzcd}$$

That $F \otimes_G -$ is exact is that F is flat.

Definition 8.8. A G-module is **coinduced** if it is of the form $A = \mathrm{Hom}(\mathbb{Z}[G], X)$ for X an abelian group. Likewise A is called **induced** if $A = \mathbb{Z}[G] \otimes X$ for some abelian group X.

When G is finite, we have $\mathrm{Hom}(\mathbb{Z}[G], X) \cong \mathbb{Z}[G] \otimes X$ and so coinduction is the same thing as induction. This is sort of a generalization of freeness, because if X is a free module, then we would get a free $\mathbb{Z}[G]$-module. The coinduced modules are going to be "cohomologically trivial" objects, and the induced modules are going to be "homologically trival".

Proposition 8.9 (Baby Frobeinus reciprocity)**.** $\mathrm{Hom}_G(\mathbb{Z}[G] \otimes X, B) \cong \mathrm{Hom}(X, B)$ *and* $\mathrm{Hom}_G(B, \mathrm{Hom}(\mathbb{Z}[G], X)) \cong \mathrm{Hom}(B, X)$.

Proposition 8.10. *Every G-module A injects into a coinduced G-module, and every A has a surjection from an induced G-module.*

Proof. We take $A' = \operatorname{Hom}(\mathbb{Z}[G], A)$ where A is taken to have a trivial G-action. Then the map $a \mapsto \phi_a$ given by $\phi_a(g) = ga$ is injective. Likewise, we have a surjection $\mathbb{Z}[G] \otimes A \to A$. □

Next time, we are going to construct group cohomology functors $H^i(G, A)$ that are $\mathbb{Z}$-modules. These will be derived functors of $A \to A^G$. That is, if $0 \to A \to B \to C \to 0$ then

$$0 \to A^G \to B^G \to C^G \to H^1(G, A) \to H^1(G, B) \to H^1(G, C) \to H^2(G, A) \to \cdots .$$

We will also construct $H_i(G, A)$ that gives

$$\cdots \to H_2(G, C) \to H_1(G, A) \to H_1(G, B) \to H_1(G, C) \to A_G \to B_G \to C_G \to 0.$$

It turns out we can splice these together to get Tate cohomology, which is $\hat{H}^i(G, A) = H^i(G, A)$ if $i \geq 1$ and $\hat{H}^i(G, A) = H_{-1-i}(G, A)$ for $i \leq -2$. Here, we will get

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

So if $A = L^\times$, then $\hat{H}^0(G, A) = K^\times/NL^\times$.

9 September 28, 2017

The goal for today is to define group cohomology. But there is a correction I want to make. When we defined coinduction, we define $\mathrm{Coind}^G(X) = \mathrm{Hom}(\mathbb{Z}[G], X)$. In general, we defined $\mathrm{Hom}(A, B)$ for G-modules A and B as $g\varphi = g \circ \varphi \circ g^{-1}$, because we needed to make A have a right G-action. But note that $\mathbb{Z}[G]$ has a natural right action. So we can simply define the group action on $\mathrm{Coind}^G(X)$ as

$$(g\varphi)(b) = \varphi(bg).$$

Actually, the results are isomorphic, i.e., there exists an isomorphism $\mathrm{Hom}(\mathbb{Z}[G], X) \to \mathrm{Coind}^G(X)$.

9.1 Group cohomology

Theorem 9.1. *There exist functors $H^q(G, -) : G{-}\mathsf{Mod} \to \mathbb{Z}{-}\mathsf{Mod}$ for $q \geq 0$ with the following properties:*

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

(ii) if $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$ is a short exact sequence, then it induces a long exact sequence

$$0 \to H^0(G, A) \xrightarrow{i_*} H^0(G, B) \xrightarrow{j_*} H^0(G, C) \xrightarrow{\delta} H^1(G, A) \xrightarrow{i_*}\to \cdots .$$

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

Moreover, such $H^q(G, -)$ are unique up to natural isomorphism.

This is a special case of derived functors.

Proof. For existence, let us take a free resolution

$$\cdots \xrightarrow{d_3} P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{\epsilon} \mathbb{Z} \to 0,$$

so that all P_i are free and the sequence is exact. Such a resolution exists, because for any G-module A, there exists a free G-module that surjects onto A.

Define a chain complex $K^i = \mathrm{Hom}_G(P_i, A)$. Then

$$K^0 = \mathrm{Hom}_G(P_0, A) \xrightarrow{d^1} K^1 = \mathrm{Hom}_G(P_1, A) \xrightarrow{d^2} K^2 = \mathrm{Hom}_G(P_2, A) \to \cdots ,$$

and let $H^i(G, A)$ be the cohomology of this complex,

$$H^i(G, A) = \ker d^{i+1} / \operatorname{im} d^i.$$

Let us verify that this satisfies the properties. We have

$$H^0(G, A) = \ker d^1 = \mathrm{Hom}_G(P_0 / \operatorname{im} d_1, A) = \mathrm{Hom}_G(\mathbb{Z}, A) = A^G.$$

If $0 \to A \to B \to C \to 0$ is a short exact sequence, for each q we have a short exact sequence

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

and so we have a short exact sequence of chain complexes. Then we can apply cohomology and get the long exact sequence. This long exact sequence is further natural in the sense that a morphism of short exact sequences induce a morphism of long exact sequences. Finally, if $A = \mathrm{Coind}^G(X)$, then

$$K^q = \mathrm{Hom}_G(P_q, \mathrm{Coind}^G) = \mathrm{Hom}_{\mathbb{Z}}(P_q, X).$$

Because P_q is a free $\mathbb{Z}$-module, this is exact.

Now let us show uniqueness of $H^q(G, A)$ by induction on q. First we see that the case $q = 0$ is given by the axiom. For $q > 0$, we are going to use dimension shifting. Let A be any G-module, and take a short exact sequence

$$0 \to A \to A' \to A^* \to 0$$

where A' is coinduced by A. This gives a long exact sequence

$$\cdots \to H^{q-1}(A') \xrightarrow{j^*}\to H^{q-1}(A^*) \to H^q(A) \to H^q(A') = 0 \to \cdots.$$

So $H^q(A)$ is the cokernel of $j^* : H^{q-1}(A') \to H^{q-1}(A^*)$ is determined by H^{q-1}. □

Example 9.2. Take $G = C_n = \langle t \rangle$. We can take the projective resolution

$$\cdots \to \mathbb{Z}[G] \xrightarrow{\times(t-1)} \mathbb{Z}[G] \xrightarrow{\times N} \mathbb{Z}[G] \xrightarrow{\times(t-1)} \mathbb{Z}[G] \xrightarrow{t \mapsto 1} \mathbb{Z} \to 0.$$

Then our chain complex is

$$0 \to A \xrightarrow{\times(t-1)} A \xrightarrow{\times N} A \xrightarrow{\times(t-1)} A \to \cdots$$

and we can now compute cohomology. We have

$$\begin{aligned} H^0(G, A) &= \ker(t-1) = A^G, \\ H^{2q-1}(G, A) &= \ker(N)/(t-1)A = \ker(N)/I_G A, \\ H^{2q}(G, A) &= \ker(t-1)/\operatorname{im}(N) = A^G/NA. \end{aligned}$$

If we extend to Tate cohomology, all the odd things will be the same and all the even things will be the same.

9.2 Standard bar resolution

Let G be any group and let $P_i = \mathbb{Z}[G^{i+1}] = \mathbb{Z}[G]$ be the formal span of tuples $(g_0, \ldots, g_i) \in G^{i+1}$. Let us make this a G-module by a diagonal action $g(g_0, \ldots, g_i) = (gg_0, \ldots, gg_i)$. Then this is a free $\mathbb{Z}[G]$-module with basis $(1, g_1, \ldots, g_i)$. Define

$$d_i : P_i \to P_{i-1}; \quad d_i(g_0, \ldots, g_i) = \sum_j (-1)^j (g_0, \ldots, \hat{g}_j, \ldots, g_i).$$

We can easily check that $d_{i-1}d_i = 0$. To show exactness, suppose that some linear combination of $(g_0, \dots, g_i)$ is in $\ker d_i$. If we put an arbitrary $s \in G$ in front of every such tuple, then we check

$$d_{i+1}(s, g_0, \dots, g_i) = (g_0, \dots, g_i) - (s, d_i(g_0, \dots, g_i)).$$

So this is going to be in the image.

Now we have

$$H^q(G, A) = \frac{\ker(d^{q+1} : \mathrm{Hom}_G(P_q, A) \to \mathrm{Hom}_G(P_{q+1}, A))}{\mathrm{im}(d^q : \mathrm{Hom}_G(P_{q-1}, A) \to \mathrm{Hom}_G(P_q, A))}.$$

We can interpret $\mathrm{Hom}(P_q, A)$ as **homogeneous cohains** $\tilde{C}_q(A)$, as maps $f : G^{i+1} \to A$ such that

$$f(gg_0, \dots, gg_i) = gf(g_0, \dots, g_i).$$

The kernel of d^{q+1} are homogeneous cocyles and the image of d^q are homogeneous boundaries.

But this is a cumbersome condition, and we can make a change of variables. For example, take $q = 1$. The function $f : G \to A$ in $\tilde{C}_0(A)$ is determined by $f(1) = a \in A$. The function $f : G^2 \to A$ that satisfy $f(gg_0, gg_1) = gf(g_0, g_1)$ is determined by $f(1, g) = \varphi(g)$. So the boundary map is

$$d^1 : \tilde{C}_0 \to \tilde{C}_1; \quad a \mapsto ((1, g) \mapsto a - ga).$$

That is, the image is $\varphi(g) = a - ga$. These are the inhomogeneous 1-coboundaries. For $q = 2$, we are going to let $(g_0, g_1, g_2) = (1, g, gh)$. Then the coboundary map is

$$d^2 : \varphi \mapsto ((g, h) \mapsto g\varphi(h) - \varphi(gh) + \varphi(g)).$$

10 October 3, 2017

The plan for today is to continue on ways to compute group cohomology. Last time we defined homogeneous cochains

$$\tilde{C}^i(G,A) = \{(f : G^{i+1} \to A) : f(gg_0, \dots, gg_n) = gf(g_0, \dots, g_n)\}.$$

The differentials are defined as

$$d : \tilde{C}^i(G,A) \to \tilde{C}^{i+1}(G,A);$$
$$f \mapsto (df : (g_0, \dots, g_{i+1}) \mapsto f(g_1, \dots, g_{i+1}) - f(g_0, g_2, \dots, g_{i+1}) + \cdots).$$

This is now very explicitly defined.

We are now going to change variables. **Inhomogeneous cochains**

$$C^i(G,A) = \{\varphi : G^i \to A\}$$

and identify with $\tilde{C}^i(G,A)$ via

$$\tilde{C}^i(G,A) \to C^i(G,A); \quad f \mapsto (\varphi : (g_1, \dots, g_i) \mapsto f(1, g_1, g_1g_2, \dots, g_1 \cdots g_i)).$$

Through this bijection, we get the differentials

$$d^i : C^i(G,A) \to C^{i+1}(G,A),$$

which maps $\varphi \in C^i(G,A)$ to

$$d^i\varphi(g_1, \dots, g_{i+1}) = g_1\varphi(g_2, \dots, g_{i+1}) - \varphi(g_1g_2, g_3, \dots, g_{i+1}) + \varphi(g_1, g_2g_3, \dots, g_{i+1})$$
$$- \cdots + (-1)^i\varphi(g_1, \dots, g_{i-1}, g_ig_{i+1}) + (-1)^{i+1}\varphi(g_1, \dots, g_i).$$

10.1 Explicit descriptions of cohomology

We can use these efficient cochains to compute the cohomologies. We have

$$d^0 : C^0(G,A) \to C^1(G,A); \quad a \mapsto (\varphi : g \mapsto ga - a).$$

Then the next differential is

$$d^1 : C^1(G,A) \to C^2(G,A); \quad \varphi \mapsto ((g_1, g_2) \mapsto g_1\varphi(g_2) - \varphi(g_1g_2) + \varphi(g_1)),$$

and the next one is

$$d^2 : C^2(G,A) \to C^3(G,A);$$
$$\varphi \mapsto ((g_1, g_2, g_3) \mapsto g_1\varphi(g_2, g_3) - \varphi(g_1g_2, g_3) + \varphi(g_1, g_2g_3) - \varphi(g_1, g_2)).$$

From this, we can immediately read

$$H^1(G,A) \cong \frac{\{(\varphi : G \to A) : \varphi(g_1g_2) = \varphi(g_1) + f_1\varphi(g_2)\}}{\{(\varphi_a : G \to A) : \varphi_a(g) = ga - a\}}.$$

These φ satisfying $\varphi(g_1g_2) = \varphi(g_1) + g_1\varphi(g_2)$ are called **crossed homomorphisms**. If G acted on A trivially, this would just be $\varphi(g_1g_2) = \varphi(g_1) + \varphi(g_2)$. Then we are quotienting out by nothing, so

$$H^1(G,A) = \mathrm{Hom}_{\mathsf{Grp}}(G,A).$$

Definition 10.1. If G is a group and A is a G-module, we define the **semidirect product** $G \ltimes A = G \times A$ with multiplication

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

This is a group, and fits in the short exact sequence

$$0 \to A \to G \ltimes A \to G \to 0.$$

Now we can interpret $Z^1(G, A)$ as a splitting of this exact sequence, i.e., sections of $G \ltimes A \to G$. This is because the map

$$G \to G \ltimes A; \quad g \mapsto (g, \varphi(g))$$

is a group homomorphism if and only if φ is a crossed homomorphism.

On the other hand, φ_1 and φ_2 are equivalent modulo $B^1(G, A)$ if and only if the splittings $G \to G \ltimes A$ are conjugate by some element of A.

These is a similar interpretation for $H^2(G, A)$. This classifies short exact sequences of groups

$$0 \to A \to X \to G \to 0,$$

such that the G-action on A by conjugation agrees with the G-module structure. Here, $0 \in H^2$ corresponds to $0 \to A \to G \ltimes A \to G \to 0$. The idea is that given such an X, take a section (as a set) $s : G \to X$ and compare $s(gh)$ and $s(g)s(h)$. This lies in the kernel, so there exists a unique $\varphi(g, h)$ such that

$$s(gh) = \varphi(g, h)s(g)s(h).$$

This is a cocycle, after using associativity.

Recall that if we have a short exact sequence of G-modules $0 \to A \xrightarrow{i} B \xrightarrow{j} C \to 0$, we get a connecting homomorphism

$$H^0(G, C) \to H^1(G, A).$$

This can be described explicitly with cocycles. If $c \in C^G$, choose $b \in B$ with $j(b) = c$ and then

$$g \mapsto gb - b \in A$$

is an element of $Z^1(G, A)$. This is well-defined up to elements like $ga - a$, which is $B^1(G, A)$. So we get this boundary map.

10.2 The first cohomology and torsors

Let A be an abelian group.

Definition 10.2. An A**-torsor** is a set X with a simply transitive action of A. (Simple means that stabilizers are trivial.)

Now let A be a G-module.

Definition 10.3. An **A-torsor** is a G-set X such that X is an A-torsor in the previous sense and

$$g(a+x) = ga + gx.$$

(If you want to use multiplication as the action, use ${}^g(ax) = ({}^g a)({}^g x)$.)

A is an A-torsor. If A is just a group, then every A-torsor is isomorphic to A as sets non-canonically.

Example 10.4. Suppose L/K is a field extension, and suppose that $\mu_n \subseteq L$. Let $A = \mu_n(L)$. For any $c \in (L^\times)^n$, let

$$X = \{a \in L : a^n = c\}.$$

Then this is a torsor for $A = \mu_n(L)$. We can also bring in a group $G = \operatorname{Gal}(L/K)$. If $c \in (K^\times)^n$ then the G-action is trivial. But we can also imagine a situation in which $\mu_n(L) \subseteq K$ but c has no nth roots in K. Then G acts trivially on A but not on X.

Theorem 10.5. *$H^1(G,A)$ classifies A-torsors with the G-action.*

Proof. I will construct maps in both directions. Given $[\varphi] \in H^1(G,A)$, we can construct a torsor X with $X = A$ as a set but with G-action

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

This really is a group action because

$$g *_\varphi (h *_\varphi x) = g(hx + \varphi(h)) + \varphi(g) = ghx + g\varphi(h) + \varphi(g) = (gh)x + \varphi(gh).$$

Now we want a map from A-torsors to $H^1(G,A)$. Given X an A-torsor, choose an element $x_0 \in X$ and define

$$g(x_0) = \varphi(g) + x_0.$$

It can be checked that $\varphi \in Z^1(G,A)$, and if we replace x_0 by $a + x_0$, then

$$g(a+x_0) = g(a) + g(x_0) = (ga - a) + \varphi(g) + (a + x_0).$$

This gives a map to $H^1(G,A)$. □

Using torsors, there is another way of describing the connecting homomorphism $H^0(G,C) = C^G \to H^1(G,A)$. For $c \in C^G$, the set $j^{-1}(c) \subseteq B$ is an A-torsor. The class of this torsor gives the connecting morphism.

Example 10.6. In the short exact sequence

$$0 \to \mu_n(L) \to L^\times \xrightarrow{j} (L^\times)^n \to 0,$$

$j^{-1}(c)$ is the nth roots of c.

10.3 Group homology

Recall we have the functor $G{-}\mathsf{Mod} \to \mathbb{Z}{-}\mathsf{Mod};\ A \mapsto A_G$. This is defined as

$$A_G = A/I_G A = A/(ga - a) = A \otimes_G \mathbb{Z}.$$

This is right exact but not left exact.

Definition 10.7. There exist homology functors $H_q(G, A)$ for $q \geq 0$, satisfying

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

(b) $H_q(G, A) = 0$ for $q \geq 1$ if A is induced,

(c) if $0 \to A \to B \to C \to 0$ is a short exact sequence, there is a long exact sequence

$$\cdots \to H_1(G, B) \to H_1(G, C) \to H_0(G, A) \to H_0(G, B) \to H_0(G, C) \to 0.$$

The proof of this is virtually identical. Take a flat (free) resolution

$$\cdots \to F_2 \to F_1 \to F_0 \to \mathbb{Z} \to 0$$

and take the homology of

$$\cdots \to F_2 \otimes_G A \to F_1 \otimes_G A \to F_0 \otimes_G A \to 0.$$

Uniqueness is again by dimension shifting.

11 October 5, 2017

Last time we defined group homology by

(a) $H_0(G,A) = A_G = A/I_GA$,

(b) $H_q(G,A) = 0$ for $q \geq 1$ if G is induced,

(c) a short exact sequence gives a long exact sequence.

We can construct it as the homology of the free resolution of $\mathbb{Z}$ tensored with A. So we can use the standard resolution to get explicit descriptions. Class field theory only uses a limited range of (co)homology groups, H^0, H^1, H^2, $\hat{H}^0$, $\hat{H}^{-1}$, H_0, H_1.

Theorem 11.1. *We have* $H_1(G,\mathbb{Z}) \cong I_G/I_G^2 = G^{\mathrm{ab}}$.

Proof. We use the short exact sequence

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

of G-modules. This gives a long exact sequence

$$H_1(G,\mathbb{Z}[G]) = 0 \to H_1(G,\mathbb{Z}) \to H_0(G,I_G) = I_G/I_G^2 \xrightarrow{0} H_0(G,\mathbb{Z}[G]) = \mathbb{Z}[G]/I_G.$$

So we get $H_1(G,\mathbb{Z}) \cong H_0(G,I_G) = I_G/I_G^2$. For the next isomorphism, write $a_g = g-1$. Note that I_G^2 is spanned by

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

This shows that I_G/I_G^2 is generated by a_g, with relations $a_{gh} = a_g + a_h$. This is precisely G^{ab}. □

Let $H \subseteq G$. There is a short exact sequence

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

of H-modules. Also $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module. So

$$\begin{aligned} H_1(H,\mathbb{Z}[G]) = 0 &\to H_1(H,\mathbb{Z}) \\ &\to H_0(H,H_G) = I_G/I_GI_H \to H_0(H,\mathbb{Z}[G]) = \mathbb{Z}[G]/I_H\mathbb{Z}[G]. \end{aligned}$$

This shows that

$$H_1(H,\mathbb{Z}) = \ker(I_G/I_GI_H \to \mathbb{Z}[G]/I_H\mathbb{Z}[G]) = I_H\mathbb{Z}[G]/I_GI_H.$$

It is a good exercise to check that this is just I_H/I_H^2.

11.1 Changing the group

Both the functors $H_i(G, A)$ and $H^i(G, A)$ depend on G and A. These are covariant functors of A. H_i is also going to be covariant in G, and H^i will be contravariant in G.

Definition 11.2. Two pairs (G, A) and (G', A') are **compatible for cohomology** if there exist morphisms $\rho : G' \to G$ and $\lambda : A \to A'$ such that

$$\lambda(\rho(g'), a) = g'\lambda(a).$$

Example 11.3. If $G' = H \subseteq G$ is a subgroup, then we can set $\rho = i : H \hookrightarrow G$ and $\lambda = \mathrm{id}_A$.

Example 11.4. If $H \subseteq G$ is a normal subgroup, then $\rho : G \to G/H$ and $\lambda : A^H \to A$ gives a map from (G, A) to $(G/H, A^H)$.

Then ρ maps

$$\rho_* : P_q(G') = \mathbb{Z}[(G')^{q+1}] \to P_q(G) = \mathbb{Z}[G^{q+1}].$$

This gives a map

$$\mathrm{Hom}_G(P_q(G), A) \to \mathrm{Hom}_{G'}(P_q(G'), A')$$

of cochain complexes. So we get maps on homology

$$\rho^* : H^q(G, A) \to H^q(G', A').$$

This can be described explicitly in homogeneous cochains. It sends $[\varphi]$ to $[\varphi']$ where

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

Example 11.5. If (G, A) and (H, A) are compatible by (i, id_A), then this induces **restriction**

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

is just done by restricting the function.

Example 11.6. Consider (G, A) and $(G/H, A^H)$. This gives the **inflation** map

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

which is done by replacing ϕ by $\mathrm{Inf}\,\phi(g_1, \dots, g_q) = \phi(g_1H, \dots, g_qH)$.

One thing we see is that

$$\mathrm{Res} \circ \mathrm{Inf} = 0$$

for $q \geq 1$, because this is induced by $(G/H, A^H)$ and (H, A) with the map of groups being trivial.

Definition 11.7. For pairs (G, A) and (G', A'), a **compatible map for homology** is $\rho : G \to G'$ and $\lambda : A \to A'$ such that $\lambda(ga) = \rho(g)\lambda(a)$.

Example 11.8. For $H \subseteq G$ a subgroup, there is a map from (H, A) to (G, A). For $H \subseteq G$ a normal subgroup, there is $(G, A) \to (G/H, A_H)$.

As before, compatible maps give induced homomorphisms $H_q(G, A) \to H_q(G', A')$. So there is the **corestriction**

$$\mathrm{coRes} : H_q(H, A) \to H_q(G, A)$$

and **coinflation**

$$\mathrm{Coinf} : H_q(G, A) \to H_q(G/H, A_H).$$

The functors Res and coRes are compatible with long exact sequence maps. If $0 \to A \to B \to C \to 0$ is a short exact sequence of G-modules, the long exact sequence for $H^q(H, -)$ and $H^q(G, -)$ commute with the restriction maps. Likewise, the long exact sequence for homology commute with corestriction.

Also note that Res is completely determined by the property that Res : $A^G \to A^H$ and compatibility with the long exact sequence, using dimension shifting.

$$\begin{tikzcd}
0 \arrow[r] & H^q(G, \ldots) \arrow[r, "\cong"] \arrow[d, "\mathrm{Res}"] & H^{q+1}(G, \ldots) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & H^q(H, \ldots) \arrow[r, "\cong"] & H^{q+1}(H, \ldots) \arrow[r] & 0
\end{tikzcd}$$

That is, this is a "universal δ-functor". Later, we will define

$$\mathrm{Res} : \hat{H}^q(G, A) \to \hat{H}^q(H, A), \quad \mathrm{coRes} : \hat{H}^q(H, A) \to \hat{H}^q(G, A)$$

for all $q \in \mathbb{Z}$ by dimension shifting.

11.2 Inflation-restriction exact sequence

Let $H \lhd G$ be a normal subgroup. If $q \geq 1$, we can look at the sequence

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

Is this exact?

Theorem 11.9. *The sequence*

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

is exact.

In general, there is a spectral sequence for higher degree, but we are going to just do this explicitly.

Proof. First let us prove that $\mathrm{Inf} : H^1(G/H, A^H) \to H^1(G, A)$ is injective. Suppose $[\varphi] \in \ker \mathrm{Inf}$, so that $\varphi(gH) = ga - a$ for all $g \in G$. Now we have $\varphi(H) = ha - a$, which is constant for all $h \in H$. So $a \in A^H$ and $\varphi \in B^1(G/H, A^H)$.

Now we need to prove $\ker \operatorname{Res} \subseteq \operatorname{im} \operatorname{Inf}$. Take $\phi \in Z^1(G,A)$ such that $\operatorname{Res} \varphi \in B^1(H,A)$. Then $\phi(h) = ha - a$ for some $a \in A$. But φ is living in $H^1(G,A)$, so we can subtract $g \mapsto (ga - a)$ from ϕ and take this as ϕ instead. Then $\phi(h) = 0$ for all $h \in H$. Now

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

for all $g \in G$ and $h \in H$. So ϕ is defined on G/H and

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

That is, ϕ maps to A^H. This shows that ϕ comes from a crossed homomorphism $G/H \to A^H$. □

Proposition 11.10. *Suppose $H^i(H,A) = 0$ for $1 \leq i < q$. Then there exists an exact sequence*

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

Proof. This goes by dimension shifting. If $q = 1$, we already know this. Now suppose we know this for $q-1$. Let A be a G-module satisfying the above, and let $A^* = \operatorname{Coind}^G(A)$ so that $A \hookrightarrow A^*$. Then we have a short exact sequence

$$0 \to A \to A^* \to A' \to 0.$$

Because A^* is coinduced as a G-module, it is also coinduced as a H-module. This is because $\mathbb{Z}[G]$ is a free $\mathbb{Z}[H]$-module. So

$$\begin{tikzcd}
H^{q-1}(G,A') \arrow[r, "\cong"] \arrow[d] & H^q(G,A) \arrow[d] \\
H^{q-1}(H,A') \arrow[r, "\cong"] & H^q(H,A).
\end{tikzcd}$$

If we further take H-invariants of our short exact sequence. Here, we get

$$0 \to A^H \to (A^*)^H \to (A')^H \to H^1(A,H) = 0.$$

So we get an compatible

$$\begin{tikzcd}
H^{q-1}(G/H,(A')^H) \arrow[r, "\cong"] \arrow[d, "\operatorname{Inf}"] & H^q(G/H,A^H) \arrow[d, "\operatorname{Inf}"] \\
H^{q-1}(G,(A')^H) \arrow[r] & H^q(G,A^H).
\end{tikzcd}$$

But A' satisfies $H^i(G,A') = H^{i+1}(G,A) = 0$ for $i < q-1$. So you can dimension shift. □

12 October 10, 2017

Today we are going to define Tate cohomology.

12.1 Tate cohomology

We have defined $H^q(G,A)$ and $H_q(G,A)$ for $q \geq 0$. We will define

$$\hat{H}^q(G,A) = \begin{cases} H^q(G,A) & q \geq 1 \\ H_{-1-q}(G,A) & q \leq -2 \end{cases}$$

and we will fill in the module. These are called **Tate cohomology**. We are going to focus only on finite groups G.

For G finite, we have this operator $N = \sum_{g \in G} g \in \mathbb{Z}[G]$, and sends

$$N : A \to A; \quad a \mapsto Na = \sum_{g \in G} ga.$$

Then $\operatorname{im} N \subseteq A^G$ and $\ker N \supseteq I_G A$. So we actually have a map $N^* : A_G \to A^G$. This allows to define

$$\hat{H}^{-1}(G,A) = \ker(N^* : A_G \to A^G), \quad \hat{H}^0(G,A) = \operatorname{coker}(N^* : A_G \to A^G).$$

Because we have

$$\begin{tikzcd}
\cdots \arrow[r] & H_1(G,C) \arrow[r] & A_G \arrow[r] \arrow[d, "N_A^*"] & B_G \arrow[r] \arrow[d, "N_B^*"] & C_G \arrow[r] \arrow[d, "N_C^*"] & 0 & \\
& 0 \arrow[r] & A^G \arrow[r] & B^G \arrow[r] & C^G \arrow[r] & H^1(G,A) \arrow[r] & \cdots .
\end{tikzcd}$$

Then a standard application of the snake lemma gives

$$\cdots \to \hat{H}^{-2}(G,C) \to \hat{H}^{-1}(G,A) \to \hat{H}^{-1}(G,B) \to \hat{H}^{-1}(G,C)$$
$$\to \hat{H}^0(G,A) \to \hat{H}^0(G,B) \to \hat{H}^0(G,C) \to \hat{H}^1(G,A) \to \cdots .$$

Proposition 12.1. *For A a G-module that is induced (or equivalently, coinduced), $\hat{H}^q(G,A) = 0$ for all q.*

Proof. We know this except for $q = 0$ and q. So it suffices to show that $N^* : A_G \to A^G$ is an isomorphism. Suppose $A = \bigoplus_{g \in G} gX$ where $X \subseteq A$ is a $\mathbb{Z}$-submodule. We claim that both A_G and A^G are isomorphic to X. An element $\sum_g gx_g$ is in A^G if and only if all x_g are equal in X. So we get an isomorphism

$$X \to A^G; \quad x \mapsto \sum_{g \in G} gx.$$

Conversely, we have a map

$$A_G \to X; \quad \sum_g gx_g \mapsto \sum_g x_g.$$

These two are isomorphisms and N^* is just the composite. □

There is a slightly different perspective on how to splice these sequences. Let

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

be a (finite rank) free resolution. Then we can dualize and get

$$0 \to \mathbb{Z} \to \mathrm{Hom}(P_0, \mathbb{Z}) = P^{-1} \to \mathrm{Hom}(P_1, \mathbb{Z}) = P^{-2} \to \cdots .$$

This is still exact because all objects are free $\mathbb{Z}$-modules. Now we can compose these can get a complete resolution

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

Now we can define

$$\hat{H}^q(G, A) = H^q(K^\bullet = \mathrm{Hom}_G(P_\bullet, A)).$$

To show this for $q \geq 0$, we only need to check that

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

This is done by noticing that $\mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_{\mathbb{Z}}(P_q, \mathbb{Z}), A) \cong P_i \otimes_{\mathbb{Z}} A$. Then if we take the G-invariants of both side, the left hand side is what we want, and the right hand side is $(P_i \otimes_{\mathbb{Z}} A)^G \cong (P_i \otimes_{\mathbb{Z}} A)_G = P_i \otimes_G A$.

Example 12.2. Let $G = C_n = \langle t : t^n = 1 \rangle$. Recall that we have the projective resolution

$$\cdots \to \mathbb{Z}[G] \xrightarrow{\times(t-1)} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \xrightarrow{\times(t-1)} \mathbb{Z}[G] \xrightarrow{\epsilon} \mathbb{Z} \to 0.$$

Now dualizing gives

$$0 \to \mathbb{Z} \xrightarrow{1 \mapsto N} \mathbb{Z}[G] \xrightarrow{\times(t^{-1}-1)} \mathbb{Z}[G] \xrightarrow{N} \mathbb{Z}[G] \to \cdots .$$

So we can put them together to get

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

Thus

$$\hat{H}^{2q} = A^G/NA, \quad \hat{H}^{2q-1} = (\ker N)/I_G A.$$

12.2 Restriction and corestriction

We have defined restriction for cohomology and corestriction for homology. These are defined for

$$\operatorname{Res} : \hat{H}^q(G,A) \to \hat{H}^q(H,A) \text{ for } q \geq 1, \quad \operatorname{coRes} : \hat{H}^q(H,A) \to \hat{H}^q(G,A) \text{ for } q \leq -2.$$

We want these for all $q \in \mathbb{Z}$.

We can construct these by dimension shifting. If we define A^+ as the cokernel of $A \to \operatorname{coInd}^G(A)$, then we get a short exact

$$0 \to A \to \operatorname{coInd}^G(A) \to A^+ \to 0.$$

Then we have $\hat{H}^{q+1}(G,A) \cong \hat{H}^q(G,A^+)$. So if Res^{q+1} are already defined, we can define Res^q by

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

We can likewise define coRes_q for $q \in \mathbb{Z}$ by upwards induction. Both of these are functors, and are compatible with long exact sequences. Note that the only thing we needed is that Res_0 is $A^G \to A^H$ and $\operatorname{coRes}_0 = A_H \to A_G$. After that, we have only used dimension shifting.

Let us just look at how the map

$$\operatorname{Res}_{-1} : \hat{H}^{-1}(G,A) \to \hat{H}^{-1}(H,A)$$

is defined. This is induced by the map

$$N'_{G/H} : A_G \to A_H; \quad [a] \mapsto \sum_{g \in G/H} [g^{-1}a].$$

Proof. It is enough to show that if $0 \to A \to B \to C \to 0$ is a short exact sequence,

$$\begin{tikzcd}
\hat{H}^{-1}(G,C) \arrow[r, "\delta"] \arrow[d, "N'_{G/H}"] & \hat{H}^0(G,A) \arrow[d, "\operatorname{Res}_0"] \\
\hat{H}^{-1}(H,C) \arrow[r, "\delta"] & \hat{H}^0(H,A)
\end{tikzcd}$$

commutes. Let $b \mapsto c$. An element $[c] \in \hat{H}^{-1}(G,C)$ maps to $[Nb] \in A^G/\operatorname{im} N^*$ in $\hat{H}^0(G,A)$, and this maps to $N_G b = \sum_{g \in G} gb$. On the other hand $[c]$ maps downwards to $\sum_{g \in H \backslash G} [gc]$ and this maps to

$$\sum_{g \in H \backslash G} N_H(gb) = \sum_{g \in H \backslash G} \sum_{h \in H} hgb = \sum_{g \in G} gb.$$

So the diagram commutes. □

Likewise,

$$\mathrm{coRes}_0 : \hat{H}^0(H, A) \to \hat{H}^0(G, A)$$

comes from the map

$$N_{G/H} : A^H \to A^G; \quad a \mapsto \sum_{g \in G/H} ga.$$

Proposition 12.3. *For all q, we have*

$$\hat{H}^q(G, A) \xrightarrow{\mathrm{Res}_q} \hat{H}^q(H, A) \xrightarrow{\mathrm{coRes}_q} \hat{H}^q(G, A).$$

The composite is multiplication by $[G : H]$.

Proof. By dimension shifting, it suffices to show this for $q = 0$. The groups are

$$A^G/N_G A \xrightarrow{\mathrm{Res}} A^H/N_H A \xrightarrow{\mathrm{coRes}} A^G/N_G A.$$

This comes from $a \mapsto a \mapsto \sum_{g \in G/H} ga = [G : H]a$. □

Corollary 12.4. *If $|G| = n$, then $\hat{H}^q(G, A)$ are n-torsion.*

Proof. We that $\hat{H}^q(G, A) \to \hat{H}^q(\{1\}, A) \to \hat{H}^q(G, A)$ is multiplication by n. But $\hat{H}^q(\{1\}, A) = 0$. □

Corollary 12.5. *For G finite and A a finitely generated $\mathbb{Z}[G]$-module, $\hat{H}^q(G, A)$ is also finite.*

Proof. This is because $\hat{H}^q(G, A)$ is finitely generated by the explicit description. Then it is torsion, so it is finite. □

Corollary 12.6. *If $|G| = n$ and if $n : A \to A$ is an isomorphism, then $\hat{H}^q(G, A) = 0$.*

Proof. Then $n : \hat{H}^q(G, A) \to \hat{H}^q(G, A)$ is an isomorphism. □

Corollary 12.7. *If G_p is a Sylow p-subgroup of G, then*

$$\mathrm{Res} : (\hat{H}^q(G, A))_p \to \hat{H}^q(G_p, A)$$

is injective.

Proof. The map $\mathrm{coRes} \circ \mathrm{Res} : (\hat{H}^q(G, A))_p \to (\hat{H}^q(G, A))_p$ is injective. □

Corollary 12.8. *If $\hat{H}^q(G_p, A) = 0$ for all p, then $\hat{H}^q(G, A) = 0$.*

13 October 12, 2017

13.1 Cup products

If A and B are G-modules, there exists a map

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

for $p, q \geq 0$, and if G is finite, there is a map

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

for all $p, q \in \mathbb{Z}$. This satisfy the axioms:

- The product is natural in both A and B.
- If $p, q = 0$, the map is $\smile : A^G \times B^G \to (A \times B)^G$; $a \smile b = a \otimes b$.
- This is compatible with exact sequences. That is, if $0 \to A \to A' \to A'' \to 0$ is an exact sequence such that $0 \to A \otimes B \to A' \otimes B \to A'' B \to 0$ is also exact, then for $a'' \in H^p(G, A'')$ and $b \in H^q(G,B)$
$$\delta(a'' \smile b) = (\delta a'') \smile b.$$

This axioms uniquely determine the cup product on $\hat{H}$, and the proof is by dimension-shifting. (This is in the Bonn lectures of Neukirch.) You can also explicitly construct this using resolutions.

There are explicit formulas for the cup product. Let $f \in C^p(G,A)$ and $g \in C^q(G,B)$ be homogeneous cochains. Then

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

If $\varphi \in C^p(G,A)$ and $g \in C^q(G,B)$ are inhomogeneous cochains, then

$$(\varphi \smile \psi)(g_1, \dots, g_{p+q}) = \varphi(g_1, \dots, g_p) \otimes g_1 \cdots g_p \psi(g_{p+1}, \dots, g_{p+q}).$$

Cassels and Frölich wirte down explicit formulas in all dimensions. The Bonn lectures do some explicit computations in small dimensions.

Cup product satisfies

- $(a \smile b) \smile c = a \smile (b \smile c)$ under the identification $(A \otimes B) \otimes C \cong A \otimes (B \otimes C)$.
- $a \smile b = (-1)^{pq} b \smile a$ under $A \otimes B \cong B \otimes A$.
- $\operatorname{Res}(a \smile b) = (\operatorname{Res} a) \smile (\operatorname{Res} b)$.
- $\operatorname{coRes}(a \smile \operatorname{Res} b) = \operatorname{coRes}(a) \smile b$.

To prove this, check for $p = q = 0$ and then dimension shift. For instance, the last formula is, for $a \in A^H$ and $b \in B^G$,

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

For $p = 0$ and q arbitrary, the map

$$a \smile - : H^q(G,B) \to H^q(G, A \otimes B)$$

is just tensoring with a.

13.2 Galois cohomology

Let L/K be any Galois extension of local fields. We are going to use the notation

$$H^q(L/K, A) = H^q(\mathrm{Gal}(L/K), A).$$

This is called Galois cohomology, and we are going to use $A = L^\times$ and $A = \mathbb{Z}$ normally.

The group $H^2(L/K, L^\times)$ is called the **Brauer group** of L/K, and we are going to get an explicit isomorphism

$$H^2(L/K, L^\times) \xrightarrow{\cong} \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}$$

where $n = [L : K]$. Now there is the preferred generator $\frac{1}{n}$ on the right hand side, and we will call the preimage $u_{L/K}$. This will give a cup product

$$- \smile u_{L/K} : \hat{H}^{-2}(L/K, \mathbb{Z}) \to \hat{H}^0(L/K, L^\times).$$

Note that the left hand side is just the abelianization $\mathrm{Gal}(L/K)^{\mathrm{ab}}$. But the right hand side is $K^\times/NL^\times$. This map is what we call the **Artin map**. To get this, we will need to compute some Galois cohomology.

Let L/K be a finite extension. For motivation, I can ask, what is $\hat{H}^q(L/K, L^+)$? Does this have any interesting Galois cohomology? The answer is no, because L^+ is an induced $\mathrm{Gal}(L/K)$-module. This follows from the following theorem.

Theorem 13.1 (Normal basis theorem)**.** *There exists a $x \in L$ such that $\{gx\}_{g\in\mathrm{Gal}(L/K)}$ is a basis for L as a K-vector space.*

However multiplicative group is more interesting. We are mainly going to talk about the second cohomology, but what about H^1?

Theorem 13.2 (Hilbert 90)**.** *$H^1(L/K, L^\times) = 0$.*

Proof. We use inhomogeneous cochains. Suppose that $\varphi \in Z^1(L/K, L^\times)$ so that $\varphi(gh) = \varphi(g) \cdot g\varphi(h)$. We need to show that there exists some $a \in L^\times$ such that $\varphi(g) = a/ga$. Let $x \in L$, and we are going to let

$$a = \sum_{g\in G} \phi(g) \cdot gx \neq 0.$$

We can choose x so that $a \neq 0$, by linearly independence of characters. Now

$$\begin{aligned} a &= \sum_{g'\in G} \varphi(g') \cdot g'x = \sum_{gg'\in G} \varphi(gg') \cdot (gg'x) \\ &= \sum_{g'\in G} \varphi(g) \cdot g\varphi(g') \cdot gg'x = \varphi(g) \sum_{g'\in G} g(\varphi(g') \cdot g'x) = \varphi(g) \cdot ga. \end{aligned}$$

□

Here is the original Hilbert 90. Let L/K be a cyclic extension and let $\mathrm{Gal}(L/K) = \langle g \rangle$. Then we have

$$H^1(L/K, L^\times) = \frac{\ker(N : L^\times \to L^\times)}{\mathrm{im}(g-1 : L^\times \to L^\times;\, x \mapsto gx/x)}.$$

So the theorem is saying that if $x \in L^\times$ with $Nx = 1$, then there exists a $y \in L^\times$ such that $x = gy/y$.

Example 13.3. Here is a nice application. Suppose $L = \mathbb{Q}(i)/K = \mathbb{Q}$ and let $x \in \mathbb{Q}(i)$ be such that $Nx = 1$. That is, x is on the unit circle. Then there exists a $y \in \mathbb{Q}(i)$ such that $x = \bar{y}/y$. If we write $y = a + bi$, then

$$x = \frac{a+bi}{a-bi} = \frac{(a^2-b^2)+2abi}{a^2+b^2}.$$

This parametrizes Pythagorean triples.

13.3 Cohomology of profinite groups

Let's say that G is a group. Recall that G is **profinite group** if it can be written as $\varprojlim_{i\in I} G_i$ with each G_i finite. For example,

$$\mathrm{Gal}(\overline{K}/K) = \varprojlim_{L/K \text{ finite}} \mathrm{Gal}(L/K)$$

is profinite. We can give a natural topology on G by setting $\ker(G \to G_i)$ as the neighborhood basis at 1.

Theorem 13.4. *A topological group G is profinite if and only if G is compact and totally disconnected. G is profinite if and only if $G = \varprojlim G/U$ where U runs over open finite index subgroups of G.*

So an open subgroup $U \subseteq G$ necessarily has finite index.

Definition 13.5. A **discrete G-module** A is a $\mathbb{Z}$-module A (with the discrete topology) with a group action $G \times A \to A$ such that this map is continuous, or equivalently, all stabilzers are open in G, or equivalently,

$$A = \bigcup_{U \subseteq G \text{ open}} A^U.$$

Let $U \subseteq G$ be open and normal. If $V \subseteq U$, we can inflate

$$\mathrm{Inf}_{U,V} : H^q(G/U, A^U) \to H^q(G/V, A^V).$$

Then we have

$$H^q(G, A) = \varinjlim_{U \lhd G} H^q(G/U, A^U).$$

For any K, we write $H^i(K, A) = H^i(\mathrm{Gal}(\overline{K}/K), A)$. This is

$$H^i(K, A) = \varinjlim_{L/K \text{ finite Galois}} H^i(\mathrm{Gal}(L/K), A).$$

In particular, we have

$$H^1(K, \overline{K}^\times) = \varinjlim_{L/K \text{ finite Galois}} H^1(L/K, L^\times) = 0.$$

This is now a profinite form of Hilbert 90.

Because direct limit commute with exactness, we still have our long exact sequences. We can also define cohomology in terms of continuous cochains. A map $\varphi : G^n \to A$ is continuous if and only if it factors as

$$\varphi : G^n \to (G/U)^n \to A$$

for some open subgroup U. Inflation and restriction also works for $H \subseteq G$ closed. We don't have Tate cohomology because the groups are not finite, but we do have cup products.

14 October 17, 2017

For K any field, we can look at the separable closure K^{sep}. This is just $\overline{K}$ if $\operatorname{char} K = 0$. This what we should use if we want to do Galois theory.

Definition 14.1. If A is a $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$-module, then

$$H^q(K, A) = H^q(\mathrm{Gal}(K^{\mathrm{sep}}/K), A).$$

Now the correct Hilbert theorem 90 is

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

14.1 Kummer theory

Let n be an integer relatively prime to $\operatorname{char} K$. There is a short exact sequence of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-modules

$$0 \to \mu_n(K^{\mathrm{sep}}) \to (K^{\mathrm{sep}})^\times \xrightarrow{n} (K^{\mathrm{sep}})^\times \to 0,$$

where the last map is surjective because K^{sep} has all n-th roots because $x^n - a$ is always irreducible for $a \neq 0$. The associated long exact sequence is

$$0 \to \mu_n(K) \to K^\times \xrightarrow{n}\to K^\times \to H^1(K, \mu_n) \to H^1(K, (K^{\mathrm{sep}})^\times) = 0 \to \cdots.$$

Thus $H^1(K, \mu_n)$ is just the cokernel of $n : K^\times \to K^\times$. That is,

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

is an isomorphism.

Suppose that $\mu_n \subseteq K$. Then μ_n has trivial $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-action, and so we have

$$H^1(K, \mu_n) = \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mu_n).$$

If $\varphi : \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mu_n$ is a continuous homomorphism, then $\ker \varphi$ is an open subgroup of $\mathrm{Gal}(K^{\mathrm{sep}}/K)$, which is $\mathrm{Gal}(K^{\mathrm{sep}}/L)$ for some L. So this map φ factors as

$$\varphi : \mathrm{Gal}(K^{\mathrm{sep}}/K) \twoheadrightarrow \mathrm{Gal}(L/K) \hookrightarrow \mu_n.$$

The connecting homomorphism δ can be described explicitly as

$$\delta(a) = \varphi_a : g \mapsto \frac{g(\sqrt[n]{a})}{\sqrt[n]{a}} \in \mu_n.$$

Suppose I have some cyclic Galois L/K of degree n, where I still assume $\mu_n \subseteq K$. Take some

$$(\varphi : \mathrm{Gal}(L/K) \xrightarrow{\cong} \mu_n) \in H^1(L/K, \mu_n) \hookrightarrow H^1(K^{\mathrm{sep}}/K, \mu_n).$$

Because $\delta : K^\times/(K^\times)^n \to H^1(K, \mu_n)$ is an isomorphism, this is $\inf \varphi = \varphi_a$ for some $a \in K^\times/(K^\times)^n$. Then

$$\mathrm{Gal}(K^{\mathrm{sep}}/L) = \ker \varphi_a = \mathrm{Gal}(K^{\mathrm{sep}}/K(\sqrt[n]{a})).$$

This shows that $L = K(\sqrt[n]{a})$ by the Galois correspondence.

14.2 Second Galois cohomology of unramified extensions

When L/K is an unramified extension of local fields, we want to study the second cohomology $H^2(L/K) = H^2(L/K, L^\times)$. Note that we have already classified all unramified extensions, and it turned out that $\mathrm{Gal}(L/K)$ is cyclic. Then

$$\hat{H}^2(L/K, L^\times) \cong \hat{H}^0(L/K, L^\times) = K^\times/NL^\times \xrightarrow{v_K, \cong} \mathbb{Z}/n\mathbb{Z} = \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

But this is not very satisfactory. If $L'/L/K$ is unramified, we can try to think about what $\mathrm{Inf} : \hat{H}^2(L/K, L^\times) \to \hat{H}^2(L'/K, L'^\times)$. But inflation is not defined on $\hat{H}^0$. It turns out that this is just $\frac{1}{n}\mathbb{Z}/\mathbb{Z} \hookrightarrow \frac{1}{N}\mathbb{Z}/\mathbb{Z}$, but I'm getting ahead of myself.

Lemma 14.2. *$\hat{H}^q(L/K, \mathcal{O}_L^\times) = 0$ for all q provided that L/K is unramified.*

Proof. Because L/K is cyclic, we can check this for $\hat{H}^0$ and $\hat{H}^1$. We have shown that

$$\hat{H}^0(L/K, \mathcal{O}_L^\times) = \mathcal{O}_K^\times/N\mathcal{O}_L^\times = 0.$$

For $\hat{H}^1(L/K, \mathcal{O}_L^\times)$ is almost Hilbert's theorem 90. We have a short exact sequence $0 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v_L} \mathbb{Z} \to 0$, so

$$0 \to \mathcal{O}_K^\times \to K^\times \to \mathbb{Z} \to H^1(L/K, \mathcal{O}_L^\times) \to H^1(L/K, L^\times) = 0 \to \cdots .$$

Because L/K is unramified, $v_K : K^\times \to \mathbb{Z}$ is surjective and then we conclude $\hat{H}^1(L/K, \mathcal{O}_L^\times) = 0$. □

Now we know that all stuff coming from $\mathcal{O}_L^\times$ is trivial, and so we see that

$$(v_L)_* : H^2(L/K, L^\times) \to H^2(L/K, \mathbb{Z})$$

is an isomorphism. We can further dimension shift this using $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$. Here, $\mathbb{Q}$ has trivial cohomology because multiplication by $[L : K]$ is an isomorphism $\mathbb{Q} \to \mathbb{Q}$. So we get a connecting homomorphism

$$\delta : H^1(L/K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\cong} H^2(L/K, \mathbb{Z})$$

which is an isomorphism. Now the first cohomology can be computed as

$$H^1(L/K, \mathbb{Q}/\mathbb{Z}) = \mathrm{Hom}(\mathrm{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \cong \tfrac{1}{n}\mathbb{Z}/\mathbb{Z},$$

because there is a preferred generator $\mathrm{Frob}_K \in \mathrm{Gal}(L/K)$.

Now we have a canonical identification

$$\mathrm{inv}_{L/K} : H^2(L/K, L^\times) \xrightarrow{v_*} H^2(L/K, \mathbb{Z}) \xleftarrow{\delta} H^1(L/K, \mathbb{Q}/\mathbb{Z}) \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

This is called the **invariant map**.

Now I want to compute $H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times)$. This is defined as the direct limit

$$H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times) = \varinjlim_{\substack{L/K \text{ unram.} \\ \text{fin. Gal.}}} H^2(L/K, L^\times) = \varinjlim_n H^2(K_n/K, K_n^\times),$$

where K_n/K is the unique unramified extension of degree n. Then we need to know what the connected homomorphisms are, for $n \mid N$. This can be checked by the diagram

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

because the restriction of the Frobenius is still the Frobenius. So we get

$$H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times) = \varinjlim_n H^2(K_n/K, K_n^\times) \xrightarrow{\mathrm{inv}_K, \cong} \varinjlim_n \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Q}/\mathbb{Z}.$$

Ultimately, we want to compute the Brauer group

$$\mathrm{Br}(K) = H^2(K^{\mathrm{sep}}/K, (K^{\mathrm{sep}})^\times) \cong \mathbb{Q}/\mathbb{Z}.$$

This is going to take more time. What we need to show is that if L/K is any Galois extension with $[L : K] = n$,

$$\mathrm{inv} : H^2(L/K, L^\times) \to \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}$$

is an isomorphism.

To show this, we compare the two invariant maps

$$H^2(L^{\mathrm{unr}}/L, (L^{\mathrm{unr}})^\times) \xrightarrow{\mathrm{inv}_L} \mathbb{Q}/\mathbb{Z}, \quad H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times) \xrightarrow{\mathrm{inv}_K} \mathbb{Q}/\mathbb{Z}.$$

Note that $L^{\mathrm{unr}} = L \cdot K^{\mathrm{unr}}$ because the unramified closure is constructed by adjoining all roots of unity of order prime to p. So we get $\mathrm{Gal}(L^{\mathrm{unr}}/L) \hookrightarrow \mathrm{Gal}(K^{\mathrm{unr}}/K)$. This map gives a restriction map

$$\mathrm{Res} : H^2(K^{\mathrm{unt}}/K, (K^{\mathrm{unr}})^\times) \to H^2(L^{\mathrm{unr}}/L, (L^{\mathrm{unr}})^\times).$$

14.3 Some diagrams

We claim that the diagram

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

commutes. We are actually in the section titled "Some diagrams" in Serre's local fields part in Cassels–Fröhlich.

First note that $e \neq 1$ now, and so we have

$$\begin{tikzcd}
(K^{\mathrm{unr}})^\times \arrow[r, "ev_K"] \arrow[d, hook] & \mathbb{Z} \arrow[d, equal] \\
(L^{\mathrm{unr}})^\times \arrow[r, "v_L"] & \mathbb{Z}.
\end{tikzcd}$$

So we get

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

Here, the last square commutes because Frob_K corresponds to $x \mapsto x^{|k|}$ while Frob_L corresponds to $x \mapsto x^{|\ell|} = (x^{|k|})^f$.

Proposition 14.3. *If L/K is a finite extension, then $n \cdot \mathrm{inv}_K = \mathrm{inv}_L \circ \mathrm{Res}$.*

We want to show that if L/K is finite Galois with degree n, then $H^2(L/K, L^\times) \cong \frac{1}{n}\mathbb{Z}/\mathbb{Z}$. First we will find an element $u_{L/K} \in H^2(L/K, L^\times)$. If L/K, we can just set $u_{L/K} = \mathrm{inv}^{-1}(\frac{1}{n})$. If L/K is ramified, we can set K_n/K to be the extension of the same degree, and then compare the inflation maps

$$\begin{tikzcd}
0 \arrow[r] & H^2(K_n/K, K_n^\times) \arrow[r, "\mathrm{Inf}"] & H^2(L_n/K, L_n^\times) \arrow[d, equal] \\
0 \arrow[r] & H^2(L/K, L^\times) \arrow[r, "\mathrm{Inf}"] & H^2(L_n/K, L_n^\times).
\end{tikzcd}$$

Then we will show $|H^2(L/K, L^\times)| \leq n$ by induction.

15 October 19, 2017

Last time, if K_n/K is an unramified finite Galois extension of local field of degree $n = [K_n : K]$, then there is an isomorphism

$$\mathrm{inv} : H^2(K_n/K, K_n^\times) \xrightarrow{\cong} \tfrac{1}{n}\mathbb{Z}/\mathbb{Z}.$$

There is also a profinite version

$$\mathrm{inv} : H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}.$$

The goal of today is to get, for any finite Galois extension L/K of local fields with $n = [L : K]$,

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

This would imply

$$\mathrm{inv} : H^2(K^{\mathrm{sep}}/K, (K^{\mathrm{sep}})^\times) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}.$$

15.1 Second Galois cohomology of finite extensions

Because $\mathrm{inv} : H^2(K_n/K, K_n^\times) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z}$ is an isomorphism, we can look at the inverse image u_n of $\frac{1}{n}$. We want to find the element $u_{L/K} \in H^2(L/K, L^\times)$ of order n. Let $L_n = K_n \cdot L$ so that L_n/L is a Galois extension with $[L_n : L] \mid n$. We have an inclusion $\mathrm{Gal}(L_n/L) \hookrightarrow \mathrm{Gal}(K_n/K)$ and so we have a restriction map

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

Because u_n maps to $\frac{1}{n}$ in $\mathbb{Q}/\mathbb{Z}$, this shows that u_n maps to 0 in the upper right $\mathbb{Q}/\mathbb{Z}$. That is, $\mathrm{Res}\, u_n = 0$.

Now note that we have a inflation-restriction exact sequence

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

So we can push u_n to $H^2(L_n/K, L_n^\times)$ and then because it vanishes at $H^2(L_n/L, L_n^\times)$, it comes from $H^2(L/K, L^\times)$. Let us call this $u_{L/K} \in H^2(L/K, L^\times)$. This is going to be the order of element n we want.

To show that $H^2(L/K, L^\times)$ is actually generated by u_n, we will show that $|H^2(L/K, L^\times)| \leq n$. We induct on $[L : K]$.

15.2 Estimating the size

In the base case, assume that L/K is cyclic. Then

$$H^2(L/K, L^\times) = \hat{H}^0(L/K, L^\times) \cong K^\times/NL^\times.$$

This can be shown on the nose. One way of doing it is to use the Herbrand quotient. You can use the following lemma.

Lemma 15.1. *If L/K is a finite Galois extension of local fields, there exists an $\mathrm{Gal}(L/K)$-invariant open subgroup $V \subseteq \mathcal{O}_L^\times$ such that*

$$\hat{H}^q(L/K, V) = 0$$

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

Proof. We'll choose V to be coinduced. Let $V = \exp_p(A)$ for some coinduced $A \subseteq \mathcal{O}_L^+$. We know that L is coinduced as a $\mathrm{Gal}(L/K)$-module. That is, there exists an $a \in L$ such that $L = \bigoplus_{g\in\mathrm{Gal}(L/K)} K \cdot (ga)$. Without loss of generality, we may assume that $a \in (\pi_L)^r$ by rescaling. (We are going to choose r later.) Now define

$$A = \bigoplus_{g\in\mathrm{Gal}(L/K)} \mathcal{O}_K \cdot (ga) \subseteq (\pi_L)^r.$$

Now take r large enough such that $\exp_p : \pi_L^r \mathcal{O}_L \to U_{L,r}$ is an isomorphism of topological groups. This $V = \exp_p(A)$ is now an open subgroup of $\mathcal{O}_L^\times$. Also V is coinduced because A is coinduced. □

Recall from the homework that if G is cyclic and A is a G-module, then the **Herbrand quotient** is

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

if both are defined. This satisfies

- $0 \to A \to B \to C \to 0$ exact implies $h(B) = h(A)h(C)$ if any two are defined,
- $h(A) = 1$ if A is finite,
- $h(\mathbb{Z}) = |G|$.

Proposition 15.2. *$h(\mathcal{O}_L^\times) = 1$.*

Proof. There is a short exact sequence

$$0 \to V \to \mathcal{O}_L^\times \to \mathcal{O}_L^\times/V \to 0$$

or $\mathrm{Gal}(L/K)$-modules. Then $h(V) = 1$ and $h(\mathcal{O}_L/V) = 1$ because $\mathcal{O}_L^\times/V$ is finite. This shows that $h(\mathcal{O}_L^\times) = 1$. □

Proposition 15.3. *$h(L^\times) = n$.*

Proof. Again we have a short exact sequence

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

and look at the Herbrand quotients. □

So we have

$$\frac{|\hat{H}^0(L/K, L^\times)|}{|\hat{H}^1(L/K, L^\times)|} = n$$

and by Hilbert's theorem 90, $H^1(L/K, L^\times) = 0$. This shows that $|H^2(L/K, L^\times)| = n$.

Theorem 15.4. *Let L/K be any Galois extension. Then $|H^2(L/K, L^\times)| \leq n = [L : K]$.*

Proof. We induct on $[L : K]$. The base case is when $[L : K]$ is prime. This case is covered by the cyclic case. Otherwise $\mathrm{Gal}(L/K)$ is solvable so there exists a normal subgroup $H \lhd \mathrm{Gal}(L/K)$. Let $M = L^H$.

We have a inflation-restriction sequence

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

Then we have

$$|H^2(L/K, L^\times)| \leq |H^2(M/K, M^\times)||H^2(L/M, L^\times)| \leq [M : K][L : M] = [L; K]$$

by the inductive hypothesis. □

Theorem 15.5. *If L/K is any Galois extension of local fields, $H^2(L/K, L^\times)$ is cyclic of order $n = [L : K]$.*

Proof. There is an element $u_{L/K} \in H^2(L/K, L^\times)$ of order n, and we have the estimate $|H^2(L/K, L^\times)| \leq n$. □

15.3 Brauer group of a local field

Theorem 15.6. *If K is a local field, 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.

Proof. If is injective because inflation is injective. (All H^1 vanish.) Now we just need surjectivity. The Brauer group is $\lim_{L/K} H^2(L/K, L^\times)$, and so any element of $\mathrm{Br}(K)$ is represented by some element $au_{L/K} \in H^2(L/K, L^\times)$. But recall that we have

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

So $au_{L/K}$ is also represented by $au_n \in H^2(K_n/K, K_n^\times)$ in the direct limit. □

So we have an isomorphism

$$\mathrm{inv}_K : \mathrm{Br}(K) \xrightarrow{\cong} \mathbb{Q}/\mathbb{Z}.$$

Proposition 15.7. *For L/K a finite extension of local fields of degree $n = [L : K]$, the following commutes:*

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

Proof. Just use the definition $\mathrm{Br}(K) \cong H^2(K^{\mathrm{unr}}/K, (K^{\mathrm{unr}})^\times)$ and the result last time. □

Corollary 15.8. *Let $E/L/K$ be a tower of local fields and assume E/K is Galois. The restriction map*

$$\mathrm{Res}_{L/K} : H^2(E/K, E^\times) \to H^2(E/L, E^\times)$$

sends $u_{E/K}$ to $u_{E/L}$.

Proof. Look at the diagram

$$\begin{tikzcd}
H^2(E/K, E^\times) \arrow[r, "\mathrm{Res}"] \arrow[d, "\mathrm{inv}_K"] & H^2(E/L, E^\times) \arrow[d, "\mathrm{inv}_L"] \\
\frac{1}{[E:K]}\mathbb{Z}/\mathbb{Z} \arrow[r, "{[L:K]}"] & \frac{1}{[E:L]}\mathbb{Z}/\mathbb{Z}
\end{tikzcd}$$

and track where $u_{E/K}$ and $u_{E/L}$ maps to. □

Similarly, if L/K is Galois, then $\mathrm{Inf}(u_{E/K}) = [L : K]u_{L/K}$.

15.4 Tate's theorem

Theorem 15.9 (Tate). *Let G be a finite group and A be a G-module. Assume that for all $H \subseteq G$, $H^1(H, A) = 0$ and $H^2(H, A)$ is cyclic of order $|H|$. If a generates $H^2(G, A)$, then*

$$- \smile a : \hat{H}^q(G, \mathbb{Z}) \to \hat{H}^{q+2}(G, A)$$

is an isomorphism for all $q \in \mathbb{Z}$.

Let $G = \mathrm{Gal}(L/K)$ and $A = L^\times$. This satisfies the assumptions by Hilbert's theorem 90 and the theorem we have just proven. Apply the theorem to $q = -2$. Then we get

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} = \hat{H}^{2}(L/K, \mathbb{Z}) \xrightarrow{\cong} \hat{H}^0(L/K, L^\times) = K^\times/NL^\times,$$

This which comes from taking the cup product with $u_{L/K}$.

Idea of proof. We construct some module M such that there exists a long exact sequence

$$\cdots \to \hat{H}^q(G,\mathbb{Z}) \xrightarrow{- \smile a} \hat{H}^{q+2}(G,A) \to \hat{H}^{q+2}(G,M) \to \hat{H}^{q+1}(G,\mathbb{Z}) \to \cdots .$$

Then we will show that $H^q(H,M) = 0$ for all $H \subseteq G$ and some two consecutive q. This implies (by the homework) that $H^q(H,M) = 0$ for all $H \subseteq G$ and all q. □

16 October 24, 2017

We need to prove Tate's theorem.

Theorem 16.1 (Tate)**.** *Let G be a finite group and A a G-module such that for all $H \subseteq G$ we have $H^1(H,A) = 0$ and $H^2(H,A)$ is cyclic of order $|H|$. If a is a generator of $H^2(G,A)$, then*

$$- \smile a : \hat{H}^q(G,\mathbb{Z}) \to \hat{H}^{q+2}(G,A)$$

is an isomorphism for all $q \in \mathbb{Z}$.

Proof. Last time I gave the idea. Let us set this up. By dimension-shifting twice, there exists a $B = (A^+)^+$ such that $\hat{H}^q(G,B) \cong \hat{H}^{q+2}(G,A)$. Let $b \in \hat{H}^0(G,B)$ be a preimage of $a \in \hat{H}^2(G,A)$ under this isomorphism. Then

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

commutes.

The condition can be reformulated as

$$\hat{H}^{-1}(H,B) = 0, \quad \hat{H}^0(H,B) \cong \mathbb{Z}/|H|\mathbb{Z}$$

for all $H \subseteq G$. If b is a generator of $\hat{H}^0(G,B)$, we want to show that

$$- \smile b : \hat{H}^q(G,\mathbb{Z}) \to \hat{H}^q(G,B)$$

is an isomorphism. This maps are induced by $\mathbb{Z} \to B$ with $n \mapsto nb$.

Letting $B' = B \oplus \mathbb{Z}[G]$, we get an isomorphism $\hat{H}^q(G,B) \cong \hat{H}^q(G,B')$ induced by $B \hookrightarrow B'$. Define

$$i : \mathbb{Z} \to B' = B \oplus \mathbb{Z}[G]; \quad n \mapsto (nb, nN),$$

and we get a short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{i} B' \xrightarrow{j} M = \operatorname{coker} i \to 0$$

of G-modules. This is analogous to the mapping cylinder construction in topology.

This gives a long exact sequence

$$\cdots \to \hat{H}^{-1}(H,B') = 0 \to \hat{H}^{-1}(H,M) \xrightarrow{\delta} \hat{H}^0(H,\mathbb{Z}) \\ \xrightarrow{- \smile b} \hat{H}^0(H,B) \to \hat{H}^0(H,M) \xrightarrow{j_*} \hat{H}^1(H,\mathbb{Z}) = 0 \to \cdots .$$

Here, the map $\hat{H}^0(H,\mathbb{Z}) \to \hat{H}^0(H,B)$ is given by $[n] \mapsto nb$. Here, b is a generator of $B/N_G B$ so b is a generator of $B/N_H B = \hat{H}^0(H,B)$. Because both are cyclic groups of order $|H|$, the map $- \smile b : \hat{H}^0(H,\mathbb{Z}) \to \hat{H}^0(H,B)$ is an isomorphism.

This shows that $\hat{H}^{-1}(H,M) = \hat{H}^0(H,M) = 0$, for all $H \subseteq G$. The homework problem shows that all cohomology of M are $\hat{H}^q(G,M) = 0$. Then the long exact sequence implies that

$$- \smile b : \hat{H}^q(G,\mathbb{Z}) \to \hat{H}^q(G,B)$$

are isomorphisms. □

16.1 Reciprocity map

Last time, for L/K a Galois extension of local field, we used Tate's theorem to give an isomorphism

$$\mathrm{Gal}(L/K)^{\mathrm{ab}} = \hat{H}^{-2}(L/K,\mathbb{Z}) \xrightarrow{u_{L/K}} \hat{H}^0(L/K,L^\times) = K^\times/NL^\times.$$

This gives the reciprocity map

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

People also write this as

$$\theta_{L/K}(a) = (a, L/K).$$

This is called the **norm residue symbol** and can be thought of as the obstruction of a being a norm. It is reminiscent of quadratic reciprocity. Now I am going to give another way of describing this map, which may be more convenient in some contexts.

Proposition 16.2. *For $[a] \in K^\times/NL^\times$, its image $\theta_{L/K}([a]) \in G^{\mathrm{ab}}$ is characterized by: for any $\chi \in \mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z}) = H^1(L/K,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta,\cong} H^2(L/K,\mathbb{Z})$,*

$$\chi(\theta_{L/K}([a])) = \mathrm{inv}_{L/K}([a] \smile \delta\chi) \in \mathbb{Q}/\mathbb{Z}.$$

The proof involves a lot of homological algebra chasing, and I am going to do part of it and leave part of it on the homework.

Proof. By definition of $\theta_{L/K}$, we have

$$[a] = [\theta_{L/K}(a)] \smile u_{L/K}.$$

So

$$\begin{aligned}\mathrm{inv}([a] \smile \delta\chi) &= \mathrm{inv}(\theta_{L/K}(a) \smile u_{L/K} \smile \delta\chi) = \mathrm{inv}((\theta_{L/K}(a) \smile \chi) \smile u_{L/K}) \\ &= \mathrm{inv}(\delta(\chi \smile \theta_{L/K}(a)) \smile u_{L/K}).\end{aligned}$$

What is $\chi \smile \theta_{L/K}(a)$? Here $\chi \in \hat{H}^1(G,\mathbb{Q}/\mathbb{Z})$ and $\theta_{L/K}(a) \in \hat{H}^{-2}(G,\mathbb{Z}) \in G^{\mathrm{ab}}$. We claim that

$$\chi \smile [g] = \chi(g) \in \mathbb{Q}/\mathbb{Z}.$$

The proof of this fact is homework. Given this fact, we have

$$\mathrm{inv}([a] \smile \delta\chi) = \mathrm{inv}(\delta(\chi(\theta_{L/K}(a))) \smile u_{L/K}).$$

We also claim that the map

$$\frac{1}{|G|}\mathbb{Z}/\mathbb{Z} \cong \hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} \hat{H}^0(G, \mathbb{Z}) \cong \mathbb{Z}/|G|\mathbb{Z}$$

is just $\times|G|$. So

$$\begin{aligned}\mathrm{inv}([a] \smile \delta\chi) &= \mathrm{inv}([L:K]\chi(\theta_{L/K}(a))u_{L/K}) \\ &= [L:K]\chi(\theta_{L/K}(a))\frac{1}{[L:K]} = \chi(\theta_{L/K}(a)).\end{aligned}$$

This is the desired result. □

The consequence of this is the following compatibility.

Proposition 16.3. *Let $E/L/K$ be a tower with E/K and L/K Galois. There is a natural quotient map $\pi_{E/L} : \mathrm{Gal}(E/K)^{\mathrm{ab}} \to \mathrm{Gal}(L/K)^{\mathrm{ab}}$. For any $a \in K^\times$,*

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

Proof. It is enough to show that

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

But we can always lift χ to $\tilde{\chi} : \mathrm{Gal}(E/K) \to \mathbb{Q}/\mathbb{Z}$ and then the left hand side is

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

by the compatibility of Brauer groups. □

The upshot is that we have a commutative diagram

$$\begin{tikzcd}
K^\times/NE^\times \arrow[r, "\theta_{E/K}"] \arrow[d, two heads] & \mathrm{Gal}(E/K)^{\mathrm{ab}} \arrow[d, two heads] \\
K^\times/NL^\times \arrow[r, "\theta_{L/K}"] & \mathrm{Gal}(L/K)^{\mathrm{ab}}.
\end{tikzcd}$$

So we get a map

$$\theta_{/K} : K^\times \to \varprojlim_{L/K \text{ fin. Gal.}} \mathrm{Gal}(L/K)^{\mathrm{ab}} = \varprojlim_{L'/K \text{ fin. abe.}} \mathrm{Gal}(L'/K) = \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

that has dense image.

16.2 Group of universal norms

What is the kernel of $\theta_{/K} : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$? This is going to be simply the intersection of the kernels, and is

$$\ker \theta_{/K} = \bigcap_{L/K} N_{L/K} L^\times.$$

This is called the **group of universal norms**.

Proposition 16.4. *The only universal norm in $K^\times$ is 1.*

Definition 16.5. A subgroup $A \subseteq K^\times$ is called **normic** if there exists a Galois L/K such that $A = N_{L/K} L^\times$.

We'll show that any finite index open subgroup of $K^\times$ is normic. For profinite groups, open subgroups have finite index. But note that $K^\times$ is not profinite/compact, and in particular contains $\mathcal{O}_K^\times$. On the other hand, finite index subgroups of $K^\times$ are open. This is because $(K^\times)^n$ contains an open ball around 1.

Proposition 16.6. *If L/K is Galois, and L'/K is the maximal abelian subextension, then $N_{L/K} L^\times = N_{L'/K}(L')^\times$.*

Proof. The inclusion $N_{L/K} L^\times \subseteq N_{L'/K}(L')^\times$ is clear. On the other hand,

$$K/N_{L/K} L^\times \cong \mathrm{Gal}(L/K)^{\mathrm{ab}} = \mathrm{Gal}(L'/K) \cong K/N_{L'/K}(L')^\times.$$

This means that the quotient map $K/N_{L/K} L^\times \to K/N_{L'/K}(L')^\times$ is an isomorphism. □

17 October 26, 2017

Recall that at the end of last time we defined that a subgroup $A \subseteq K^\times$ is **normic** if there exists some Galois extension L/K such that $A = N_{L/K}L^\times$. Our goal is to prove that finite index subgroups of $K^\times$ are normic.

17.1 Normic subgroups

We showed that we may only take L/K abelian. So we have a map

$$\{\text{abelian extensions } L/K\} \longrightarrow \{\text{normic subgroups of } K^\times\}.$$

This is order-reversing, i.e., $L \subseteq L'$ implies $NL' \subseteq NL$. By local class field theory,

$$[L : K] = [K^\times : NL^\times].$$

This map is clearly surjective. Because we have $\theta_{/K} : K^\times \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$, there is also an inverse map

$$A \mapsto (K^{\mathrm{ab}})^{\theta_{/K}(A)}.$$

To checked that this is indeed an inverse, we need to check that $(K^{\mathrm{ab}})^{\theta_{/K}(NL^\times)} = L$. The inclusion $(K^{\mathrm{ab}})^{\theta_{/K}(NL^\times)} \supseteq L$ is easily verified, and equality follows from $[L : K] = [K^\times : NL^\times]$.

Proposition 17.1. *If $A = NL^\times$ and $B = NM^\times$, then $A \cap B = N(LM)^\times$.*

Proof. We clearly have $N(LM)^\times \subseteq NL^\times \cap NM^\times$. If $a \in K^\times$ such that $a \in NL^\times$ and $a \in NM\times$ then $\theta_{L/K}([a]) = 1_L$ and $\theta_{M/K}([a]) = 1_M$. This implies that $\theta_{LM/K}([a]) = 1_{LM}$. That is, $a \in N(LM)^\times$. □

Proposition 17.2. *If $A = NL^\times$ is normic and $B \supseteq A$, then B is normic.*

Proof. We have $\mathrm{Gal}(L/K) \cong K^\times/A$. We may consider B/A as a subgroup and $K^\times/A$, and this will correspond to some $\theta_{L/K}(B/A) \subseteq \mathrm{Gal}(L/K)$.

Take $M = L^{\theta_{L/K}(B/A)}$. Then

$$\begin{tikzcd}
K^\times/A \arrow[r, "\theta_{L/K}", "\cong"'] \arrow[d, two heads] & \mathrm{Gal}(L/K) \arrow[d, two heads] \\
K^\times/NM^\times \arrow[r, "\theta_{M/K}", "\cong"'] & \mathrm{Gal}(M/K).
\end{tikzcd}$$

Here,

$$\begin{aligned}
\theta_{L/K}(B/A) &\cong \mathrm{Gal}(L/M) = \ker(\mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)) \\
&= \theta_{L/K}(\ker(K^\times/A \to K^\times/NM^\times)) = \theta_{L/K}(NM^\times/A).
\end{aligned}$$

So $B = NM^\times$. □

Theorem 17.3. *Suppose K is local of characteristic 0. If $A \subseteq K^\times$ is finite index (and thus open), then A is normic.*

Proof. Note that if $A \subseteq K^\times$ is finite index, then $A \supseteq (K^\times)^n$ for some n. So it is enough to show that $(K^\times)^n$ are normic.

Let us first do this in the case when $\mu_n \subseteq K$. Let L be the maximal exponent n of an abelian extension of K. By Kummer theory,

$$\begin{aligned} L &= K(\{\sqrt[n]{a} : a \in K^\times/(K^\times)^n\}) \\ &= \text{composium of all extensions } \{K(\sqrt[n]{a})\}. \end{aligned}$$

Then

$$NL^\times = \bigcap_{a \in K^\times/(K^\times)^n} NK(\sqrt[n]{a})^\times \supseteq (K^\times)^n.$$

To show that $NL^\times = (K^\times)^n$, it is enough to show that $[K^\times : (K^\times)^n] = [K^\times : NL^\times] = |\mathrm{Gal}(L/K)|$.

We are going look at the Pontryagin dual

$$\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n) = \mathrm{Hom}(\mathrm{Gal}(K^{\mathrm{ab}}/K), \mu_n) = H^1(K^{\mathrm{ab}}/K, \mu_n) \cong K^\times/(K^\times)^n.$$

This shows that $\mathrm{Gal}(L/K)$ and $K^\times/(K^\times)^n$ have the same order.

We now generalize to the case when K might not contain μ_n. Let $K' = K(\mu_n)$. Then

$$N_{L'/K'}(L')^\times = ((K')^\times)^n.$$

We don't know if L'/K is Galois, so take L/K such that $L \supseteq L'$ and L/K is Galois. Then

$$N_{L/K}L^\times \subseteq N_{L'/K}(L')^\times = N_{K'/K}N_{L'/K'}(L')^\times = N_{K'/K}((K')^\times)^n \subseteq (K^\times)^n.$$

This implies that $(K^\times)^n$ is normic. □

This gives us

$$\mathrm{Gal}(K^{\mathrm{ab}}/K) = \varprojlim_{L/K \text{ abelian}} (K^\times/NL^\times) = \varprojlim_{[K^\times:A]<\infty} K^\times/A = \widehat{K}^\times.$$

This group $\widehat{K}^\times$ is called the **profinite completion** of K.

We can be more explicit in describing $\widehat{K}^\times$. We have $K^\times = \mathcal{O}_K^\times \times \pi^{\mathbb{Z}}$. So

$$\widehat{K}^\times = \widehat{\mathcal{O}}_K^\times \times \hat{\mathbb{Z}}^\times = \mathcal{O}_K^\times \times \pi^{\hat{\mathbb{Z}}}.$$

17.2 Quadratic reciprocity

Let us get back to general local field of any characteristic. Let L/K be unramified.

Proposition 17.4. *For $a \in K^\times$, $\theta_{L/K}([a]) = (\mathrm{Frob}_{L/K})^{v(a)}$.*

Proof. From last time, $\theta_{L/K}([a])$ is characterized by

$$\chi(\theta_{L/K}([a])) = \mathrm{inv}([a] \smile \delta\chi).$$

Recall that the invariant map was defined as

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

By functoriality, v_* maps $[a] \smile \delta\chi$ to $v_*([a]) \smile \delta\chi = v(a) \cdot \delta x$. Then δ^{-1} sends it to $v(a)\chi$ and then evaluating at the Frobenius gives $v(a)\cdot\chi(\mathrm{Frob}\,) = \chi(\mathrm{Frob}^{v(a)})$. This give the right thing. □

We are now going to look at quadratic extensions, because these are the simplest examples. Let L/K be a quadratic extension so that $\mathrm{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z}$. Then $K^\times/NL^\times \cong \mathbb{Z}/2\mathbb{Z}$.

Example 17.5. Let $K = \mathbb{Q}_p$ and $L = \mathbb{Q}_p(\sqrt{a})$. We have

$$a \in \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = \{1, u, p, up\}$$

where $u \in \mathbb{Z}_p^\times$ is a unit with $(\frac{u}{p}) = -1$. So there are three cases to consider.

If $a = u$, then L/K is unramified and $NL^\times = \{x : v_p(x) \text{ even}\}$, which is an index 2 subgroup of $\mathbb{Q}_p^\times$, generated by $(\mathbb{Q}_p^\times)^2$ and u.

If $a = p$, then L/K is totally ramified. Then we can say that $NL^\times$ is generated by $(\mathbb{Q}_p^\times)^2$ and $-p$.

Likewise, if $a = up$ then L/K is totally ramified and $NL^\times$ is generated by $(\mathbb{Q}_p^\times)^2$ and $-up$.

Let us look a global example.

Example 17.6. Let ℓ be an odd prime. Take $\ell^* = (-1)^{(\ell-1)/2}\ell$ ($\equiv 1 \bmod 4$) and take $K/\mathbb{Q} = \mathbb{Q}(\sqrt{\ell^*})/\mathbb{Q}$. Let $a \in \mathbb{Z}$ with $a > 0$ and $(a, 2\ell) = 1$. For each place v of $\mathbb{Q}$, consider the function

$$a \mapsto (a, K_w/\mathbb{Q}_v) = \theta_{K_w/\mathbb{Q}_v}(a) \in \mathrm{Gal}(K_w/\mathbb{Q}_v) \hookrightarrow \mathrm{Gal}(K/\mathbb{Q}) \cong \{\pm 1\}$$

where w is a place of K above v.

If $v = \ell$, we have total ramification and

$$NL_w^\times = (\mathbb{Q}_\ell^\times)^2 \times \{1, (-\ell^*)\}.$$

So for $a \in \mathbb{Z}_\ell^\times$ if and only $(\frac{a}{\ell}) = 1$, i.e.,

$$(a, K_w/\mathbb{Q}_\ell) = \left(\frac{a}{\ell}\right).$$

Let $v = p$ be an odd prime with $p \neq \ell$. Thre are two cases. If ℓ^* is a square in $\mathbb{Q}_p$, then $K_w = \mathbb{Q}_p$ and so

$$(a, K_w/\mathbb{Q}_p) = 1$$

for all $a \in \mathbb{Z}_p^\times$. If not, then $K_w = \mathbb{Q}_p(\sqrt{\ell^*})$ is unramified. So we just have

$$(a, K_w/\mathbb{Q}_p) = (-1)^{v_p(a)}.$$

In general, we see that

$$(a, K_w/\mathbb{Q}_p) = \Big(\frac{\ell^*}{a}\Big)^{v_p(a)}.$$

Let us now consider the case $p = 2$. Because $\ell^* \equiv 1 \bmod 4$, either $\ell^* \in (\mathbb{Q}_2^\times)^2$ if $\ell^2 \equiv 1 \bmod 8$ or $\mathbb{Q}_2(\ell^*) = \mathbb{Q}_2(\sqrt{5})$ if $\ell^* \equiv 5 \bmod 8$. Since a is a unit modulo 2, we always get

$$(a, K_w/\mathbb{Q}_2) = 1.$$

Finally, consider the case $v = \infty$. Either $K_w = \mathbb{R}$ in which case $(a, K_w/\mathbb{R}) = 1$, or $K_w = \mathbb{C}$ in which case the function takes signs. Because $a > 0$, we get $(a, K_w/\mathbb{C}) = 1$.

Now we have computed all the symbols. We have not talked about this, but the global reciprocity law tells us that

$$\prod_v (a, K_w/\mathbb{Q}) = 1.$$

Say $a = p$. Then

$$\Big(\frac{p}{\ell}\Big)\Big(\frac{\ell^*}{p}\Big) = 1.$$

This is a form of the standard quadratic reciprocity.

17.3 Reciprocity map on units

Let L/K be a Galois extension of local fields. Let T/K be the maximal unramified subextension. We have the characterization $T = L^{I(L/K)}$.

Proposition 17.7. *We have $\theta_{L/K}(\mathcal{O}_K^\times) = I(L/K)$.*

Proof. We first prove $\theta_{L/K}(\mathcal{O}_K^\times) \subseteq I(L/K)$. Note that $\theta_{T/K}(\mathcal{O}_K^\times) = \{1\}$. Then

$$\begin{tikzcd}
K^\times \arrow[r, "\theta_{L/K}"] \arrow[dr, "\theta_{T/K}"'] & \mathrm{Gal}(L/K) \arrow[d] \\
& \mathrm{Gal}(T/K)
\end{tikzcd}$$

shows the inclusion.

Now let us prove the other direction. We know that $\theta_{L/K} : K^\times \to \mathrm{Gal}(L/K)$ is surjective. It is enough to show that if $\theta_{L/K}(x) \in I(L/K)$ then $[x] = [u]$ for some $u \in \mathcal{O}_K^\times$. If $\theta_{L/K}([a]) \in I_{L/K}$ then $\theta_{T/K}([a]) = \mathrm{Frob}_{T/K}^{v_K(a)} = 1$ and so $[T : K] = f$ divides $v(a)$. Take $b = a \cdot N(\pi_L) - v_k(a)/f$. This is a unit. □

18 October 31, 2017

Today we are moving to our next topic, Lubin–Tate theory. We have local Kronecker–Weber for $\mathbb{Q}_p$ from the problem set. Let K be a local field. We have an Artin map

$$\theta_{/K} : K^\times = \mathcal{O}_K^\times \times \pi^{\mathbb{Z}} \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$$

This map is not surjective, but we can extend it to

$$\theta_{/K} : \widehat{K}^\times = \mathcal{O}_K^\times \times \pi^{\widehat{\mathbb{Z}}} \to \mathrm{Gal}(K^{\mathrm{ab}}/K).$$

So we can decompose

$$\begin{tikzcd}
 & K^{\mathrm{ab}} \arrow[dl, dash, "\mathcal{O}_K^\times"'] \arrow[dr, dash, "\pi^{\widehat{\mathbb{Z}}}"] & \\
K^{\mathrm{unr}} \arrow[dr, dash, "\pi^{\widehat{\mathbb{Z}}}"'] & & K^\pi \arrow[dl, dash, "\mathcal{O}_K^\times"] \\
 & K &
\end{tikzcd}$$

When $K = \mathbb{Q}_p$, we can actually describe these fields. Note that K^π depends on π, so we choose $\pi = p \in \mathbb{Q}_p$. Then

$$\begin{tikzcd}
 & \mathbb{Q}_p^{\mathrm{ab}} = \mathbb{Q}_p(\zeta_\infty) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}_p^{\mathrm{unr}} = \mathbb{Q}_p(\zeta_{(n,p)=1}) \arrow[dr, dash] & & \mathbb{Q}_p(\zeta_{p^\infty}) \arrow[dl, dash] \\
 & \mathbb{Q}_p &
\end{tikzcd}$$

as you've computed in your problem set. Now we want to see what $\theta_{/\mathbb{Q}_p}(a)$ is. Let $a = p^r u$. On $\mathbb{Q}_p^{\mathrm{unr}}$, we know that $\theta_{L/K}(a) = \mathrm{Frob}_{L/K}^r$ if L/K is unramified. So it is going to map $\zeta_n \mapsto \zeta_n^{p^r}$. On the other hand, it is harder to figure out what ζ_{p^k} is mapped to. It turns out that $\zeta_{p^k} \mapsto \zeta_{p^k}^{u^{-1}}$.

There is a global proof of this fact. If we use global reciprocity on $\mathbb{Q}(\zeta_p^k)/\mathbb{Q}$, the images should cancel out so it has to be $\zeta_{p^k}^{u^{-1}}$. But we want to do everything locally, and there is a proof using Lubin–Tate theory.

18.1 Affine group schemes

Here is one motivating question. Let A be any ring. For which (commutative) A-algebras R is $\mathrm{Hom}_{A-\mathsf{Alg}}(R, B)$ naturally a group for all A-algebras B?

Example 18.1. If $R = A[t]$, then $\mathrm{Hom}(R, B) \cong B$ as sets, so it is a group under addition. This is called the **additive group** and we say $B = \mathbb{G}_a(B)$.

Example 18.2. If $R = A[t, t^{-1}]$, then $\mathrm{Hom}(R, B) \cong B^\times = \mathbb{G}_m(B)$. This is called the **multiplicative group**.

Example 18.3. Set $R = A[t, t^{-1}]/(t^n - 1)$. Then $\mathrm{Hom}(R, B) \cong \mu_n(B)$ and this is a group scheme μ_n.

Example 18.4. Here is a non-abelian example. We want $\mathrm{Hom}(R, B) \cong \mathrm{GL}_n(B)$. To achieve this, we can take

$$R = A[(t_{i,j})_{1 \le i,j \le n}, (\det[t_{ij}])^{-1}].$$

The answer is that we want R to be a **Hopf algebra**. This means that there exist maps

- comultiplication $\Delta : R \to R \otimes R$
- coinversion $S : R \to R$
- coidentity $\epsilon : R \to A$

with axioms

- coassociativity

$$\begin{tikzcd}
R \arrow[r, "\Delta"] \arrow[d, "\Delta"] & R \otimes R \arrow[d, "1\otimes\Delta"] \\
R \otimes R \arrow[r, "\Delta\otimes 1"] & R \otimes R \otimes R
\end{tikzcd}$$

- identity

$$\begin{tikzcd}
R \arrow[r] \arrow[rr, bend right, "\mathrm{id}"'] & R \otimes R \arrow[r, "1\otimes\epsilon"] & R
\end{tikzcd}$$

- coinversion

$$\begin{tikzcd}
R \otimes R \arrow[rr, "1\otimes s"] & & R \otimes R \arrow[d] \\
R \arrow[u, "\Delta"] \arrow[r, "\epsilon"] \arrow[d, "\Delta"'] & A \arrow[r] & R \\
R \otimes R \arrow[rr, "s\otimes 1"] & & R \otimes R \arrow[u]
\end{tikzcd}$$

This is exactly what we need to get associativity

$$\begin{tikzcd}
\mathrm{Hom}(R,B) \times \mathrm{Hom}(R,B) \times \mathrm{Hom}(R,B) \arrow[r] \arrow[d] & \mathrm{Hom}(R,B) \times \mathrm{Hom}(R,B) \arrow[d] \\
\mathrm{Hom}(R,B) \times \mathrm{Hom}(R,B) \arrow[r] & \mathrm{Hom}(R,B).
\end{tikzcd}$$

Example 18.5. Let $R = A[t]$. The comultiplication map is

$$\Delta : A[t] \to A[t] \otimes A[t]; \quad t \mapsto 1 \otimes t + t \otimes 1.$$

Then $S = A[t] \to A[t]$ is $t \mapsto -t$ and $\epsilon : A[t] \to A$ is $t \mapsto 0$. This is the right map because

$$\Delta^* : \mathrm{Hom}(A[t] \otimes A[t], B) \to \mathrm{Hom}(A[t], B)$$

is given by $(\varphi, \psi) \mapsto \varphi + \psi$ because $t \mapsto 1 \otimes t + t \otimes 1$ is sent to $\psi + \varphi$.

Example 18.6. Let $R = A[t, t^{-1}]$. Here,

$$\begin{aligned} \Delta &: A[t,t^{-1}] \to A[t,t^{-1}] \otimes A[t,t^{-1}]; \quad t \mapsto t \otimes t,\ t^{-1} \mapsto t^{-1} \otimes t^{-1}, \\ S &: A[t,t^{-1}] \to A[t,t^{-1}]; \quad t \mapsto t^{-1},\ t^{-1} \mapsto t, \\ \epsilon &: A[t,t^{-1}] \to A; \quad t \mapsto 1,\ t^{-1} \mapsto 1. \end{aligned}$$

Why are group schemes useful? Suppose we have an affine abelian group scheme G defined over a field K. Assume that it comes from some Hopf algebra R, and also assume that R is finite over A (i.e., is a finite dimensional K-vector space). Then we can look at $G(\overline{K}) = \mathrm{Hom}(R, \overline{K})$. This is going to be a finite group with an action of $\mathrm{Gal}(\overline{K}/K)$.

If we take $G = \mu_n$, then we are going to get $\mu_n(\overline{K}) = G(\overline{K})$. So we get

$$\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(\mu_n(\overline{K})),$$

and $\mu_n(\overline{K}) \cong \mathbb{Z}/n\mathbb{Z}$. This sounds like a great plan, but we need a source of finite group schemes. So we would like a group scheme with lots of subschemes. $\mathbb{G}_m$ is a good example. Note that μ_n is actually

$$\ker(\times[n] : \mathbb{G}_m \to \mathbb{G}_m).$$

The problem is that there aren't many affine abelian group schemes. It can be proven that over $\overline{K}$ of characteristic 0, the only affine abelian group schemes are $\mathbb{G}_a$, $\mathbb{G}_m$, μ_n, and their products. There are two ways to go from here:

- Drop the affine condition. Here we may consider elliptic curves, abelian varieties, etc. These all have a lot of subgroup schemes. If you have an elliptic curve E, the n-torsion points $E[n]$ are group schemes.
- Take the completion. This works only over local fields.

There is also another problem. In general, Aut of an abelian group is not necessarily abelian. So we need some extra structure on $G(\overline{K})$ that rigidifies the structure.

18.2 Formal groups

Let A be any ring. We are going to consider the ring $A[[x]]$ and we want to make this into something like a Hopf algebra. Say, e.g., $A = \mathcal{O}_K$. I can look at

$$\mathrm{Hom}_{\mathrm{cts}}(A[[x]], \mathcal{O}_K),$$

where $A[[x]]$ has the x-adic topology. This group is isomorphic to $\pi_K\mathcal{O}_K$ because we are looking only at continuous maps.

We need something like comultiplication, but we are not going to look at $A[[x]] \to A[[x]] \otimes_A A[[x]]$. Instead, we look at

$$A[[x]] \to A[[x_1, x_2]].$$

This is because

$$\mathrm{Hom}_{\mathrm{cts}}(A[[x_1, x_2]], \mathcal{O}_L) \to \mathrm{Hom}_{\mathrm{cts}}(A[[x_1]], \mathcal{O}_L) \times \mathrm{Hom}_{\mathrm{cts}}(A[[x_2]], \mathcal{O}_L)$$

is bijective.

Definition 18.7. A **formal group law** F over A is a power series $F(x, y) \in A[[x, y]]$ such that

- $F(x, y) \equiv x + y \pmod{\deg 2}$,
- $F(x, y) = F(y, x)$,
- $F(x, F(y, z)) = F(F(x, y), z)$,
- there exists an $i_F(x) \in A[[x]]$ with $F(x, i_F(x)) = 0$,
- $F(0, y) = y$, $F(x, 0) = x$.

Example 18.8. The additive group $\mathbb{G}_a$ still works as a formal group. The comultiplication $x \mapsto x \otimes 1 + 1 \otimes x$ now is interpreted as $F(x, y) = x + y$.

,

Example 18.9. For the multiplicative group, we need to shift the origin. Then $F(x, y) = x + y + xy$. The power series

$$i_F(x) = \frac{1}{1+x} - 1 = -x + x^2 - x^3 + x^4 - \cdots$$

works as an inverse.

If $A = \mathcal{O}_K$ and L/K is a finite extension, then $\pi_L\mathcal{O}_L$ using the group law given by F.

19 November 2, 2017

We were doing formal groups.

Definition 19.1. A **formal group** over A is a power series $F(x,y) \in A[[x,y]]$ such that

- $F(x,y) \equiv x + y \pmod{\deg 2}$,
- $F(x,y) = F(y,x)$,
- $F(x, F(y,z)) = F(F(x,y),z)$,
- there exists an $i_F(x) \in A[[x]]$ such that $F(x, i_F(x)) = 0$ (this is actually redundant),
- $F(0,y) = y$ and $F(x,0) = x$.

19.1 Morphisms between formal groups

A **homomorphism** $h : F \to G$ is a power series $h \in A[[x]]$ with $h(0) = 0$ such that

$$G(h(x), h(y)) = h(F(x,y)) \in A[[x,y]].$$

Recall that if F is a formal group over $\mathcal{O}_K$ and L/K is a finite extension then $F(\pi_L \mathcal{O}_L)$ is $\pi_L \mathcal{O}_L$ made into a group by $a +_F b = F(a,b)$. If K^{sep}/K is the separable closure, then we can look at its maximal ideal

$$K^{\text{sep}} \supseteq \mathcal{O}_{K^{\text{sep}}} \supseteq \mathfrak{p}_{K^{\text{sep}}},$$

which is not a principal ideal now. So we can define $F(\mathfrak{p}_{K^{\text{sep}}})$.

If $h : F \to G$ is a formal group homomorphism, we get group homomorphisms

$$h : F(\pi_L \mathcal{O}_L) \to G(\pi_L \mathcal{O}_L); \quad a \mapsto h(a),$$

or $F(\mathfrak{p}_{K^{\text{sep}}}) \to G(\mathfrak{p}_{K^{\text{sep}}})$.

Example 19.2. Take $A = \mathbb{Q}_p$. The additive and multiplicative groups are $\widehat{\mathbb{G}}_a(x,y) = x + y$ and $\widehat{\mathbb{G}}_m(x,y) = x + y + xy$. The power series $h = \exp_p -1 \in \mathbb{Q}_p[[x]]$ is then a formal group homomorphism because

$$\widehat{\mathbb{G}}_m(h(x), h(y)) = \exp_p(x+y) - 1 = h(\widehat{\mathbb{G}}_a(x,y)).$$

There is also an inverse $h^{-1}(y) = \log_p(1+y)$. So $\widehat{\mathbb{G}}_a$ and $\widehat{\mathbb{G}}_m$ are isomorphic over $\mathbb{Q}_p$. These are not isomorphic over $\mathbb{Z}_p$. For instance, $L = \mathbb{Q}_p(\zeta_p)$ has $\zeta_p - 1 \in \pi_L \mathcal{O}_L$ and so $\widehat{\mathbb{Q}}_m(\pi_L L)$ has p-torsion. But $\widehat{\mathbb{Q}}_a(\pi_L L)$ never has torsion.

Example 19.3. Let us look at $\widehat{\mathbb{G}}_m$ over $\mathbb{Z}_p$. For $n \in \mathbb{Z}$, define

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

Then $h_n \in \operatorname{End}(\widehat{\mathbb{G}}_m)$. Actually this can be defined for all $n \in \mathbb{Z}_p$. The coefficients are still going to be integers in $\mathbb{Z}_p$.

If F and G Are formal groups, then $\mathrm{Hom}(F, G)$ is an abelian group, with $h_1 +_G h_2 = G(h_1, h_2)$. Then $\mathrm{End}(F) = \mathrm{Hom}(F, F)$ is a (possibly non-commutative) ring with addition $+_F$ and multiplication composition. In the above example, you can show that

$$h_n +_{\widehat{\mathbb{G}}_m} h_m = h_{n+m}, \quad h_n \circ h_m = h_{nm}.$$

So we have a ring homomorphism

$$\mathbb{Z}_p \to \mathrm{End}(\widehat{\mathbb{G}}_m).$$

In this case, this is actually and isomorphism although I am not going to prove this.

Suppose F and G be formal groups over $\mathcal{O}_K$. Last time I talked about getting cyclotomic field from group schemes. Given $h : F \to G$, how can we think of $\ker h$? We have a group homomorphism

$$F(\mathfrak{p}_{K^{\mathrm{sep}}}) \to G(\mathfrak{p}_{K^{\mathrm{sep}}}).$$

and so we can look at the kernel of this homomorphism. Often we are going to be in the case when h is a monic polynomial. Then the kernel is the set of solutions to $h(X) = 0$. The ring

$$\mathcal{O}_K[[x]]/h(x)$$

is then going to be a finite $\mathcal{O}_K$-algebra, and this gives a finite group scheme over $\mathcal{O}_K$.

Example 19.4. For instance, if $K = \mathbb{Q}_p$ and $F = \widehat{\mathbb{G}}_m$, with h_p, we would get the ring $\mathcal{O}_K[[x]]/(x+1)^p - 1$. Then our formal group obtained by taking the kernel is $\mu_p(\mathcal{O}_K)$.

19.2 Lubin–Tate theory

We can look at $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ acting on $\{x \in \mathfrak{p}_{K^{\mathrm{sep}}} : h(X) = 0\} = \ker(F(\mathfrak{p}_{K^{\mathrm{sep}}}) \to G(\mathfrak{p}_{K^{\mathrm{sep}}}))$.

Definition 19.5. Let K be a local field with $|k| = q$ and $\pi \in \mathcal{O}_K$ be a uniformizer. The **Lubin–Tate series** is given as

$$\mathcal{F}_\pi = \{f(x) \in \mathcal{O}_K[[x]] : f(x) \equiv \pi x \bmod \deg 2,\ f(x) \equiv x^q \bmod \pi\}.$$

Example 19.6. For $K = \mathbb{Q}_p$, the polynomial $f(x) = (x+1)^p - 1$ is a Lubin–Tate series. Actually constructing them are easy, because you can take anything like $f(x) = x^p + \pi x$.

Theorem 19.7. *(a) For any $f \in \mathcal{F}_\pi$, there exist a unique formal group F_f such that $f \in \mathrm{End}(F_f)$.*

(b) *For any $a \in \mathcal{O}_K$, there exists a unique endomorphism $[a]_f$ of F_f such that $[a]_f$ commutes with f and $[a]_f \equiv aX \pmod{\deg 2}$. Then the map*

$$\mathcal{O}_K \to \operatorname{End}(F_f); \quad a \mapsto [a]_f$$

is an isomorphism of rings.

(c) *If $f, g \in \mathcal{F}_\pi$ then $F_f \cong F_g$ as formal groups over $\mathcal{O}_K$.*

We're going to have a "workhorse lemma".

Lemma 19.8. *For $f, g \in \mathcal{F}_\pi$ and a linear polynomial $\Phi_1(x_1, \dots, x_r)$ over $\mathcal{O}_K$, the equation*

$$f(\Phi(x_1, x_2, \dots, x_r)) = \Phi(g(x_1), g(x_2), \dots, g(x_r))$$

will have a unique solution $\Phi \in \mathcal{O}_K[[x_1, \dots, x_r]]$ such that $\Phi \equiv \Phi_1 \pmod{\deg 2}$.

Proof. We do this by induction. It is enough to show that there is a unique polynomial $\Phi_k \in \mathcal{O}_K[x_1, \dots, x_r]$ of degree k such that $\Phi_k \equiv \Phi_1 \pmod{\deg 2}$ and

$$f(\Phi_k(x_1, \dots, x_r)) \equiv \Phi_k(g(x_1), \dots, g(x_r)) \pmod{\deg(k+1)}.$$

We already have our base case $k = 1$. Assume we have our unique Φ_k already. Then any Φ_{k+1} satisfying the condition must reduce to Φ_k modulo degree $k+1$. Then $\Phi_{k+1} = \Phi_k + Q$ where Q is a homogeneous polynomial of degree $k+1$. Here

$$f(\Phi_{k+1}(x_1, \dots, x_r)) \equiv f(\Phi_k(x_1, \dots, x_r)) + \pi Q(x_1, \dots, x_r) \pmod{\deg(k+2)}$$

and

$$\begin{aligned} \Phi_{k+1}(g(x_1), \dots, g(x_r)) &= \Phi_k(g(x_1), \dots, g(x_r)) + Q(g(x_1), \dots, g(x_r)) \\ &\equiv \Phi_k(g(x_1), \dots, g(x_r)) + \pi^{k+1} Q(x_1, \dots, x_r) \pmod{\deg(k+2)}. \end{aligned}$$

This shows that there exists a unique Q. But we still need to show that Q has coefficients in $\mathcal{O}_K$.

Working modulo π, we have

$$f(\Phi_k(x_1, \dots, x_n)) \equiv \Phi_k(x_1, \dots, x_r)^q \equiv \Phi_k(x_1^q, \dots, x_r^q) \equiv \Phi_k(g(x_1), \dots, g(x_r)).$$

So Q actually has coefficients in $\mathcal{O}_K$ because $\pi - \pi^{k+1}$ is π times a unit. □

Now we can start proving the theorem. We construct F_f as the unique power series in $\mathcal{O}_K[[x, y]]$ such that

$$F_f(f(x), f(y)) = f(F_f(x, y))$$

and $F_f(x, y) \equiv x + y \pmod{\deg 2}$.

We need to show that F_f is a commutative formal group. Commutativity follows from the uniqueness. We also get associativity because $F_f(F_f(x, y), z)$ and $F_f(x, F_f(y, z))$ both have the same linear term and satisfy the same functional equation. To show that $F_f(x, 0) = x$, we note that both are power series in x that commute with f. Again uniqueness shows that $F_f(x, 0) = x$. This proves (a).

20 November 7, 2017

Recall our setup

$$\mathcal{F}_\pi = \{f \in \mathcal{O}_K[[x]] : f(x) \equiv \pi x \bmod \deg 2,\ f(x) \equiv x^q \bmod \pi\}.$$

We proved the lemma saying that if $f, g \in \mathcal{F}_\pi$ and $\Phi_1 \in \mathcal{O}_K[x_1, \dots, x_r]$ is a homogeneous linear polynomial, then

$$f(\Phi(x_1, \dots, x_r)) = \Phi(g(x_1), \dots, g(x_r))$$

has a unique solution $\Phi \in \mathcal{O}_K[x_1, \dots, x_r]$ such that $\Phi \equiv \Phi_1 \bmod \deg 2$.

Proof of Theorem 19.7. We have shown (a) last time. If $f \in \mathcal{F}_\pi$ then there exists a unique formal group F_f such that f is an endomorphism of F_f.

Next we want to show that F has lots of endomorphisms and we want to show that $F_f \cong F_g$ for all $f, g \in \mathcal{F}_\pi$. We accomplish both of this by defining $[a]_{g,f}$ for $a \in \mathcal{O}_K$ such that

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

and $[a]_{g,h} \equiv aX \bmod \deg 2$. Uniqueness immediately shows that

$$[a]_{g,f} +_{F_g} [b]_{g,f} = [a+b]_{g,f}, \quad [a]_{h,g} \circ [b]_{g,f} = [ab]_{h,f}.$$

Note that $[a]_{g,h}$ is a formal group homomorphism $F_f \to F_g$ because

$$F_f \circ ([a]_{g,f}, [a]_{g,f}), \quad [a]_{g,f} \circ F_g$$

both have the property that $\Phi \circ (f \times f) = g \circ \Phi$ and have linear terms $ax + ay$. So they are equal by uniqueness.

Specializing to $f = g$ and writing $[a]_f = [a]_{f,f}$ shows that the map

$$\mathcal{O}_K \to \mathrm{End}(F_f); \quad a \mapsto [a]_f$$

is a ring homomorphism. For any $f, g \in \mathcal{F}_\pi$ and $a \in \mathcal{O}_K^\times$, we have

$$[a]_{f,g} \circ [a^{-1}]_{g,h} = x$$

and so $[a]_{f,g}$ is an isomorphism between F_f and F_g. □

20.1 Torsion points in a formal group

Definition 20.1. A **formal $\mathcal{O}_K$-module** F is a formal group F over $\mathcal{O}_K$ along with a ring homomorphism

$$\mathcal{O}_K \to \mathrm{End}(F); \quad a \mapsto [a]_F$$

such that $[a]_F \equiv ax \bmod \deg 2$.

For example F_f is a formal $\mathcal{O}_K$-module. If F is a formal $\mathcal{O}_K$-module, then $F(\mathfrak{p}_{K^{\text{sep}}})$ is an actual $\mathcal{O}_K$-module with

$$a \cdot x = [a]_f(x) \in \mathfrak{p}_{K^{\text{sep}}}.$$

Definition 20.2. If f is a Lubin–Tate series and F_f the corresponding formal group, we define

$$E_{f,n} = \{x \in \mathfrak{p}_{K^{\text{sep}}} : [\pi^n]_f(X) = 0\}.$$

These are the "π^n-torsion of f".

Let $K^{\pi,n}$ be the field generated by $E_{f,n}$, and write

$$E_f = \bigcup_n E_{f,n}, \quad K^\pi = \bigcup_n K^{\pi,n}.$$

Proposition 20.3. *Let $f, g \in \mathcal{F}_\pi$. There exists an isomorphism*

$$E_{f,n} \xrightarrow{\cong} E_{g,n}; \quad x \mapsto [1]_{g,f}(x).$$

Then field $K^{\pi,n}$ does not depend on the choice of f.

Proof. Note that $x \in E_{f,n}$ if and only if $[\pi^n]_f(x) = 0$ if and only if

$$0 = [1]_{g,f}[\pi^n]_f(x) = [\pi^n]_g[1]_{g,f}.$$

This happens if and only if $[1]_{g,f}(x) \in E_{g,n}$.

Now we show that the field is independent of f. Suppose $x \in E_{f,n}$. Then

$$[1]_{g,f}(x) \in K(x)$$

because $K(x)$ is still a complete field. Then $K^{\pi,n,f} = K(E_{f,n}) \supseteq E_{g,n}$ and so $K^{\pi,n,f} \supseteq K^{\pi,n,g}$. Symmetry shows that $K^{\pi,n,f} = K^{\pi,n,g}$. □

Note that $E_{f,n}$ is an $\mathcal{O}_K$-submodule of $\mathfrak{p}_{K^{\text{sep}}}$ (with the formal group law) annihilated by π^n.

Theorem 20.4. *As $\mathcal{O}_K$-modules, $E_{f,n} \cong \mathcal{O}_K/\pi^n\mathcal{O}_K$, non-canonically.*

Proof. Without loss of generality, let f be a monic polynomial of degree q, e.g., $x^q + \pi x$. Note here that $[\pi]_f = f$ and $[\pi^k]_f = f \circ \cdots \circ f = f^{(k)}$. Then

$$E_{f,n} = \{x \in \mathfrak{p}_{K^{\text{sep}}} : f^{(n)}(x) = 0\}.$$

Note that $f^{(n)} \mid f^{(n+1)}$ because $x \mid f$ and so we can factor

$$f^{(n)} = x \cdot \frac{f}{x} \cdot \frac{f^{(2)}}{f} \cdot \frac{f^{(3)}}{f^{(2)}} \cdot \cdots \cdot \frac{f^{(n)}}{f^{(n-1)}}.$$

We claim that all $f^{(k)}/f^{(k-1)}$ are Eisenstein polynomials. We just check

$$g \equiv x^{q^k}/x^{q^{k-1}} \equiv x^{q^k - q^{k-1}} \pmod{\pi}$$

and the constant term is π. So they are all irreducible, and all of its roots have absolute value less than 1. Then all of these roots lie in $\mathfrak{p}_{K^{\text{sep}}}$. Therefore $|E_{f,n}| = q^n$ whatever it is.

Note that $E_{f,n}$ is a module over $\mathcal{O}_K$, which is a DVR. So $E_{f,n}$ is going to be a direct sum

$$E_{f,n} \cong \mathcal{O}_K/\pi^{d_1} \oplus \cdots \oplus \mathcal{O}_K/\pi^{d_m}.$$

But the π-torsion submodule of $E_{f,n}$ is $E_{f,1}$ which has order q. So $m = 1$ and $E_{f,n} \cong \mathcal{O}_K/\pi^n$. □

$E_{f,n}$ is not canonically isomorphic to $\mathcal{O}_K/\pi^n\mathcal{O}_K$, but it is true that

$$(\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathrm{Aut}_{\mathcal{O}_K}(E_{f,n}); \quad a \mapsto [a]_f.$$

Corollary 20.5. *$E_f = \bigcup_n E_{f,n}$ is isomorphic to $K/\mathcal{O}_K$ as $\mathcal{O}_K$-modules.*

Proof. Choose a generator $\alpha_1 \in E_{f,1}$ and then for $n \geq 2$ inductively choose α_n such that $[\pi]_f\alpha_n = \alpha_{n-1}$. Then glue them together using $E_f \to K/\mathcal{O}_K$ by $\alpha_n \mapsto \pi^{-n}$. □

Again, $E_f \cong K/\mathcal{O}_K$ is not canonical but

$$\mathrm{Aut}_{\mathcal{O}_K}(E_f) \cong \varprojlim_n \mathrm{Aut}_{\mathcal{O}_K}(E_{f,n}) = \varprojlim_n (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times \cong \mathcal{O}_K^\times$$

is canonical.

20.2 Field obtained by adjoining torsion points

Proposition 20.6. *The field $K^{\pi,n} = K(E_{f,n}) = K(\alpha_n)$ is a Galois extension of K, where α_n is any generator of α_n.*

Proof. The field $K^{\pi,n}$ is Galois because it is the splitting field of $f^{(n)}$. To show that it is generated by α_n, note that for any $x \in E_{f,n}$, there exists an $a \in \mathcal{O}_K$ such that $x = [a]_f(\alpha_n)$. But $[a]_f$ is an infinite series with coefficients in $\mathcal{O}_K$, so $x \in K(\alpha_n)$ because $K(\alpha_n)$ is complete. □

Here α_n is a root of $f^{(n)}$ but is not a root of $f^{(n-1)}$, so that α_n is a root of $f^{(n)}/f^{(n-1)}$. So this is the minimal polynomial for α_n.

Now we'd like to understand $\mathrm{Gal}(K^{\pi,n}/K)$. The Galois group acts on $E_{f,n}$, because it is just the set of roots of a polynomial. It also preserves the $\mathcal{O}_K$-module structure. So we have a homomorphism

$$\mathrm{Gal}(K^{\pi,n}/K) \to \mathrm{Aut}_{\mathcal{O}_K}(E_{f,n}) \cong (\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times.$$

Proposition 20.7. *This map is an isomorphism.*

Proof. The map is clearly injective, because $E_{f,n}$ generates $K^{\pi,n}$. For surjectivity, we just count the orders of both side. The size of the Galois group is

$$|\mathrm{Gal}(K^{\pi,n}/K)| = \deg(f^{(n)}/f^{(n-1)}) = q^n - q^{n-1}$$

and the size of the units on the right hand side is

$$|(\mathcal{O}_K/\pi^n\mathcal{O}_K)^\times| = q^n - q^{n-1}$$

because we have to remove that non-units, which are multiplies of π. So this is an isomorphism. □

Corollary 20.8. $\mathrm{Gal}(K^\pi/K) = \varprojlim \mathrm{Gal}(K^{\pi,n}/K) = \mathrm{Aut}_{\mathcal{O}_K}(E_f) \cong \mathcal{O}_K^\times$.

So we've constructed this field K^π by our bare hands, without using any class field theory. Now I would like to show that this is the same as the K^π we have defined before, using the reciprocity map.

Proposition 20.9. $\pi \in N_{K^{\pi,n}/K}(K^{\pi,n})^\times$.

Proof. We have

$$N\alpha_n = (-1)^{q^n - q^{n-1}}\pi = \pi$$

unless q is even and $n = 1$, in which case $N(-\alpha_n) = \pi$. □

We can construct the field

$$L^\pi = K^\pi \cdot K^{\mathrm{unr}}$$

and this is a candidate for K^{ab}. There is a map

$$r_\pi : K^\times \to \mathrm{Gal}(L^\pi/K)$$

given by, for $u \in \mathcal{O}_K^\times$,

$$r_\pi(u)|_{K^{\mathrm{unr}}} = \mathrm{id}\,|_{K^{\mathrm{unr}}}, \quad r_\pi(u)(x) = [u^{-1}]_f(x) \text{ where } x \in E_f,$$

and

$$r_\pi(\pi)|_{K^\pi} = \mathrm{id}\,|_{K^\pi}, \quad r_\pi(\pi)|_{K^{\mathrm{unr}}} = \mathrm{Frob}\,.$$

Next time, we are going to prove that L^π and r_π does not depend on π. Then we will show that $r_\pi = \theta_{L^\pi/K}$. This will give us that L^π is actually K^{ab}.

21 November 9, 2017

Last time we were able to use Lubin–Tate theory to construct K^π and

$$L^\pi = K^{\text{unr}} \cdot K^\pi.$$

This is the candidate for K^{ab}. We also define the map

$$r_\pi : K^\times \to \text{Gal}(L^\pi/K)$$

which is the candidate for $\theta_{K^{\text{ab}}/K}$.

21.1 Characterization of the Artin map

How do we show that something is the Artin map? Let $L = K^{\text{unr}} \cdot K^\pi$ for all π. (Here we're assuming that L^π is independent of the choice of π.)

Proposition 21.1. *Let*

$$r : K^\times \to \text{Gal}(L/K)$$

be a homomorphism such that the composition

$$K^\times \xrightarrow{r} \text{Gal}(L/K) \twoheadrightarrow \text{Gal}(K^{\text{unr}}/K)$$

is the reciprocity map $x \mapsto \text{Frob}^{v_k(x)}$ *and for any uniformizer* π*,* $r(\pi)|_{K^\pi}$ *is the identity on* K^π*. Then* $r = \theta_{L/K}$*.*

Proof. Note that $K^\times$ is generated by the uniformizers, because $u = (u\pi)\pi^{-1}$. So it is enough to check that $r(\pi) = \theta_{L/K}(\pi)$ for all uniformizers π.

But note that

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

and

$$r(\pi)|_{K^\pi} = \text{id}_{K^\pi}.$$

Here, note that we have shown $\pi \in N(K^{\pi,n})^\times$ for all n and so $\theta_{K^{\pi,n}/K}(\pi) = \text{id}_{K^{\pi,n}}$. Since this is true for all n, we get $\theta_{K^\pi/K} = \text{id}_{K^\pi}$. □

To use this characterization, we need to show that $L^\pi = K^{\text{unr}} \cdot K^\pi$ is independent of π, and also that $r_\pi = r_\varpi$ for uniformizers π and ϖ. But assuming all this, we have

$$r : K^\times \to \text{Gal}(L/K) = \theta_{L/K}.$$

We want next want to show that $L = K^{\text{ab}}$. How do we do this? First

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

Here, for an arbitrary $\pi^r u \in K^\times$,

$$\theta_{K^{\pi,n}/K}(\pi^r u)(x) = r_\pi(u)(x) = [u^{-1}]_f(x) = (u^{-1}) \cdot x.$$

This is going to be the identity if and only if $u^{-1} \equiv 1 \pmod{\pi^n}$, because this is just multiplication. So this is true if and only if $u \equiv 1 \pmod{\pi^n}$. Hence

$$N(K^{\pi,n})^\times = \ker(\theta_{K^{\pi,n}/K} : K^\times \to \text{Gal}(K^{\pi,n}/K)) = \pi^{\mathbb{Z}} \cdot U_n.$$

Theorem 21.2. *Any finite abelian extension K'/K is contained in $L = K^{\pi} \cdot K^{\mathrm{unr}}$.*

Proof. Note that $N(K')^{\times}$ is a finite index subgroup of $K^{\times}$ by class field theory. So it must contain $\pi^{f\mathbb{Z}} \cdot U_n$ for some f and n. Then

$$N(K')^{\times} \supseteq N(K^{\pi,n})^{\times} \cap N(K^{\mathrm{unr},f}) = N(K^{\pi,n} \cdot K^{\mathrm{unr},f}).$$

This implies that $K' \subseteq K^{\pi,n} \cdot K^{\mathrm{unr},f}$. Therefore K' is contained in L. □

21.2 Independence on the uniformizers

Let π and ϖ be uniformizers, and let f, g be Lubin–Tate polynomials for π, ϖ. Let F_f and G_g be the Lubin–Tate formal groups for f and g. The problem is that F_f and G_g are not isomorphic over $\mathcal{O}_K$. So we need to work over a larger field. The natural thing to do is to work over K^{unr}, because $K^{\pi} \cdot K^{\mathrm{unr}} = K^{\varpi} \cdot K^{\mathrm{unr}}$. But a problem here is that K^{unr} is not complete. So we are going to look at its completion $\widehat{K}^{\mathrm{unr}}$ and its ring of integers $\widehat{\mathcal{O}}_K^{\mathrm{unr}}$.

Let me say a bit about infinite algebraic extensions. Let K be a local field and L/K be an infinite algebraic extension. Then it is not complete, because it is a countable-dimensional vector space and all Banach spaces are uncountable-dimensional vector spaces. Then we can form the completion $\widehat{L}$.

Example 21.3. Let $K = \mathbb{Q}_p$ and $L = \overline{\mathbb{Q}}_p$. Then we can complete it, and it is generally referred to as $\widehat{L} = \widehat{\overline{\mathbb{Q}}}_p = \mathbb{C}_p$.

Any $g \in \mathrm{Gal}(L/K)$ extends continuously to $g \in \mathrm{Aut}(\widehat{L}/K)$. For example, we can define

$$\mathrm{Frob} \in \mathrm{Aut}(\widehat{K}^{\mathrm{unr}}/K).$$

Proposition 21.4. *Let K be local and L/K algebraic. Take any $x \in \widehat{L}$ such that x is separable over L. Then $x \in L$.*

Proof. Let L' be the separable closure of L in $\widehat{L}$. We want to show that L' is a separable extension of L. Then it is normal so L'/L is Galois. Any element $g \in \mathrm{Gal}(L'/L)$ preserves the norm because L'/L is algebraic. Because $L' \subseteq \widehat{L}$, it also preserves the absolute value on L'. Then g is continuous. Because L is dense in L', we have $g = \mathrm{id}_{L'}$. Therefore $L' = L$. □

Let $\varpi = u\pi$.

Lemma 21.5. *There exists a non-unique $\alpha(x) \in \widehat{\mathcal{O}}^{\mathrm{unr}}[[x]]$ such that $\alpha(x) = \epsilon x \bmod \deg 2$ with $\epsilon \in (\widehat{\mathcal{O}}^{\mathrm{unr}})^{\times}$ and*

(a) $\mathrm{Frob}(\alpha) = \alpha^{\varphi} = \alpha \circ [u]_f$,

(b) $\alpha^{\varphi} \circ f = g \circ \alpha$,

(c) $\alpha : F_f \to G_g$ *is a formal group isomorphism,*

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

Proof. I think this is the Lubin–Tate strategy. I am following Milne's notes. First we figure out what we want to take as ϵ. Because we want (a), we need

$$\epsilon^\varphi x = (\epsilon x)^\varphi = (\epsilon x) \circ [u]_f = u\epsilon x \pmod{\deg 2}.$$

This is guaranteed by homework, and we can choose an $\epsilon \in \widehat{\mathcal{O}}^{\mathrm{unr}}$ such that $\epsilon^\varphi/\epsilon = u$. You will even show that this is unique up to multiplication by $\mathcal{O}_K^\times$.

We now build α satisfying (a) inductively. We want polynomials α_n of degree n such that $\alpha_n^\varphi = \alpha_n \circ [u]_f \pmod{\deg(n+1)}$. We already have our basecase. Induction step goes like, if I have α_n we write $\alpha_{n+1} = \alpha_n + cx^{n+1}$. Then we have

$$\alpha_{n+1}^\varphi = \alpha_n^\varphi + c^\varphi x^{n+1},$$
$$\alpha_{n+1} \circ [u]_f = (\alpha_n + cx^{n+1}) \circ [u]_f \equiv \alpha_n \circ [u]_f + cu^{n+1}x^{n+1}.$$

We are good if we can always solve

$$d = cu^{n+1} - c^\varphi.$$

To solve this, change to $b = c\epsilon^{n+1}$. What we want is

$$d = b(u\epsilon)^{n+1} - b^\varphi(\epsilon^\varphi)^{n+1}$$

or $b - b^\varphi = d/(u\epsilon)^{n+1}$. This exist by homework.

Now we have have a power series $\alpha \in \widehat{\mathcal{O}}^{\mathrm{unr}}$ such that $\alpha^\varphi = \alpha \circ [u]_f$. We want $\alpha^\varphi \circ f = g \circ \alpha$ to hold, but it probably doesn't. So we will have to modify $\alpha \mapsto \alpha'$. This is done by $\alpha' = h \circ \alpha$ for some $\mathcal{O}_K[[x]]$.

I want to figure out how badly this fails. Define an auxiliary power series

$$g' = \alpha^\varphi \circ f \circ \alpha^{-1} = \alpha[u]_f \circ f \circ \alpha^{-1}.$$

We want to show that $g' \in \mathcal{O}_K[[x]]$. I also want to show that $g'\mathcal{F}_\varpi$. It suffices to show that $(g')^\varphi = g$. But

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

because f and $[u]_f$ are endomorphisms of F_f. On the other hand, we have

$$g' \equiv \alpha^\varphi \circ x^q \circ \alpha^{-1} \equiv \alpha^\varphi \circ (\alpha^{-1})^q \pmod{\mathfrak{m} = (\pi) = (\varpi)}.$$

But note that $h((x^q))^\varphi \equiv h^q$ for $h \in \widehat{\mathcal{O}}^{\mathrm{unr}}[[x]]$. So we get

$$g' \equiv \alpha^\varphi \circ (\alpha^{-1})^\varphi \circ x^q = x^q \pmod{\varpi}.$$

This shows that $g' \in \mathcal{F}_\varpi$.

Note that we already have $\mathcal{F}_\varpi$. So there exists a power series $[1]_{g,g'} \in \mathcal{O}_K[[x]]$ such that $[1]_{g,g'} \circ g' \circ [1]_{g,g'}^{-1} - g$. Now take

$$\alpha' = [1]_{g,g'} \circ \alpha.$$

Then $g = (\alpha')^\varphi \circ f \circ (\alpha')^{-1}$ and α also satisfies (a). □

22 November 14, 2017

Let K be local fields and π, ϖ be uniformizers. Let f and g be Lubin–Tate series for π and ϖ, with corresponding formal groups F_f and G_g. Let $\widehat{\mathcal{O}}^{\mathrm{unr}}$ be the ring of integers in $\widehat{K}^{\mathrm{unr}}$.

Let $u = \varpi/\pi$. Last time we constructed an $\alpha \in \widehat{\mathcal{O}}^{\mathrm{unr}}[[x]]$ such that

$$\alpha^{\phi} = \alpha \circ [u]_f$$

and α is an isomorphism of formal $\mathcal{O}_K$-modules $F_f \to G_g$. Recall that

$$L^{\pi} = K^{\pi} \cdot K^{\mathrm{unr}}$$

and similarly $L^{\varpi} = K^{\varpi} \cdot K^{\mathrm{unr}}$.

Theorem 22.1. *The two fields L^{π} and L^{ϖ} are actually equal.*

Proof. We are first going to show that the $\widehat{L}^{\pi} = \widehat{L}^{\varpi}$. Then from the lemma last time, L^{π} is the separable closure of L in $\widehat{L}^{\pi}$ and likewise L^{ϖ} is the separable closure of L in $\widehat{L}^{\varpi}$ so we deduce that $L^{\pi} = L^{\varpi}$.

Consider the bijection

$$E_f \xrightarrow{\cong} E_g; \quad x \mapsto \alpha(x).$$

We get that

$$K^{\varpi,n} = K(E_{g,n}) = K(\{\alpha(x) : x \in E_{f,n}\}) \subseteq K^{\pi,n} \cdot \widehat{K}^{\mathrm{unr}}.$$

By symmetry, we get $K^{\varpi,n} \cdot \widehat{K}^{\mathrm{unr}} = K^{\pi,n} \cdot \widehat{K}^{\mathrm{unr}}$. Taking the union over n gives $K^{\varpi} \cdot \widehat{K}^{\mathrm{unr}} = K^{\pi} \cdot \widehat{K}^{\mathrm{unr}}$ and then taking completion gives $\widehat{L}^{\varpi} = \widehat{L}^{\pi}$. □

So the field L^{π} is independent of π. Now we show that the candidate Artin map is also independent of π. Note that we defined the map

$$r_{\pi} : K^{\times} \to \mathrm{Gal}(L^{\pi}/K)$$

as $r_{\pi}(v)|_{K^{\mathrm{unr}}} = \mathrm{id}\,|_{K^{\mathrm{unr}}}$ and $r_{\pi}(v)(x) = [v]_f(x)$ for $x \in E_f$ on $v \in \mathcal{O}_K^{\times}$, and $r_{\pi}(\pi)|_{K^{\mathrm{unr}}} = \mathrm{Frob}$ and $r_{\pi}(\pi)|_{K^{\pi}} = \mathrm{id}\,|_{K^{\pi}}$.

Theorem 22.2. *The two maps r_{π} and r_{ϖ} are equal.*

Proof. Because $K^{\times}$ is generated by uniformizers, it suffices to to show that $r_{\pi}(y) = r_{\varpi}(y)$ for any uniformizers $y \in \mathcal{O}_K$. Then it suffices to show that $r_{\pi}(y) = r_y(y)$ for any uniformizer $y \in \mathcal{O}_K$. Rename $y = \varpi$ and we are going to show that $r_{\pi}(\varpi) = r_{\varpi}(\varpi)$.

We know that

$$r_{\pi}(\varpi)|_{K^{\mathrm{unr}}} = r_{\pi}(u)|_{K^{\mathrm{unr}}} \cdot r_{\pi}(\pi)|_{K^{\mathrm{unr}}} = \mathrm{Frob} = r_{\varpi}(\varpi)|_{K^{\mathrm{unr}}}.$$

Now we need to check that

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

I need to get my hands dirty with formal groups. Let $x \in E_g$ be a torsion element. Then there exists an $x' \in E_f$ such that $x = \alpha(x')$. Because $r_\pi(\varpi)$ acts continuously it extends to $\widehat{K}^{\mathrm{unr}}$ and so we can write

$$\begin{aligned} r_\pi(\varpi)(x) &= r_\pi(\varpi)(\alpha(x')) = (r_\pi(\varpi)(\alpha))(r_\pi(\varpi)(x')) \\ &= \alpha^\phi(r_\pi(u) \circ r_\pi(\pi)(x)) = \alpha^\phi(r_\pi(u)x') = \alpha^\phi([u]_f^{-1}x') = x. \end{aligned}$$

So we get $r_\pi(\varpi) = r_\varpi(\varpi)$ on K^ϖ. □

At this point we are done, because last time we have shown that if L^π and r_π are independent of choice of π, then $L^\pi = K^{\mathrm{ab}}$ and $r_\pi = \theta_{/K}$.

22.1 Artin map and the ramification filtration

Suppose L/K is abelian. We have the Artin map

$$\theta_{L/K} : K^\times \twoheadrightarrow \mathrm{Gal}(L/K), \quad \mathcal{O}_K^\times \twoheadrightarrow I(L/K).$$

Recall that there is a filtration on both $\mathcal{O}_K^\times$ and $I(L/K)$, given by

$$\begin{aligned} U_{K,m} &= \{a \in \mathcal{O}_K^\times : a \equiv 1 \pmod{\pi_K^m}\} \\ G_i(L/K) &= \{g \in I(L/K) : g(\pi_L) \equiv \pi_L \pmod{\pi_L^{i+1}}\}. \end{aligned}$$

We know the successive quotient

$$U_{K,0}/U_{K,1} \cong k^\times, \quad U_{K,m}/U_{K,m+1} \cong k^+$$

for $m \geq 1$, and also

$$G_0/G_1 \hookrightarrow k^\times, \quad G_i/G_{i+1} \hookrightarrow k^+$$

for $i \geq 1$. So we might think that the Artin map relates these two.

Let $L = K^{\pi,n}$ so that L/K is totally ramified. We have

$$\theta_{L/K} : \mathcal{O}_K^\times \to \mathrm{Gal}(L/K) \cong \mathrm{End}(E_{f,n}) \cong \mathcal{O}_K^\times / U_{K,n},$$

with the map being $u \mapsto [u^{-1}]_f \mapsto u^{-1}$. So the kernel of $\theta_{L/K}$ is actually just to be $U_{K,n}$. This shows that

$$G_i = \begin{cases} \mathrm{Gal}(L/K) & i = 0 \\ \theta_{L/K}(U_{K,m}) & q^{m-1} \leq i < q^m \\ 1 & q^n \leq i. \end{cases}$$

Now let us switch to the upper numbering:

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

and we defined

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

In the case $L = K^{\pi,n}$, we have

$$[G_0 : G_i] = [U_{K,0} : U_{K,m}] = \begin{cases} (q-1)q^{m-1} & m \leq n \\ (q-1)q^{n-1} & m > n. \end{cases}$$

So we will get

$$\phi^{-1}(i) = q^{i-1} \text{ for } i = 1, 2, \ldots, n+1.$$

Then

$$G^i(L/K) = G_{q^{i-1}}(L/K) = \theta_{L/K}(U_{K,i}).$$

Proposition 22.3. *If $E/L/K$ is a tower, then*

$$\begin{tikzcd} G^i(E/K) \arrow[r, hookrightarrow] \arrow[d, twoheadrightarrow] & I(E/K) \arrow[d, twoheadrightarrow] \\ G^i(L/K) \arrow[r, hookrightarrow] & I(L/K). \end{tikzcd}$$

You can find this is Neukirch. We can use this to define $G^i(L/K)$ for L infinite, by

$$G^i(L/K) = \varprojlim_{L'} G^i(L'/K).$$

Example 22.4. Taking $L = K^\pi = \bigcup_n K^{\pi,n}$ gives

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

Because $\theta_{K^\pi/K} : \mathcal{O}_K^\times \to \mathrm{Gal}(K^\pi/K)$ is an isomorphism by the construction of Lubin–Tate, we actually have that the two filtrations agree.

Example 22.5. Let us take $L = K^{\mathrm{ab}} = K^\pi \cdot K^{\mathrm{unr}}$ now. We have

$$\begin{tikzcd} I(K^{\mathrm{ab}}/K) \arrow[r, hookrightarrow] & \mathrm{Gal}(K^{\mathrm{ab}}/K) \arrow[r, twoheadrightarrow] & \mathrm{Gal}(K^\pi/K) \\ \mathcal{O}_K^\times \arrow[r, hookrightarrow] \arrow[u, twoheadrightarrow] & K^\times \arrow[r, twoheadrightarrow] \arrow[u, hookrightarrow] & \mathcal{O}_K^\times. \arrow[u, "\cong"] \end{tikzcd}$$

Then $G^i(K^{\mathrm{ab}}/K)$ in $I(K^{\mathrm{ab}}/K)$ corresponds to $G^i(L/K)$ in $\mathrm{Gal}(K^\pi/K)$. Then

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

22.2 Brauer group and central simple algebras

We have been looking at the **Brauer group**

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

This came up in the context of non-commutative algebra. We are now going to give a different definition of the Brauer group. Let K be a field. Some non-commutative algebras over K we might care are

- $n \times n$ matrices $M_n(K)$ over K,
- $\mathbb{H}$ over $\mathbb{R}$,
- $\mathbb{H}_\mathbb{C} = \mathbb{H} \otimes_\mathbb{R} \mathbb{C}$, which actually is isomorphic to $M_2(\mathbb{C})$.

In this sense, $\mathbb{H}$ is a "twist" of $M_2(\mathbb{R})$ because $\mathbb{H} \cong M_2(\mathbb{R})$. We are interested in algebras A/K such that $A \otimes_K \overline{K}$ is isomorphic to some $M_n(\overline{K})$. We are then looking at

$$H^1(K, \mathrm{PGL}_n(K^{\mathrm{sep}})),$$

where $\mathrm{PGL}_n(K^{\mathrm{sep}})$ is a non-abelian $\mathrm{Gal}(K^{\mathrm{sep}}/K)$-module. We can define this, and there is a connecting homomorphism

$$H^1(K, \mathrm{PGL}_n(K^{\mathrm{sep}})) \to H^2(K, (K^{\mathrm{sep}})^\times) = \mathrm{Br}(K).$$

Definition 22.6. An (non-commutative) algebra A/K is **simple** if A has no nontrivial 2-sided ideals.

Example 22.7. $M_n(K)$ is simple. For $a, b \in K^\times$, the algebra

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

is a 4-dimensional simple algebra. If $K = \mathbb{R}$, then $H(-1, -1) = \mathbb{H}$.

Definition 22.8. A **central simple algebra** is a simple algebra that has center K.

We will show that central simple algebras over K are twists of $M_n(K)$, and are classified by $H^2(K, (K^{\mathrm{sep}})^\times)$.

23 November 16, 2017

Recall that a (non-commutative) K-algebra A is

- **simple** if A has no 2-sided ideals other than 0 and A, which is equivalent to any homomorphism $A \to B$ (with $B \neq 0$) being injective,
- **central** if and only if the center is $Z(A) = K$.

For example, if L/K is an extension, then L is a simple K-algebra but L is not a central K-algebra.

Proposition 23.1. *The matrices $M_n(K)$ is central simple.*

Proof. Consider a nonzero ideal $I \subseteq M_n(K)$. Pick a nonzero $a \in I$, and i, j such that $a_{ij} \neq 0$. We can rescale to get $a_{ij} = 1$. If we multiply by the elementary matrices, we get

$$e_{ii} a e_{jj} = e_{ij} \in I.$$

Then we can get $e_{kl} = e_{ki} e_{ij} e_{jl} \in I$ and they generate everything.

If $a \in M_n(K)$ commutes with everything, then $ae_{ii} = e_{ii}a$ implies that a is diagonal, and then $ae_{ij} = e_{ij}a$ implies that all diagonal entries are equal. □

If D is a division algebra (i.e., $x \neq 0$ implies $x^{-1} \in D$), then D is simple over K. This D may or may not be central over K.

Example 23.2. On the current homework you will consider $H(a, b)$, which is $K\langle i, j\rangle$ quotiented out by $i^2 = a$, $j^2 = b$, and $ij = -ji$.

Example 23.3. Let L/K be a cyclic extension and $[L : K] = n$ and $g \in \mathrm{Gal}(L/K)$ a generator. We can define the **cyclic algebra** A_a, a K-algebra generated by L and an additional element γ with

$$\gamma^n = a, \quad \gamma b = (gb)\gamma$$

for $b \in L$. You can check that A_a is central simple with dimension n^2 over K.

If $a' = Nb$ for some $b \in L$, then

$$A_a \to A_{aa'}; \quad L \xrightarrow{\mathrm{id}} L, \quad \gamma_a \mapsto b^{-1}\gamma_{a'}$$

is an isomorphism. So the isomorphism class of A_a depends only on the class of $a \in K^\times/NL^\times = H^2(L/K, L^\times)$. Also, for $a = 1$ we have

$$A_1 \cong \mathrm{End}_K(L) \cong M_n(K); \quad \ell \mapsto m_\ell, \quad \gamma \mapsto g.$$

This is injective by linear independence of automorphisms and then is an isomorphism by a dimension argument.

23.1 Tensor product of central simple algebras

One useful fact is that if L/K is an extension, then we can base change from K to L.

Proposition 23.4. *If $A \otimes_K L$ is a simple L-algebra, then A is a simple K-algebra.*

Proof. If $I \subseteq A$ is an ideal, then $I \otimes_K L \subseteq A \otimes_K L$ is an ideal and so either $I \otimes_K L = 0$ or $I \otimes_K L = A \otimes_K L$. □

The converse is not true. Consider $A = \mathbb{C}$ as a simple $\mathbb{R}$-algebra. Then $A \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$ is not simple.

Proposition 23.5. *If A is central simple, then $A \otimes_K L$ is simple. (In fact, it is central simple over L.)*

Theorem 23.6. *If A, B are K-algberas, with A central simple and B simple, then $A \otimes_K B$ is simple.*

Proof. Let us take an ideal $I \subseteq A \otimes_K B$ and assume $I \neq 0$. We need to show that $I = A \otimes_K B$. Take an element $a_1 \otimes b_1 + \cdots + a_n \otimes b_n \in I$ that is nonzero, so that the number of terms is fewest possible.

First of all we can take $a_1 = 1$. This is because $Aa_1A = A$ by simplicity of A and so we can scale. The resulting thing is nonzero because we have started out with a minimal presentation. Let $a \in A$ be arbitrary. Then

$$\begin{aligned}(a \otimes 1)(1 \otimes b_1 + \cdots + a_n \otimes b_n) - (1 \otimes b_1 + \cdots + a_n \otimes b_n)(a \otimes 1)\\ = (aa_2 - a_2a) \otimes b_2 + \cdots + (aa_n - a_na) \otimes b_n \in I.\end{aligned}$$

Because $b_2, \dots, b_n$ are linearly independent, we have that $a_2, \dots, a_n$ all commute with a. Then $a_2, \dots, a_n \in Z(A) = K$ and so we get $n = 1$.

Now $1 \otimes b \in I$ and $1 \supseteq 1 \otimes BbB = 1 \otimes B$ because B is simple. So $I = A \otimes B$. □

You can show as an exercise that if A, B are K-algebra, then $Z(A \otimes_K B) = Z(A) \otimes_K Z(B)$.

Corollary 23.7. *If A and B are central simple, then $A \otimes_K B$ is central simple. That is, (finite-dimensional) central simple algebras form an abelian monoid under $\otimes$.*

The matrices algebras $\{M_n(K)\}$ form a sub-monoid, because $M_n(K) \otimes_K M_m(K) \cong M_{nm}(K)$.

Definition 23.8. We define the **Brauer group** as

$$\operatorname{Br}(K) = (\text{f.d. CSAs } /K)/(\text{matrix algebras } /K).$$

To show that this is indeed a group, we consider the opposite algebra A^{op} such that $a \cdot_{A^{\text{op}}} b = b \cdot_A a$. Clearly A is central/simple if and only if A^{op} is central/simple.

Proposition 23.9. *For finite-dimensional central simple A over K, $A \otimes_K A^{\mathrm{op}}$ is isomorphic to $\mathrm{End}_K(A)$ where A is regarded as K-vector spaces.*

Proof. We define

$$\varphi : A \otimes_K A^{\mathrm{op}} \to \mathrm{End}_K(A); \quad a \otimes 1 \mapsto l_a, \quad 1 \otimes a \mapsto r_a$$

where $l_a a' = aa'$ and $r_a a' = a'a$. Because $A \otimes A^{\mathrm{op}}$ is central simple, φ is injective. To show that φ is surjective, we just count dimension. □

Corollary 23.10. *The Brauer group $\mathrm{Br}(K)$ is actually a group, with $[A]^{-1} = [A^{\mathrm{op}}]$.*

23.2 Structure theorem for central simple algebras

We define the Brauer group, we don't have any machinery to compute it. Our next goal is to show that if A is a central simple algebra over K, then $A = M_n(D)$ where D is a division algebra over K. If we have this, then in the Brauer group,

$$[A] = [M_n(K) \otimes_K D] = [D].$$

Definition 23.11. Let A be a K-algebra and M be a left A-module. We say that M is

- **simple** if M has no submodules other than 0 and M.
- **semisimple** if $M = \bigoplus M_i$ where M_i are simple.
- **decomposable** if $M = M_1 \oplus M_2$ for some proper $M_1, M_2 \subsetneq M$.

If A is a K-algebra, then A can be considered as a left A-module over itself, as ${}_AA$. The algebra A being simple *does not* imply that ${}_AA$ is simple as a left A-module. This is because submodules are just left ideals.

Lemma 23.12 (Schur's lemma)**.** *If S is a simple A-module, then $\mathrm{End}_A(S)$ is a division algebra.*

Proof. Suppose $\varphi \in \mathrm{End}_A(S)$ is nonzero. Then $\ker(\varphi) = 0$ and $\mathrm{im}(\varphi) = S$. So φ is invertible. □

Proposition 23.13. *Let D be a division algebra. Then all finitely generated D-modules are isomorphic to D^n.*

Proof. You can basically do the same proof as for vector spaces over a field. □

Let us try to figure out $\mathrm{End}_A({}_AA)$. We have

$$\mathrm{End}_A({}_AA) \cong \{a \mapsto ab : b \in A\} \cong A^{\mathrm{op}}.$$

As a consequence, if M is a free A-module of rank n, then

$$\mathrm{End}_A(M) = \mathrm{End}_A({}_AA^{\oplus n}) \cong M_n(A)^{\mathrm{op}} \cong M_n(A^{\mathrm{op}}).$$

Theorem 23.14 (Double centralizer)**.** *Let V be a finite-dimensional vector space over K. Let $A \subseteq \operatorname{End}_K(V)$ be a simple subalgebra. We define the **centralizer** as*

$$C(A) = \{b \in \operatorname{End}_K(V) : ba = ab \text{ for all } a \in A\}.$$

Then $C(C(A)) = A$.

Proof. See Milne's notes on class field theory. □

Let us now prove the classification theorem. Let A be a central simple K-algebra. Choose a nonzero simple A-module S. (Consider the minimal nonzero submodule of ${}_AA$.) This gives an embedding, because (A is simple),

$$A \hookrightarrow \operatorname{End}_K(S); \quad a \mapsto l_a.$$

The centralizer is going to be

$$D = C(A) = \operatorname{End}_A(S)$$

a division algebra by Schur. By the double centralizer theorem, we get

$$A = C(D) = \operatorname{End}_D(S) \cong M_n(D^{\mathrm{op}}).$$

This is because S over D should be isomorphic to some D^n.

Theorem 23.15 (Structure theorem)**.** *If A is central simple algebra, it is isomorphic to $M_n(D)$ for some division algebra D.*

24 November 21, 2017

Last time we showed that if A is a central simple algebra over K then $A \cong M_n(D)$. In fact, n and D are uniquely determined up to isomorphism. Recall that we have constructed D as, when S is a simple module over A, $D \cong \mathrm{End}_A(S)^{\mathrm{op}}$.

24.1 Modules over simple algebras

Simple algebras are the nicest things you could have after fields. There is going to be a unique finitely generated simple module S over A, and every module is going to be S^n for some n.

First step in proving this is to decompose ${}_A A$ as a direct sum of simple submodules. Note that $Z(A)$ is always a field, and so the classification gives $A \cong M_n(D)$ for some division ring D. Then

$$ {}_A A \cong M_n(D) \cong S_1 \oplus \cdots \oplus S_n $$

where S_i is the matrices with 0 off the ith columns. These are all simple modules, and so it is a direct sum of n copies of the simple module S.

Assume that S' is any other simple A-module. Take a nonzero $s' \in S'$. There is a map

$$ \varphi : {}_A A \to S'; \quad a \mapsto as' $$

which is a left A-module homomorphism. But note that ${}_A A \cong \bigoplus_i S_i$. This shows that

$$ \varphi_i : S_i \to S' $$

is nonzero for some i. Then Schur's lemma tells us that φ_i is an isomorphism.

For a general finitely generated A-module, we use a similar argument. Take a surjective morphism $A^n \to M$, and we can show that this can be restricted to an isomorphism $S^m \to M$ for some m.

Proposition 24.1. *Let A be a simple algebra. There is a unique finitely generated simple module S over A, and any finitely generated module over A is isomorphic to S^n for some n.*

So the S that is simple over A is unique, and so D is uniquely determined. Then $n^2 = [A : K]/[D : K]$ and so n is determined.

Example 24.2. We have $\mathrm{Br}(K) = 0$ if K is algebraically closed. To prove this, it suffices to show that if D/K is a finite dimensional division algebra over K, then $D = K$. Take $x \in D$ and let $f(x)$ be the minimal polynomial of x over K. Note that $K(x)$ is a commutative subalgebra. By assumption that D is a division algebra, f is linear and so $x \in K$.

Example 24.3. We have $\mathrm{Br}(\mathbb{F}_q) = 0$. This follows from Wedderburn's theorem, which states that any finite division algebra is a field.

Example 24.4. We have $\mathrm{Br}(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. The proof again is by classification of division algebras over $\mathbb{R}$. The only ones are $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$. But $\mathbb{C}$ doesn't count because it is not central.

24.2 Extension of base fields

This is something we observed last time. We have a map

$$\{\text{CSAs over } K\} \to \{\text{CSAs over } L\}; \quad A \mapsto A \otimes_K L.$$

This descends to a map

$$\mathrm{Br}(K) \to \mathrm{Br}(L).$$

Definition 24.5. The **Brauer group** $\mathrm{Br}(L/K)$ is defined as $\ker(\mathrm{Br}(K) \to \mathrm{Br}(L))$. This is the subgroup of classes such that $A \otimes_K L \cong M_n(L)$. This condition is called "A is split by L", and is only dependent on the class of A.

Any central simple algebra A/K is split by $\overline{K}$ because $\mathrm{Br}(\overline{K}) = 0$. So we get

$$\dim_K A = \dim_{\overline{K}} A \otimes_K \overline{K} = \dim_{\overline{K}} M_n(\overline{K}) = n^2.$$

Proposition 24.6. *There always exists a finite extension L/K such that A is split by L.*

Proof. We have an isomorphism $M_n(\overline{K}) \to A \otimes_K \overline{K}$, and the standard bases e_{ij} will be sent to some linear combination $\sum_k a_{ijk} \otimes x_{ijk}$. Then we can take $K(x_{ijk})$ and then the isomorphism restricts to $M_n(L) \to A \otimes_K L$. □

So

$$\mathrm{Br}(K) = \bigcup_{L/K \text{ fin.}} \mathrm{Br}(L/K) = \bigcup_{L/K \text{ fin. Gal.}} \mathrm{Br}(L/K).$$

If L/K is finite Galois, our goal is to prove $\mathrm{Br}(L/K) \cong H^2(L/K, L^\times)$.

If A is a central simple algebra over K, how can we tell which L/K split A? There is going to be a nice answer to this. Let's look at the quaternions over $K = \mathbb{Q}$. This is $A = H(-1,-1)$ over $\mathbb{Q}$. If $L/\mathbb{Q}$ is finite, then

$$A \otimes_{\mathbb{Q}} L = H_L(-1,-1).$$

You have worked out in the homework how to tell if $H_L(-1,-1)$ is split or not. This is split if and only if the quadratic form

$$x^2 + y^2 + z^2 = 0$$

has a nontrivial solution, or equivalently,

$$x^2 + y^2 + z^2 + w^2 = 0$$

has a nontrivial solution. Let us consider only $L = \mathbb{Q}[\sqrt{D}]$. If $D > 0$, then $L \hookrightarrow \mathbb{R}$ and so these have no nontrivial solutions in L. If $D < 0$ and $-D = x^2 + y^2 + z^2$ for $x, y, z \in \mathbb{Q}$, then $x^2 + y^2 + z^2 + (\sqrt{D})^2 = 0$ is a nontrivial solution and so L splits A. Actually this condition is equivalent to D not being of the form $4^n(8a+1)$. In this case, you can show that $x^2 + y^2 + z^2 = 0$ has no nontrivial solution by working 2-adically. So the conclusion is that $\mathbb{Q}[\sqrt{D}]$ splits $H(-1,-1)$ if and only if $-D$ is a sum of three squares.

Theorem 24.7 (Double centralizer)**.** *Let A be central simple algebra, and let $B \subseteq A$ be a simple algebra. Then $C = C(B)$ is simple and $C(C) = B$. Also we have $[A : K] = [B : K][C : K]$.*

If $B \subseteq A$ is not simple, there is a counterexample. Let $A = M_n(K)$ and $B \subseteq A$ be the upper triangular matrices. Then $C = K$ and $C(C) = M_n(K) \neq B$.

Proof. Again, this is in Milne. □

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

Proof. In general, $Z(B) = B \cap C$. But then $Z(C) = B \cap C = Z(B) = K$. For the next part, note that $B \otimes_K C$ is a central simple algebra over K. Then $B \otimes_K C \hookrightarrow A$ and then this is an isomorphism by looking at dimension. □

Corollary 24.9. *If A is a central simple algebra over K and $L \subseteq A$ is a field. The following are equivalent:*

(a) $L = C(L)$

(b) $[L : K]^2 = [A : K]$

(c) L is a maximal commutative sub K-algebra of A.

Proof. (a) to (b) is implied by the dimension part of the double centralizer theorem. For (b) to (c), consider L' a maximal commutative K-subalgebra containing L. Then

$$[L' : K]^2 \leq [L' : K][C(L') : K] = [A : K] = [L : K]^2.$$

So $L' = L$ and L is maximal. For (c) to (a), we have that for all $x \in C(L)$, $L[x]$ is commutative and so $L[x] = L$. This implies that $C(L) = L$. □

If D is a division algebra, then (c) is equivalent to that L is a maximal commutative subfield of A. In other words, all maximal subfields of D have degree $\sqrt{[D : K]}$.

Theorem 24.10. *The field L splits A if and only if there exists a B such that $[B] = [A]$ in $\mathrm{Br}(K)$, $B \supseteq L$, and $[B : K] = [L : K]^2$.*

Proof. If L splits A, it also splits A^{op}. Then

$$A^{\mathrm{op}} \otimes_K L \cong \mathrm{End}_L(V)$$

for some vector space L of dimension $\dim_L V = n$. Then $\dim_K A^{\mathrm{op}} = \dim_K A = n^2$. Let B be the centralizer of A^{op} inside $\mathrm{End}_K(V)$. Because A^{op} and $\mathrm{End}_K(V)$ are both central simple over K, we have that B is central simple over K. Then

$$A^{\mathrm{op}} \otimes_K B \cong \mathrm{End}_K(V)$$

and so $[B] = -[A^{\mathrm{op}}] = [A]$ in $\mathrm{Br}(K)$. We certainly have that $L \subseteq B$ because L commutes with everything in A^{op}, and $[B : K] = [\mathrm{End}_K(V) : K]/[A^{\mathrm{op}} : K] = [L : K]^2$.

To prove the other direction, it is enough to show that L splits B. Let $[L : K] = n$ and $[B : K] = n^2$. We want $B \otimes_K L \cong \mathrm{End}_L(V)$ for some V, with $\dim_L V = n$. We use $V = B$, where the action of L is by right multiplication $(l \cdot b = bl)$. Consider

$$B \otimes_K L \to \mathrm{End}_L(V); \quad b \otimes 1 \mapsto l_b, \quad 1 \otimes l \mapsto r_l$$

where $l_\bullet$ and $r_\bullet$ are left and right multiplication maps. We know that $B \otimes_K L$ is central simple over L, so this should be injective. Dimension counting shows that this is an isomorphism. □

25 November 28, 2017

Last time we showed the following theorem.

Theorem 25.1. *The field L splits A if and only if there exists a B such that $[B] = [A]$ in $\mathrm{Br}(K)$, $B \supseteq L$, and $[B : K] = [L : K]^2$.*

Corollary 25.2. *Let D be a division algebra with center K. If $[L : K] = \sqrt{[D : K]}$, then L splits D if and only if L embeds in D.*

Here the only thing that has correct dimension is D.

25.1 Noether–Skolem theorem

I have one more algebraic input before we can classify central simple algebras.

Theorem 25.3 (Noether–Skolem)**.** *Let A be a simple algebra over K and B be a central simple algebra over K. Then any two homomorphism $f, g : A \to B$ are conjugate, i.e., there exists a $b \in B$ such that $f(a) = bg(a)b^{-1}$ for all $a \in A$.*

Example 25.4. For example, we can take $A = B$ central simple and $g = \mathrm{id} : B \to B$. Then any automorphism $f : B \to B$ is conjugation by an element of b, or inner.

Example 25.5. Let L/K be a finite extension assume L splits B and $[B : K] = [L : K]^2$. If f, g are embeddings $L \hookrightarrow B$, then f and g are conjugate. If L/K is Galois, we can precompose $L \hookrightarrow B$ by any element of $\mathrm{Gal}(L/K)$. They are going to be related by a conjugation by some element in B.

Proof of Noether–Skolem. First assume that $B = M_n(K) \cong \mathrm{End}_K(K^n)$. Let $f, g : A \to B$ be maps. Define two A-modules M_1 and M_2, both K^n as K-modules but

$$M_1 : a *_1 v = f(a)v, \quad a *_2 v = g(a)v$$

for $a \in A$. But because A is simple, recall that A-modules are completely classified by their dimension. So there exists an isomorphism

$$\varphi : M_1 \to M_2.$$

Because φ is K-linear, we can view φ as an element of $M_n(K) = B$. Here, this φ being an isomorphism means that

$$f(a)(\varphi v) = \varphi(g(a)v)$$

So $f(a) = \varphi g(a) \varphi^{-1}$ and take $b = \varphi$.

Now let B be an arbitrary central simple algebra over K. We are going to enlarge B to make it a matrix algebra. We know that $B \otimes_K B^{\mathrm{op}} \cong \mathrm{End}_K(B)$. We have two maps

$$f \otimes 1, g \otimes 1 : A \otimes_K B^{\mathrm{op}} \to B \otimes_K B^{\mathrm{op}} \cong \mathrm{End}_K(B).$$

The domain is still simple and the codomain is a matrix algebra. So these must be conjugate by some $x \in B \otimes_K B^{\mathrm{op}}$ so that

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

for all $a \in A$ and $b' \in B^{\mathrm{op}}$. Setting $a = 1$ shows that x commutes with $1 \otimes b'$ for all $b \in B^{\mathrm{op}}$, so $x \in B \otimes 1$ because B^{op} is central. If we write $x = b \otimes 1$ then b has the desired property. □

25.2 Classification of central simple algebras

Let L/K be a finite Galois extension. Let

$$\mathcal{A}(L/K) = \{\text{central simple } A/K : A \text{ is split by } L, [A : K] = [L : K]^2\}/\text{isomorphism}$$

Then we have a bijection

$$\mathcal{A}(L/K) \to \mathrm{Br}(L/K) \subseteq \mathrm{Br}(K); \quad A \mapsto [A].$$

Now we are going to construct a bijection

$$\mathcal{A}(L/K) \to H^2(L/K, L^\times).$$

Write $G = \mathrm{Gal}(L/K)$. Recall the inhomogeneous cocycles and coboundaries

$$\begin{aligned} Z^2(L/K, L^\times) &= \{g_1\varphi(g_2, g_3) \cdot \varphi(g_1, g_2g_3) = \varphi(g_1g_2, g_3) \cdot \varphi(g_1, g_2)\} \\ B^2(L/K, L^\times) &= \{\gamma(g, h) = (g\psi(h) \cdot \psi(g))/\psi(gh)\}. \end{aligned}$$

For an arbitrary $A \in \mathcal{A}(L/k)$, pick an embedding $i : L \hookrightarrow K$. By the Noether–Skolem theorem, for any $g \in G$ there exists an $a_g \in A$ such that

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

for all $x \in L$. How unique is a_g? Recall that if $[A : K] = [L : K]^2$ then $C(L) = L$. So a_g is unique up to left multiplication by elements of $L^\times$.

Let us compare a_{gh} and $a_g a_h$. Here, we have

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

So a_{gh} and $a_g a_h$ are the same up to some element of L. Define $\varphi(g, h)$ so that

$$a_g a_h = \phi(g, h) a_{gh}.$$

The cocycle condition comes from associativity. If we expand $a_{g_1} a_{g_2} a_{g_3}$, then

$$a_{g_1}(\varphi(g_2, g_3) a_{g_2g_3}) = g_1(\varphi(g_2, g_3)) a_{g_1} a_{g_2g_3} = g_1(\varphi(g_2, g_3))\gamma(g_1, g_2g_3) a_{g_1g_2g_3}$$

equals

$$\varphi(g_1, g_2) a_{g_1g_2} a_{g_3} = \varphi(g_1, g_2)\varphi(g_1g_2, g_3) a_{g_1g_2g_3}.$$

This is precisely that φ is a cocycle.

On the other hand, a_g are unique up to multiplication by $L^\times$. So if a'_g is another choice of such elements, we should be able to write $a'_g = \psi(g)a_g$. It turns out that

$$\varphi_{a'}/\varphi_a = d\psi$$

is a coboundary. So we have a well-defined cohomology class

$$\mathcal{A}(L/K) \to H^2(L/K, L^\times).$$

Now I want to construct an inverse. This is straightforward because I know exactly what to do. Suppose I have received an arbitrary cocycle $\varphi \in H^2(L/K, L^\times)$ and I want to defined a K-algebra A_ϕ by

$$A_\varphi = \bigoplus_{g \in G} L \cdot e_g$$

with relations $e_g \cdot x = g(x)e_g$ for all $x \in L$ and

$$e_g \cdot e_h = \varphi(g, h)e_{gh}.$$

This defines a K-algebra, with identity element $e_1/\varphi(1, 1)$. It can be shown that this only depends on the cohomology class $[\varphi] \in H^2(L/K, L^\times)$. So we have a candidate for a map $H^2(L/K, L^\times) \to \mathcal{A}(L/K)$, but we need to show that it is central simple over K.

Proposition 25.6. *A_φ is central simple.*

Proof. The central part is straightforward, because if something commutes L, it must be in $L \cdot e_1$, and then if it commutes with e_g, it should be in K.

Now we need to show that it is simple. Suppose we have a nonzero ideal $I \subsetneq A_\varphi$. Take nonzero $a \in I$ with

$$a = x_1 e_{g_1} + \cdots + x_k e_{g_k}$$

for nonzero x_i such that k is minimal. If $k = 1$, we would get everything so we must have $k \geq 2$. Without loss of generality assume that $g_1 = 1$. Take $l \in L$ such that $g_2 l \neq l$. Then

$$al - la = x_1 e_2 l + x_2 e_{g_2} l + \cdots - l x_1 e_1 - l x_2 e_{g_2} - \cdots = x_2(g_2(l) - l)e_{g_2} + \cdots \in I$$

has fewer terms and is nonzero. □

So we have maps $\mathcal{A}(L/K) \to H^2(L/K, L^\times)$ and $H^2(L/K, L^\times) \to \mathcal{A}(L/K)$. We check that they are inverses. One direction is straightforward. If $A \in \mathcal{A}(L/K)$ and φ_A is the cocycle I get from A, then we have an algebra homomorphism $A_\varphi \to A$ given by sending $e_\varphi \mapsto a_\varphi$. Because A_φ is central simple, it is an isomorphism by dimension counting.

26 November 30, 2017

At the end of last time, we have reached the dramatic conclusion of this topic.

Proposition 26.1. *There is a natural bijection*

$$\mathrm{Br}(L/K) \quad \longleftrightarrow \quad H^2(L/K, L^\times)$$

via the set $\mathcal{A}(L/K)$ of algebras split by L of dimension $[L:K]^2$.

Theorem 26.2. *This bijection preserves the group structure.*

Proof. The proof is a bit painful. For cocycles φ_1 and φ_2, we know how to add them and get $\varphi_1+\varphi_2$, and we know how to construct $A_{\varphi_1}\otimes A_{\varphi_2}$ and $A_{\varphi_1+\varphi_2}$. We can show that

$$A_{\varphi_1}\otimes A_{\varphi_2} \cong A_{\varphi_1+\varphi_2}\otimes M_n(K).$$

This is messy. □

Proposition 26.3. *Assume $E/L/K$ with E/K Galois. Then the diagram*

$$\begin{tikzcd}
\mathrm{Br}(L/K) \arrow[r, "\cong"] \arrow[d, hook] & H^2(L/K, L^\times) \arrow[d, "\mathrm{inf}"] \\
\mathrm{Br}(E/K) \arrow[r, "\cong"] & H^2(E/K, E^\times)
\end{tikzcd}$$

commutes.

In particular, we have

$$\begin{aligned}\mathrm{Br}(K) &= \bigcup_{L/K\ \mathrm{Gal}} \mathrm{Br}(L/K) = \varinjlim_{L/K} \mathrm{Br}(L/K) \\ &\cong \varinjlim_{L/K} H^2(L/K, L^\times) = H^2(K, (K^{\mathrm{sep}})^\times).\end{aligned}$$

Corollary 26.4. *If $[L:K]=n$, then $\mathrm{Br}(L/K)\cong H^2(L/K,L^\times)$ is n-torsion. So $\mathrm{Br}(K)$ is also torsion.*

26.1 Fields with trivial Brauer group

We have seen a couple of examples already. We've seen that if K is separably closed, then $\mathrm{Br}(K)=0$. The other example I have given was $K=\mathbb{F}_q$.

Note that $\mathrm{Br}(K)=0$ is equivalent to that any central division algebra over K is K. The tool for studying division algebras is reduced norm. This might be familiar in the context of quaternions:

$$\mathbb{H}^\times \to \mathbb{R}^\times; \quad a+bi+cj+dk \to a^2+b^2+c^2+d^2.$$

Suppose D is a central division algebra over K. Let's say that L is a Galois extension such that L splits D. Then there is an isomorphism

$$D \otimes L \xrightarrow{\varphi} M_n(L).$$

Then we can define

$$N_{\mathrm{rd}}(d) = \det(\varphi(d \otimes 1)) \in L^\times.$$

Proposition 26.5. *For $g \in \mathrm{Gal}(L/K)$, we have $g(N_{\mathrm{rd}}(d)) = N_{\mathrm{rd}}(d)$. That is, $N_{\mathrm{rd}}(d) \in K^\times$.*

Proof. We use the Noether–Skolem theorem. For A a simple L-algebra, any two L-algebra maps $A \to M_n(L)$ are conjugate by some $b \in M_n(L)$. Take $A = D \otimes L$, and consider them map

$$\varphi_g : D \otimes L \to M_n(L); \quad d \otimes \ell \mapsto g\varphi(d \otimes g^{-1}l)$$

So if we evaluate at $d \otimes 1$ and take determinant, we get

$$N_{\mathrm{rd}}(d) = \det \varphi(d \otimes 1) = \det g\varphi(d \otimes 1) = gN_{\mathrm{rd}}(d). \qquad \square$$

Note that so far everything works for D not only a division algebra but also any central simple algebra. Let $[D : K] = n^2$ and consider $d_1, \dots, d_{n^2}$ a K-basis for D. We can take the reduced norm

$$f(c_1, \dots, c_{n^2}) = N_{\mathrm{rd}}\left(\sum_{i=1}^{n^2} c_i d_i\right) \in K[c_1, \dots, c_{n^2}]$$

which is a homogeneous polynomial in the c_is of degree n. For a nonzero $v = (v_1, \dots, v_{n^2}) \in K^{n^2}$, we have $f(v) \neq 0$ because D is a division algebra. So we have a low degree homogeneous polynomial with many variables, such that it has no nontrivial zeros.

Definition 26.6. A field K is called **quasi-algebraically closed** if any homogeneous polynomial $f \in K[x_1, \dots, x_N]$ of degree $d < N$ has a nonzero solution in K^N.

If K is quasi-algebraically closed, then any central division algebra D/K should have degree $n = n^2$ and so $D = K$.

Proposition 26.7 (Chevalley–Warning theorem)**.** *Finite fields $\mathbb{F}_q$ are quasi-algebraically closed.*

Proof. The original theorem states that if f is a homogeneous polynomial in $\mathbb{F}_q[x_1, \dots, x_N]$ of degree $d < N$, then the number of solutions is a multiple of $p = \mathrm{char}\, \mathbb{F}_q$. So there should be at least one solution other than 0.

The idea is that

$$\sum_{v \in \mathbb{F}_q^n} (1 - f(v)^{q-1})$$

is congruent to the number of solutions modulo p. Then you expand this out and write things as sums of characters. $\square$

Clearly algebraically closed field are quasi-algebraically closed.

Theorem 26.8 (Tsen's theorem)**.** *The power series ring $\mathbb{C}((t))$ is quasi-algebraically closed. More generally, the fraction field of any complete DVR with algebraically closed residue field is quasi-algebraically closed.*

Theorem 26.9. *If K is a local field, then K^{unr} is quasi-algebraically closed.*

Theorem 26.10 (Lang)**.** *If K is quasi-algebraically closed, any algebraic L/K is also quasi-algebraically closed.*

If K is quasi-algebraically closed, then $H^2(K,(K^{\text{sep}})^\times) = 0$. For L/K, we also have $H^2(L,(K^{\text{sep}})^\times) = 0$. It is also true that the corresponding H^1 vanish by Hilbert 90, and this is also true for all subextensions. So by Tate's theorem, we have that all

$$\hat{H}^q(K,(K^{\text{sep}})^\times) = 0.$$

This shows that for any L/K finite, the map $N : L^\times \to K^\times$ is surjective.

26.2 Brauer groups of local fields

Let $K = \mathbb{R}$. We can compute the Brauer group

$$H^2(\mathbb{R},\mathbb{C}^\times) \cong \hat{H}^0(\mathbb{R},\mathbb{C}^\times) = \mathbb{R}^\times/N\mathbb{C}^\times \cong \{\pm 1\}.$$

Previously we have computed this invoking the classification of central simple algebras over $\mathbb{R}$, but we can now do this using cohomology.

Suppose now that K is a non-archemedian local field. We should have

$$\text{inv} : \text{Br}(K) \cong H^2(K,(K^{\text{sep}})^\times) \cong \mathbb{Q}/\mathbb{Z}.$$

This should give, in some sense, the classification of central simple algebras. For any $x \in \text{Br}(K)$, there exists an unramified extension L such that

$$x \in \text{Br}(L/K) = \ker(\text{Br}(K) \xrightarrow{\text{Res}} \text{Br}(L)).$$

This is because, under the identification of $\text{Br}(K) \cong \mathbb{Q}/\mathbb{Z}$, it is multiplication by $n = [L : K]$. So $x \in \text{Br}(K/L)$ for some sufficiently large $n = [L : K]$. Here, L/K is cyclic, so we can understand $H^2(K,L^\times) \cong \hat{H}^0(K,L^\times) \cong K^\times/NL^\times$.

But we can understand also from the division algebra side. Let D be a central division algebra over K, and let L be its maximal subfield. Then $[D : K] = n^2$ and $[L : K] = n$. We can extend the absolute value $|-|_K$ to D, by

$$|a|_D = |N_{\text{rn}}(a)|_K^{1/n}.$$

Then this is a non-archemedian absolute value. We can likewise extend

$$v : D^\times \to \frac{1}{n}\mathbb{Z}$$

and define **ramification degree** $e = [v(D^\times) : v(K^\times)]$.

We can define

$$\mathcal{O}_D = \{a \in D : v(a) \geq 0\}, \quad \mathfrak{p}_D = \{a \in D : v(a) \geq \tfrac{1}{n}\}.$$

Then this is a principal idea $\mathfrak{p}_D = \pi_D \mathcal{O}_D = \mathcal{O}_D \pi_D$. Then $k_D = \mathcal{O}_D/\mathfrak{p}_D$ is a division ring that is finite over $k = \mathcal{O}_K/\mathfrak{p}_K \cong \mathbb{F}_q$. In particular, k_D/k is a finite extension of finite fields. So we can define **inertia degree** $f = [k_D : k]$.

Using the exactly same proof as in the case of fields, we can show that

$$ef = [D : K] = n^2.$$

But note that $e \mid n$, because $v : D^\times \to \frac{1}{n}\mathbb{Z}$. Also, we have $f \leq n$, because if $\overline{a}$ is a primitive element of k_D then $a \in \mathcal{O}_D$ has minimal polynomial degree at least f, but a maximal subfield of D has degree n. So $f \leq n$ and $e \mid n$. We therefore get

$$e = f = n.$$

Now when $\overline{a}$ generates k_D/k, and a lifts $\overline{a}$, the field $K(a)$ is unramified and splits D. By Noether–Skolem there exists some $b \in D$ such that

$$\mathrm{Frob}_{K(a)/K}(x) = bxb^{-1}.$$

Then another way to define the invariant map is

$$\mathrm{inv}([D]) = [v(b)] \in \tfrac{1}{n}\mathbb{Z}/\mathbb{Z} \subseteq \mathbb{Q}/\mathbb{Z}.$$

What happens when K is a global field? Here the Brauer group is computed too, and there exists a short exact sequence

$$0 \to \mathrm{Br}(K) \to \bigoplus_v \mathrm{Br}(K_v) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

We are going to do this next semester. In particular, if $[H] \in \mathrm{Br}(K)$ is some quaternion algebra, this says that the number of v such that $H \otimes_K K_v$ is not split is finite and even. This really quadratic reciprocity, when applied to $H(p, q)$.

Index

absolute value, 9
    non-archemedian, 9
additive group, 69
adele ring, 6
adelic class group, 7
Artin map, 6, 49
augmentation ideal, 29

bar resolution, 34
Brauer group, 49, 88, 92

central simple algebra, 86
centralizer, 90
Chevalley–Warning theorem, 99
class field, 4
coinduction, 31
coinflation, 42
compatible pair, 41
completion, 10
corestriction, 42
crossed homomorphism, 36

decomposition group, 23
discrete valuation ring, 10

Eisenstein polynomial, 25
exponential, 18

formal group
    homomorphism, 73
formal group law, 72
formal module, 76
free module, 31
Frobenius element, 5

G-module, 29
    discrete, 50
Galois cohomology, 49
global field, 17
group cohomology, 33
group homology, 39
group ring, 29

Hensel's lemma, 11
Herbrand quotient, 57
Hilbert 90, 49
homogeneous cochain, 35

indecomposable module, 89
induction, 31
inertia degree, 14, 101
inertia group, 24
    tame, 27
    wild, 27
inflation, 41
inhomogeneous cochain, 36
invariant map, 53

Kronecker–Weber theorem, 5

local field, 16
logarithm, 19
Lubin–Tate series, 74

multiplicative group, 70

Noether–Skolem theorem, 95
norm, 13
norm residue symbol, 62
Normal basis theorem, 49
normic, 64

Ostrowski's theorem, 9

p-adic integer, 6
place, 10
product formula, 17
profinite completion, 66
profinite group, 50

quasi-algebraically closed, 99

ramification group, 26
ramification index, 14, 100
restriction, 41

semidirect product, 37
semisimple module, 89
simple algebra, 86
simple module, 89
standard normalization, 16

standard resolution, 34

tamely ramified, 27
Tate cohomology, 44
Tate's theorem, 59
torsor, 37
Tsen's theorem, 100

universal norm, 64
unramified extension, 19
upper numbering, 28

valuation, 9