Classes: Mo/Fr 10:30 - 11:45am

Section: Th 1:30-2:45pm

Fabian's OH: Mo, Fr noon-1pm
or appointment

Kenz's OH: Tu 1:30-2:45pm

Grading: 70% HW
30% final paper

0. Motivation

0.1. Generalizing quadratic reciprocity

Let $p \neq 2$ be a prime number.

<u>Def</u> An integer a is a <u>quadratic residue mod p</u> if $a \equiv x^2 \bmod p$ for some $x \in \mathbb{Z}$.

<u>Lemma 0.1</u>

$$a^{\frac{p-1}{2}} \equiv \underbrace{\left\{\begin{matrix} 0, & a \equiv 0 \bmod p \\ +1, & a \not\equiv 0 \text{ quadr. res. mod } p \\ -1, & a (\not\equiv 0) \text{ not quadr. res. mod } p \end{matrix}\right\} \bmod p}_{\underline{\text{Legendre symbol}} \ \left(\frac{a}{p}\right)}$$

<u>Pf</u> Let $a \not\equiv 0 \bmod p$.

$$\Rightarrow \left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \underset{\substack{\uparrow \\ \text{little Fermat}}}{\equiv} 1 \mod p$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1 .$$

If $a \equiv x^2$, then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv +1$.

The polynomial $a^{\frac{p-1}{2}} - 1$ has at most $\frac{p-1}{2}$ roots in $\mathbb{F}_p^\times$.

But $\begin{array}{ccc} \mathbb{F}_p^\times & \longrightarrow & \mathbb{F}_p^\times \\ x & \longmapsto & x^2 \end{array}$ has kernel $\{\pm 1\}$, so its image has size $\dfrac{\# \mathbb{F}_p^\times}{2} = \dfrac{p-1}{2}$.

$\Rightarrow$ There are $\frac{p-1}{2}$ quadr. res. mod p.

nonzero

$$\Rightarrow a^{\frac{p-1}{2}} \not\equiv 1 \text{ if } a \text{ is not a quadr. res.}$$

$$\Downarrow$$

$$a^{\frac{p-1}{2}} \equiv -1 \qquad \square$$

__Obviously__, $\left(\frac{a}{p}\right)$ is periodic in a for fixed p: depends only on a mod p.

__Surprisingly__, $\left(\frac{a}{p}\right)$ is "periodic in p" for fixed a: depends only on p mod $4a$.

__Ex__ $\left(\frac{1}{p}\right) = +1$ for any p

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ only depends on p mod 4.

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ only depends on p mod 8.

One way to show "periodic in p":

Quadratic reciprocity law

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$ for all odd primes $p \neq q$.

Sadly, whether 5 is a cubic residue mod p ($\exists x \in \mathbb{Z} : x^3 \equiv 5 \bmod p$) is not "periodic in p": doesn't depend only on p mod n for any fixed $n \geq 1$.

Interestingly, the number of roots mod p of x^3-3x+1 depends only on p mod 9.

Questions Why? Which polynomials behave "periodically in p"? What's the period? Can we generalize quadr. reciprocity? Can we generalize to number fields other than $\mathbb{Q}$? ...

0.2. Local-global principle

For example, fix a polynomial

$$f(X_1,\dots,X_n) \in \mathbb{Z}[X_1,\dots,X_n].$$

Let $V(R) = \{(x_1,\dots,x_n) \in R^n \mid f(x_1,\dots,x_n) = 0\}$

for any ring R.

$V(\mathbb{Z}) \neq \emptyset$? ($\Leftrightarrow$ $f(x_1,\dots,x_n)=0$ has integer sol.)

$$\Downarrow$$

Ex $X_1^2 + X_2^2 + 1 = 0$ ↯ (no real sol.)

Ex $X_1^2 + 3X_2^2 - 2 = 0$ $\Rightarrow x_1^2 \equiv 2 \bmod 3$ ↯ (no sol. mod 3)

$V(\mathbb{R}) \neq \emptyset$ and $V(\mathbb{Z}/n\mathbb{Z}) \neq \emptyset$ $\forall n \geq 1$ ($\Leftrightarrow$ $f \equiv 0$ has sol. mod n)

$$\Updownarrow \text{ Chinese remainder theorem}$$

$$V(\mathbb{Z}/p^k\mathbb{Z}) \neq \emptyset \ \forall k \geq 0 \ \forall \text{prime } p.$$

Collect "compatible" residues mod powers of a fixed prime p:

Def The **ring of p-adic integers $\mathbb{Z}_p$** consists of sequences $(a_0, a_1, \dots) = (a_k)_{k \geq 0} \in \prod_{k \geq 0} \mathbb{Z}/p^k\mathbb{Z}$ of residue classes $a_k \in \mathbb{Z}/p^k\mathbb{Z}$ such that

$$a_k \equiv a_l \bmod p^k \text{ for } k < l.$$

Addition and multiplication are defined element-wise:

$$(a_n)_{n\geq 0} \underset{\cdot}{+} (b_n)_{n\geq 0} = (a_n \underset{\cdot}{+} b_n)_{n\geq 0} .$$

Rmk The natural map $\mathbb{Z} \longrightarrow \mathbb{Z}_p$

$x \longmapsto (x \bmod p^k)_{k\geq 0}$

is injective, so we'll say $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Pf If $x \equiv y \bmod p^k$ but $x \neq y$, then $|x-y| \geq p^k$. □

can't be true for all k.

Cor If $V(\mathbb{Z}) \neq \emptyset$, then $\underbrace{V(\mathbb{R}) \neq \emptyset \text{ and } V(\mathbb{Z}_p) \neq \emptyset\ \forall p}_{V(\mathbb{R} \times \prod_p \mathbb{Z}_p) \neq \emptyset}$.

"global"
(undecidable)

"local"
(easier)

If the converse holds, we say that V satisfies the local-global principle (also called Hasse principle).

Ex $V = \{x \mid x^n = a\}$ satisfies the local-global principle (over $\mathbb{Z}$) for any fixed $n \geq 1$ and $a \in \mathbb{Z}$.

Ex $V = \{x \mid (x^2+1)(x^2+\overset{17}{\cancel{3}})(x^2-\overset{17}{\cancel{3}}) = 0\}$ doesn't!

Ex (Minkowski)

For any homogeneous degree 2 polynomial $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$,

$V = \{(x_1, \dots, x_n) \mid f(x_1, \dots, x_n) = 0, (x_1, \dots, x_n) \neq (0, \dots, 0)\}$

satisfies the local-global principle.

Ex (Selmer)

$V = \{(x,y,z) \mid 3x^3 + 4y^3 + 5z^3 = 0, (x,y,z) \neq (0,0,0)\}$

doesn't!

Goal: Study the ring $\mathbb{Z}_p$ and its field of fractions $\mathbb{Q}_p$. (For example, how to tell whether $V(\mathbb{Z}_p) \neq \emptyset$?) Identify some more problems that satisfy a local-global principle.

"$\mathbb{R} = \mathbb{Z}_\infty$"

Def The ring of profinite integers $\hat{\mathbb{Z}}$ consists of sequences $(a_1, a_2, \dots) = (a_n)_{n \geq 1} \in \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$ of residue classes $a_n \in \mathbb{Z}/n\mathbb{Z}$ such that $a_n \equiv a_m \mod n$ for all $n \mid m$.

Thm (Chinese remainder theorem)

The natural map

$$\hat{\mathbb{Z}} \longrightarrow \prod_p \mathbb{Z}_p$$

$$(a_n)_{n \geq 1} \longmapsto \left((a_{p^k})_{k \geq 0} \right)_p$$

(~~forgetting~~ residues mod non-prime-powers) is an isomorphism.

We write $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

1. Local fields

1.0. Reminder on Dedekind domains

Def A Dedekind domain is an integral domain R (which is not a field) in which any nonzero ideal I factors uniquely as a product of prime ideals.

Ex Any principal ideal domain, e.g. $\mathbb{Z}$ or $K[T]$ for any field K.

Notation If $\mathcal{O}_K$ is a ring, denote its field of fractions by K. If $L|K$ is a field ext., we denote the integral closure of $\mathcal{O}_K$ in L by $\mathcal{O}_L$.

Rmk If $\mathcal{O}_K$ is a Dedekind dom. and $L|K$ is a finite ext., then $\mathcal{O}_L$ is also a Dedekind dom.

Ex The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain.

1.1. Valuations

<u>Def</u> Let K be a field. A valuation on K is a map

$v: K \longrightarrow \mathbb{R}\cup\{\infty\}$ such that:

a) $v(x)=\infty \iff x=0$

b) $v(xy)=v(x)+v(y)$ (i.e. $v: K^\times \to \mathbb{R}$ is a group hom.)

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

It is discrete if

d) $v(K^\times)=s\cdot\mathbb{Z}\subset\mathbb{R}$ for some $s\geq 0$.

(i.e. $v(K^\times)\subset\mathbb{R}$ is a discrete subgroup)

It is a normalised discrete valuation if

e) $v(K^\times)=\mathbb{Z}$. Then, any $\pi\in K^\times$ with $v(\pi)=1$ is called a uniformiser. We denote one of them by π_v.

Ex Trivial valuation: $v(x)=0 \quad \forall x\in K^\times$

Rmk If v is a (disc.) val., then so is $\lambda\cdot v$ for any $\lambda>0$.

Main example If $\mathcal{O}_K$ is a Dedekind domain and $\mathfrak{p}$ is a prime (= nonzero prime ideal), then

$$v_{\mathfrak{p}}(x)=\sup\{n\in\mathbb{Z} \mid x\in\mathfrak{p}^n\}$$

= number of times x is divisible by $\mathfrak{p}$

= exponent of $\mathfrak{p}$ in the factorization of (x)

defines a normalized discrete valuation on K, called the $\mathfrak{p}$-adic valuation.

Rmk Any valuation satisfies:

i) $v(1) = v(-1) = 0$

ii) If $v(x) \neq v(y)$, then equality holds in c):

$$v(x+y) = \min(v(x), v(y)).$$

Pf i) grp. hom. $\Rightarrow v(1) = 0$

$$(-1)^2 = 1 \Rightarrow 2v(-1) = v(1) = 0$$

ii) Say $v(x) < v(y)$ and assume

$$v(x+y) > \min(v(x), v(y)) = v(x)$$

$$\Rightarrow v(x) = v((x+y)+(-y)) \underset{c)}{\geq} \min(v(x+y), \underbrace{v(-y)}_{v(-1)+v(y)=v(y)}) > v(x)$$

$\lightning$

$\square$

Defthm Let v be a valuation. Then

$\mathcal{O}_v := \{x \in K \mid v(x) \geq 0\}$ is a local ring

(the valuation ring)

with field of fractions K, unit group $\mathcal{O}_v^\times = \{x \in K \mid v(x) = 0\}$, (unique) maximal ideal $\mathfrak{p}_v := \{x \in K \mid v(x) > 0\}$, and residue field $\kappa_v := \mathcal{O}_v / \mathfrak{p}_v$.

Thm If v is a normalized disc. val., then $\mathcal{O}_v$ is a PID: Any ideal is of the form

$$\{x \in K \mid v(x) \geq n\} = \mathfrak{p}_v^n = (x_0) \quad \text{for some } n \geq 0$$

for any $x_0 \in K$ with $v(x_0) = n$.

In particular, $\mathfrak{p}_v = (\pi_v)$.

Pf Consider any ideal I. Let $n = \min_{x \in I} v(x)$ and choose any $x_0' \in I$ with $v(x_0') = n$. Then,

$$I \supseteq (x_0') = \{x \in K \mid v(x) \geq n\} \supseteq I,$$

so $I = (x_0')$. For any $x_0 \in K$ with $v(x_0) = n$, we have $v\left(\frac{x_0}{x_0'}\right) = 0$, so $\frac{x_0}{x_0'} \in \mathcal{O}_v^\times$, so $(x_0) = (x_0') = I$.

In particular $\mathfrak{p}_v = (\pi_v)$.

$\Rightarrow \mathfrak{p}_v^n = (\pi_v^n)$ and $v(\pi_v^n) = n$. □

<u>Lemma</u> If v is the $\mathfrak{p}$-adic valuation for a prime $\mathfrak{p}$ in a Ded. dom. $\mathcal{O}_K$, then $\mathcal{O}_v$ is the <u>localization</u> of $\mathcal{O}_v$ at $\mathfrak{p}$ and we have $\mathfrak{p}_v = \mathfrak{p}\,\mathcal{O}_v$ and

$$\mathcal{O}_v/\mathfrak{p}_v^n \cong \mathcal{O}_K/\mathfrak{p}^n$$
$$x \bmod \mathfrak{p}_v^n \longleftarrow\!\!\!\shortmid\; x \bmod \mathfrak{p}^n$$

for any $n \geq 0$. Also, v is the $\underset{\hat{\mathcal{O}}_v}{\hat{\mathfrak{p}}_v}$-adic valuation.

<u>Ex</u> $\mathcal{O}_K = \mathbb{Z}$, $K = \mathbb{Q}$, $v = v_p$ (p-adic val.)

$\Rightarrow \mathcal{O}_v = \mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ b \not\equiv 0 \bmod p \right\} \subset \mathbb{Q}$

$\mathcal{O}_v^\times = \mathbb{Z}_{(p)}^\times = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ a, b \not\equiv 0 \bmod p \right\} \subset \mathbb{Q}$

$\mathfrak{p}_v = p\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z},\ a \equiv 0 \bmod p,\ b \not\equiv 0 \bmod p \right\} \subset \mathbb{Q}$

$\pi_v =$ for example p, $-p$.

$$\mathbb{Z}_{(p)}/p^n\mathbb{Z}_{(p)} \cong \mathbb{Z}/p^n\mathbb{Z}$$
$$x \longleftarrow\!\!\!\shortmid\; x$$
$$\frac{a}{b} \longmapsto a \cdot b^{-1} \bmod p^n$$

(note that b is invertible mod p^n because $b \not\equiv 0 \bmod p$)

Lemma Let v be a norm. disc. val.

Look at the filtration

$$\mathcal{O}_v \supseteq \mathfrak{p}_v \supseteq \mathfrak{p}_v^2 \supseteq \dots$$

We have $\mathfrak{p}_v^a/\mathfrak{p}_v^b \cong \mathcal{O}_v/\mathfrak{p}_v^{b-a}$ as groups

$$\pi_v^a \cdot x \longleftarrow\!\shortmid \; x$$

for any $a \le b$.

Rmk The isom. depends on π_v.

Lemma Let v be a norm. disc. val.

Look at the filtration

$$\mathcal{O}_v^\times \supseteq U^{(1)} \supseteq U^{(2)} \supseteq \dots$$

with $U^{(n)} = 1 + \mathfrak{p}_v^n$.

We have

a) $\mathcal{O}_v^\times / U^{(n)} \cong (\mathcal{O}_v/\mathfrak{p}_v^n)^\times$ as a group

$$x \cdot U^{(n)} \longmapsto x \bmod \mathfrak{p}_v^n$$

b) $U^{(n)}/U^{(n+1)} \cong \mathcal{O}_v/\mathfrak{p}_v = k_v$ as a group

$$1 + \pi_v^n x \longleftarrow\!\shortmid \; x$$

Rmk The isom. in b) depend on π_v.

Pf b) $f : \mathcal{O}_v \longrightarrow U^{(n)}/U^{(n+1)}$ is a group homomorphism:

$$x \longmapsto 1 + \pi_v^n x$$

$$\frac{f(x)\,f(y)}{f(x+y)} = \frac{(1+\pi^n x)(1+\pi^n y)}{1+\pi^n(x+y)}$$

$$= \frac{1+\pi^n(x+y)+\pi^{2n}xy}{1+\pi^n(x+y)} = 1+\frac{\pi^{2n}xy}{1+\pi^n(x+y)}$$

$$\equiv 1 \mod \mathfrak{p}_v^{n+1}.$$

$$\Rightarrow \frac{f(x)f(y)}{f(x+y)} \in U^{(n+1)} \Rightarrow f \text{ is a grp. hom.}$$

f is clearly surj. because $\mathfrak{p}_v^n = (\pi_v^n)$.

$\ker(f) = \mathfrak{p}_v$. $\square$

Let's see what valuations there are in a few examples of fields K!

<u>Thm 1.1</u> Any normalized disc. val. v on $\mathbb{Q}$ is of the form $v = v_p$ for some prime number p.

<u>Pf</u> For $x = \pm \prod_p p^{e_p} \in \mathbb{Q}^\times$, we have

$$v(x) = \sum_p e_p \cdot v(p).$$

$\Rightarrow$ Valuation is determined by $v(p)$ for the prime numbers p.

$\mathcal{O}_v = \{x \in \mathbb{Q} \mid v(x) \geq 0\}$ is a subring of $\mathbb{Q}$, so $\mathbb{Z} \subset \mathcal{O}_v$. $\Rightarrow v(p) \geq 0$.

$\mathfrak{p}_v \cap \mathbb{Z} = \{x \in \mathbb{Z} \mid v(x) > 0\}$ is a prime ideal of $\mathbb{Z}$.

$\Rightarrow v(p) > 0$ for (at most) one prime number p and $v(q) = 0$ for all $q \neq p$.

v normalized $\Rightarrow v(p) = 1$. $\Rightarrow v = v_p$ (p-adic val.)

$\square$

Thm A finite field $\mathbb{F}_q$ has no nontriv. val.

Pf For any $x \in \mathbb{F}_q^\times$, $x^{q-1} = 1$.

$\Rightarrow (q-1)v(x) = v(1) = 0. \Rightarrow v(x) = 0.$ □

Thm An algebraically closed field K has no nontriv. disc. val.

Pf Assume v is a norm. disc. val.

$v(\pi_v) = 1. \Rightarrow v(\sqrt{\pi_v}) = \frac{1}{2} \notin \mathbb{Z}.$

$\Rightarrow$ not normalized. □

Thm Let k be a field that has no nontriv. disc. val. Then, the norm. disc. val. of $K = k(T)$ are:

- $v = v_{f(T)}$, the $f(T)$-adic val. for some irred. monic pol. $f(T) \in k[T]$.

  $\uparrow$ the Dedekind dom.

- $v = v_{deg}$ given by

$$v_{deg}\left(\frac{a(T)}{b(T)}\right) = deg(b(T)) - deg(a(T))$$

for $a(T), b(T) \in k(T)$.

Rmk v_{deg} is the $(\frac{1}{T})$-adic val. for the ideal $(\frac{1}{T})$ of the Ded. dom. $k[\frac{1}{T}]$.

Pf of rmk

Write $a(T) = T^{deg(a)} \cdot \tilde{a}(T)$

$b(T) = T^{deg(b)} \cdot \tilde{b}(T)$

with $\tilde{a}(T), \tilde{b}(T) \in k[\frac{1}{T}]$ with nonzero const. coeff.

$v_{\frac{1}{T}}(a(T)) = -deg(a) + 0 = -deg(a)$

$v_{\frac{1}{T}}(b(T)) = -deg(b)$.

$\Rightarrow v_{\frac{1}{T}}\left(\frac{a(T)}{b(T)}\right) = deg(b) - deg(a)$.

□

Thm Let k be a field that has no nontriv. disc. val.
Then, the norm. disc. val. of $K = k(T)$ are:

- $f(T)$-adic val. for irred. $f(T) \in k[T]$
- $v_{\deg}$: $\frac{1}{T}$-adic val. $\left(\left(\frac{1}{T}\right) \subset k\left[\frac{1}{T}\right] \right)$.

Geometric intuition

Interpret any $g(T) \in k(T)$ as a "function" on the projective line $\mathbb{P}^1 = k \cup \{\infty\}$.

Then, $v_{x-a}(g) =$ order of vanishing of $g(T)$ at $T = a$
(< 0 if pole)

$v_{\infty}(g) = v_{\deg}(g) =$ order of vanishing of $g(T)$ at $T = \infty$.

Pf $v|_k$ is a disc. val. on k, so $v|_k$ is the triv. val.: $v(x)=0 \ \forall x \in k^\times$.

$\Rightarrow k \subseteq \mathcal{O}_v$.

Case 1: $v(T) \geq 0$

$\Rightarrow k[T] \subseteq \mathcal{O}_v$.

Like in Thm 1.1. (for $\mathbb{Q}$), it follows that $v = v_{f(T)}$ for some irred. $f(T)$.

Case: $v(T) < 0$

$\Rightarrow k[\frac{1}{T}] \subseteq \mathcal{O}_v$

and $\mathfrak{p}_v \cap k[\frac{1}{T}] \subseteq k[\frac{1}{T}]$ prime ideal containing $\frac{1}{T}$.

$\Rightarrow \mathfrak{p}_v \cap k[\frac{1}{T}] = (\frac{1}{T})$.

Like in Thm 1.1., it follows that $v = v_{\deg}$.

□

1.2. Topology

Let v be any valuation on K.

Fix any $\lambda > 1$. (If the res. field is $k_v = \mathbb{F}_q$, one usually picks $\lambda = q$.)

Then, $|x| = \lambda^{-v(x)}$ defines a norm on K:

a) $|x| = 0 \iff x = 0$

b) $|xy| = |x| \cdot |y|$

c) $|x+y| \leq \max(|x|, |y|)$

(stronger than the triangle inequality: $|x+y| \leq |x| + |y|$.

$\rightsquigarrow$ <u>nonarchimedean</u> norm).

<u>Rmk</u> x close to y $\iff$ $v(x-y)$ large ($|x-y|$ small)

$$\underset{\substack{\uparrow \\ \text{if } v = v_{\mathfrak{p}}}}{\iff} \quad x \equiv y \mod \mathfrak{p}^n \text{ for large } n.$$

<u>Rmk</u> The topology induced by $|\cdot|$ is indep. of λ.

Thm This makes K a topological field:

$$+ : K \times K \to K,\ (x,y) \mapsto x+y, \quad \times : K \times K \to K,\ (x,y) \mapsto xy, \quad \cdot^{-1} : K^\times \to K^\times,\ x \mapsto x^{-1}$$

are continuous.

1.3. Completion

Def/thm Let v be any norm. disc. val. on K. We call K complete w.r.t. v if every Cauchy seq. in K converges in K. The completion of K w.r.t. v is the field $\hat{K}_v$ consisting of Cauchy seq. in K modulo seq. converging to 0.

Extend $|\cdot|$ to $\hat{K}_v$ by $\left|\lim_{n\to\infty} a_n\right| := \lim_{n\to\infty} |a_n|$.

Extend v to a val. on $\hat{K}_v$ by

$$v(\lim_{n\to\infty} a_n) := \lim_{n\to\infty} v(a_n).$$

Note that v is still norm. disc. because $v(\hat{K}^\times) = \mathbb{Z}$ is disrete in $\mathbb{R}$.

We let $\hat{\mathcal{O}}_v := \{x \in \hat{K}_v \mid v(x) \geq 0\}$,

$\hat{\mathfrak{p}}_v := \{x \in \hat{K}_v \mid v(x) > 0\}$.

Lemma We have
$$\begin{array}{ccc} \hat{\mathcal{O}}_v/\hat{\mathfrak{p}}_v^n & \cong & \mathcal{O}_v/\mathfrak{p}_v^n \\ x & \mapsfrom & x \end{array}$$

for all $n \geq 0$ and $\hat{\mathfrak{p}}_v = \mathfrak{p}_v \hat{\mathcal{O}}_v$.

Lemma Let $(a_n)_{n\geq 0}$ with $a_n \in \hat{K}_v$.

The series $\sum_{n=0}^{\infty} a_n$ converges (in $\hat{K}_v$)

if and only if $a_n \xrightarrow[n\to\infty]{} 0$.

Pf "⇐" The partial sums $\sum_{n=0}^{M} a_n$ form a

Cauchy seq. because
$$\left|\sum_{n=N}^{M} a_n\right| \leq \max_{N\leq n\leq M} |a_n| \xrightarrow[N\to\infty]{} 0.$$

"⇒" as for $\mathbb{R}$. □

Lemma Let $S \subseteq \mathcal{O}_v$ be a set containing exactly one representative of each residue class in $\kappa_v = \mathcal{O}_v/\mathfrak{p}_v$. Then, each $x \in \hat{\mathcal{O}}_v$ can be written uniquely as

$$x = \sum_{i=0}^{\infty} a_i \pi_v^i \quad \text{with } a_i \in S.$$

"digits"

We have $x \in \hat{\mathcal{O}}_v^\times \iff a_0 \not\equiv 0 \bmod \mathfrak{p}_v$.

Each $x \in \hat{K}_v^\times$ can be written uniquely as

$$x = \sum_{i=-r}^{\infty} a_i \pi_v^i \text{ with } r \in \mathbb{Z},\ a_i \in S,$$
$$a_{-r} \not\equiv 0 \bmod \mathfrak{p}_v.$$

Pf For $x \in \hat{\mathcal{O}}_v$:

$$a_0 \equiv x \bmod \hat{\mathfrak{p}}_v$$

$$a_1 \equiv \frac{x - a_0}{\pi_v} \bmod \hat{\mathfrak{p}}_v$$

$$a_2 \equiv \frac{x - a_0 - a_1\pi_v}{\pi_v^2} \bmod \hat{\mathfrak{p}}_v$$

$$\vdots$$

$$x \in \hat{\mathcal{O}}_v^\times \iff v(x) = 0 \iff \overset{\overset{a_0}{\equiv}}{x} \not\equiv 0 \bmod \mathfrak{p}_v.$$

For $x \in \hat{K}_v^\times$, just look at $\frac{x}{\pi_v^{v(x)}} \in \hat{\mathcal{O}}_v^\times$.

$\square$

Ex $K = \mathbb{Q}$, $v = v_p$ (p-adic val.)

$\rightsquigarrow$ field of p-adic rationals $\mathbb{Q}_p = \hat{K}_v$

ring of p-adic integers $\mathbb{Z}_p = \hat{\mathcal{O}}_v$.

Let $S = \{0, \dots, p-1\}$ (repr. for el. of $\mathbb{Z}/p\mathbb{Z}$).

$$\Rightarrow \mathbb{Z}_p = \left\{ \sum_{i=0}^{\infty} a_i p^i \;\middle|\; a_i \in \{0, \dots, p-1\} \right\}$$

$$= \{ \dots a_2 a_1 a_0 \mid \text{—''—} \}$$

Addition / mult. with carry like in $\mathbb{Z}$.

Unit $\Leftrightarrow$ last digit $a_0 \neq 0$.

For example,

$-1 = \dots 444$ in $\mathbb{Z}_5$

$\frac{1}{2} = \dots 223$ in $\mathbb{Z}_5$.

$\mathbb{Q}_p = \{ \dots a_2 a_1 a_0 . a_{-1} a_{-2} \dots a_{-r} \}$.

Ex k any field, $K = k(T)$, $v = v_T$ (T-adic val.)

$\Rightarrow \hat{\mathcal{O}}_v = k[[T]]$ ring of power series

$\hat{K}_v = k((T))$ field of Laurent series.

Pf The residue field is $\kappa_v = k[T]/(T) = k \subset K$, so take $S = \kappa_v$ and $\pi_v = T$.

$\Rightarrow$ Every elt. of $\hat{\mathcal{O}}_v$ is

$$\sum_{i=0}^{\infty} a_i T^i \text{ with } a_i \in k.$$

Every el. of $\hat{K}_v$ is

$$\sum_{i=-r}^{\infty} a_i T^i \text{ with } a_i \in k. \qquad \square$$

The def. of $\mathbb{Z}_p$ agrees with that given in section 0.2:

<u>Thm</u> Denote by $\underbrace{\varprojlim_{n}}_{\text{“inverse limit”}} \mathcal{O}_v/\mathfrak{p}_v^n$ the set of $(a_n)_{n\geq 0} \in \prod_{n \geq 0} \mathcal{O}_v/\mathfrak{p}_v^n$ such that $a_n \equiv a_m \mod \mathfrak{p}_v^n$ for all $n \leq m$.
Equip each $\mathcal{O}_v/\mathfrak{p}_v^n$ with the discrete top.,
$\prod_{n\geq 0} \mathcal{O}_v/\mathfrak{p}_v^n$ with the prod. top.,
$\varprojlim \mathcal{O}_v/\mathfrak{p}_v^n$ with the subspace top.

Then, the map

$$\hat{\mathcal{O}}_v \longrightarrow \varprojlim_{n\to\infty} \mathcal{O}_v/\mathfrak{p}_v^n$$
$$x \longmapsto (x \bmod \mathfrak{p}_v^n)_n$$

is a homeomorphism.

REFERENCE: Neukirch, Algebraic Number Theory, Section II.

1.4. Nonarchimedean local fields

Def A (nonarch.) local field is a field K with a disc. val. v such that K complete w.r.t. v and the res. field κ_v is finite.

$$\mathcal{O}_K := \mathcal{O}_v, \quad \pi_K := \pi_v, \quad \ldots, \quad q_K := |\kappa_v|.$$

$\kappa_v = \mathbb{F}_{q_K}$.

Lemma If K is a nonarch. loc. field, then $\mathcal{O}_K$ is compact. (See also problem 5 on PSet 1.)

Pf $\kappa_v = \mathbb{F}_q. \Rightarrow \#(\mathcal{O}_v/\mathfrak{p}_v^n) = q^n < \infty$

$\Rightarrow \mathcal{O}_v/\mathfrak{p}_v^n$ compact

$\Rightarrow \prod_{n \geq 0} \mathcal{O}_v/\mathfrak{p}_v^n$ compact

$\Rightarrow \mathcal{O}_v = \varprojlim \mathcal{O}_v/\mathfrak{p}_v^n$ compact.

$\uparrow$

$\varprojlim \mathcal{O}_v/\mathfrak{p}_v^n$ is a closed subset of $\prod \mathcal{O}_v/\mathfrak{p}_v^n$

$\square$

Cor $\mathfrak{p}_v^n$ is a compact open closed subset of K for all $n \in \mathbb{Z}$.

Pf
$$\mathfrak{p}_v^n = \{x \in K \mid v(x) \geq n\}$$
$$= \{x \in K \mid |x| \leq \lambda^{-n}\} \quad \text{closed}$$
$$= \{x \in K \mid |x| < R\} \quad \text{open}$$

for R slightly larger than λ^{-n}.

$\mathcal{O}_v$ cpt., $\mathfrak{p}_v^n = \pi_v^n \cdot \mathcal{O}_v$

$\Rightarrow \mathfrak{p}_v^n$ cpt. □

Cor K is locally cpt.

Pf For any $x \in K$, the set $x + \mathcal{O}_v$ is a cpt. open closed nbhd. of x. □

Def The <u>archimedean local fields</u> are $\mathbb{R}$, $\mathbb{C}$.

1.5. Hensel's lemma

Let K be complete w.r.t. a disc. val. v.

Hensel's lemma ($\overset{V1}{\text{version}}$ 1)

Let $f(X) \in \mathcal{O}_v[X]$ and assume $\alpha \in \underset{\mathcal{O}_v/\mathfrak{p}_v}{\underset{\parallel}{k_v}}$

is a *simple* root of $(f(X) \bmod \mathfrak{p}_v) \in k_v[X]$.

Then, there is exactly one root $\beta \in \mathcal{O}_v$ of $f(X)$ such that $\beta \equiv \alpha \bmod \mathfrak{p}_v$ (a *lift* of α).

Ex If $p \neq 2$ is a prime number and $a \not\equiv 0 \bmod p$ is a quadr. res. mod p, then $\sqrt{a} \in \mathbb{Z}_p$.

Pf (assuming V1)

$f(X) = X^2 - a$ has a root $\overset{\alpha \in \mathbb{F}_p}{\text{mod}}$ p.

$f'(\alpha) = 2\alpha \not\equiv 0 \bmod p \Rightarrow$ *simple* root

$$\underset{\boxed{p \neq 2,\ \alpha \not\equiv 0}}{\uparrow}$$

$\Rightarrow f(X) = X^2 - a$ has a root in $\mathbb{Z}_p$. □

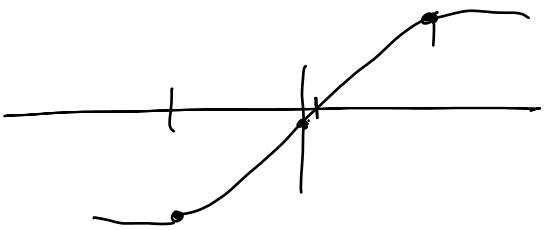
<u>Ex</u> $X^2 - 3$ has a (non-simple) root mod 3, but $\sqrt{3} \notin \mathbb{Z}_3$.

$X^2 - 3$ has a (non-simple) root mod 2, but no root mod 4.

$\Rightarrow \sqrt{3} \notin \mathbb{Z}_2$.

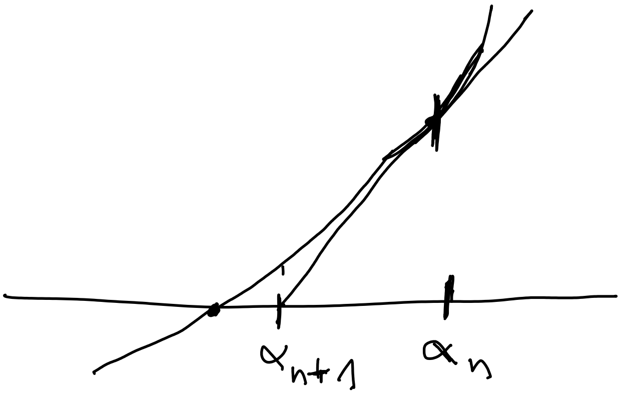
Finding roots over $\mathbb{R}$

- Intermediate value theorem



Doesn't work over $\mathbb{C}$, $\mathbb{Q}_p$ because there's no good ordering.

- Newton's method



Applies over $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}_p$, ...

$\underbrace{\phantom{\mathbb{Q}_p}}$

Hensel's lemma (V2)

Hensel's lemma (V2)

Let $f(X) \in \mathcal{O}_v[X]$ and assume $\alpha \in \mathcal{O}_v$ satisfies

$$v(f(\alpha)) > 2v(f'(\alpha)) \qquad (\mathrm{I})$$

$$|f(\alpha)| < |f'(\alpha)|^2$$

Then, there is exactly one root $\beta \in \mathcal{O}_v$ of $f(x)$ such that $v(\beta - \alpha) > v(f'(\alpha))$.

$$|\beta - \alpha) \quad < |f'(\alpha)|$$

It actually satisfies $v(\beta - \alpha) \geq v(f(\alpha)) - v(f'(\alpha)) \underset{(\mathrm{I})}{>} v(f'(\alpha))$.

$$|\beta - \alpha| \leq \left| \frac{f(\alpha)}{f'(\alpha)} \right| .$$

Ex $\sqrt{\underset{-7}{\cancel{9}}} \in \mathbb{Z}_2$ Okay, $\sqrt{9}$ is a little silly. ☺

Pf (assuming V2)

$$f(X) = X^2 \cancel{-9} + 7$$

$$v_2(f(1)) = v_2(8) = 3$$

$$v_2(f'(1)) = v_2(2) = 1. \qquad \square$$

Pf that V2 ⇒ V1

α root mod $\mathfrak{p}$ $\Rightarrow v(f(\alpha)) \geq 1$

α simple root mod $\mathfrak{p}$ $\Rightarrow v(f'(\alpha)) = 0.$ $\square$

Pf of V2

Existence

Let $\alpha_0 = \alpha$.

Let $\alpha_1 = \alpha_0 + t_1$ for some $t_1 \in \mathcal{O}_v$.

$$\left[\text{"} f(\alpha_1) = f(\alpha_0 + t_1) = f(\alpha_0) + t \cdot f'(\alpha_0) + \mathcal{O}(t^2) \text{"} \right]$$

Write $f(X) = \sum c_i X^i$.

$$\Rightarrow f(\alpha_1) = f(\alpha_0 + t_1) = \sum c_i (\alpha_0 + t_1)^i$$

$$= \sum c_i \left(\alpha_0^i + i \alpha_0^{i-1} \cdot t_1 + \ldots t_1^2 + \ldots \right)$$

$$\equiv \sum c_i \left(\alpha_0^i + i \alpha_0^{i-1} \cdot t_1 \right) \equiv \sum c_i \alpha_0^i + \sum i c_i \alpha_0^{i-1} t_1$$

$$\equiv f(\alpha_0) + t_1 \cdot f'(\alpha_0) \qquad \text{mod } t_1^2$$

Pick $t_1 = - \dfrac{f(\alpha_0)}{f'(\alpha_0)} \in \mathcal{O}_v$.

$$\Rightarrow f(\alpha_1) \equiv 0 \quad \text{mod } t_1^2 .$$

$$\Rightarrow v(f(\alpha_1)) \geq 2 v(t_1) = 2v(f(\alpha_0)) - 2v(f'(\alpha_0))$$

$$\underset{(I)}{>} v(f(\alpha_0))$$

$$f'(\alpha_1) = f'(\alpha_0 + t_1) \equiv f'(\alpha_0) \quad \text{mod } t_1 .$$

$\Rightarrow v(f'(\alpha_1)) \geq \min(v(f'(\alpha_0)), v(t_1))$ with equality if $v(f'(\alpha_0)) < v(t_1)$.

Indeed, $v(t_1) = v(f(\alpha_0)) - v(f'(\alpha_0)) \underset{(I)}{>} v(f'(\alpha_0))$.

$\Rightarrow v(f'(\alpha_1)) = v(f'(\alpha_0))$.

$\Rightarrow \alpha_1$ still satisfies (I) and we can continue:

$\alpha_2 = \alpha_1 + t_2, \quad \alpha_3 = \alpha_2 + t_3, \ldots$

We have shown that

$v(f(\alpha_0)) < v(f(\alpha_1)) < \ldots \quad \Rightarrow \quad f(\alpha_n) \xrightarrow{n\to\infty} 0$

$v(f'(\alpha_0)) = v(f'(\alpha_1)) = \ldots$

$v(t_1) < v(t_2) < \ldots \quad \Rightarrow \quad t_n \xrightarrow{n\to\infty} 0$

We have $\alpha_n = \alpha_0 + t_1 + \ldots + t_n$.

$\Rightarrow \beta = \lim\limits_{n\to\infty} \alpha_n = \alpha_0 + \sum\limits_{n=0}^{\infty} \underset{\overset{\downarrow}{0}}{t_n}$ exists in $\mathcal{O}_v$.

$$f(\beta) = f(\lim \alpha_n) = \lim f(\alpha_n) = 0.$$

Also $v(\beta - \alpha_0) = v(\sum t_n) \geq v(t_1)$

$= v(f(\alpha_0)) - v(f'(\alpha_0))$.

Uniqueness Let $\beta_1 \neq \beta_2 \in \mathcal{O}_v$ be roots of $f(X)$ such that $v(\beta_i - \alpha) > v(f'(\alpha))$ for $i = 1, 2$. As in the proof of existence, it follows that

$$v(f'(\beta_i)) = v(f'(\alpha)).$$

Write $\beta_2 = \beta_1 + t$.

$$\Rightarrow v(t) = v(\beta_1 - \beta_2) \geq \min\left(v(\beta_1 - \alpha), v(\beta_2 - \alpha)\right)$$

$$> v(f'(\alpha)) = v(f'(\beta_1)).$$

As before, $\underbrace{f(\beta_2)}_{0} \equiv \underbrace{f(\beta_1)}_{0} + t \cdot f'(\beta_1) \bmod t^2$.

$$\Rightarrow f'(\beta_1) \equiv 0 \bmod t.$$

$$\Rightarrow v(t) \leq v(f'(\beta_1)). \qquad \lightning \qquad \square$$

Hensel's lemma (V3)

Let $f(X) \in \mathcal{O}_v[X]$ and assume $f(X) \equiv \bar{g}(X)\bar{h}(X) \mod \mathfrak{p}_v$ for relatively prime polynomials $\bar{g}(X), \bar{h}(X) \in \kappa_v[X]$.

unique?

Then, there exist $g(X), h(X) \in \mathcal{O}_v[X]$ (<u>lift</u>) such that

$$g(X) \equiv \bar{g}(X) \mod \mathfrak{p}, \quad \deg(g) = \deg(\bar{g})$$
$$h(X) \equiv \bar{h}(X) \mod \mathfrak{p},$$

with $f(X) = g(X) \cdot h(X)$.

<u>Warning</u> It's possible that $\deg(f) > \deg(f \mod \mathfrak{p}_v)$.

(Leading coeff. of f is $\equiv 0 \mod \mathfrak{p}_v$.)

$\Rightarrow$ We can't simultaneously ensure $\deg(g) = \deg(\bar{g})$ <u>and</u> $\deg(h) = \deg(\bar{h})$.

<u>Pf</u> See Neukirch, Algebraic Number Theory, Thm II.4.6. $\square$

Pf that $V3 \Rightarrow V1$

If $\alpha \in \kappa_v$ is a simple root mod $\mathfrak{p}$, we can take $\bar{g}(X) = X - \alpha$, $\bar{h}(X) = \dfrac{f(X) \mod \mathfrak{p}_v}{X - \alpha}$.

simple $\Rightarrow$ rel. prime

$\rightsquigarrow$ lin. pol. $g(X) = X - \beta$ dividing $f(X)$.

$\rightsquigarrow$ root $\beta \in \mathcal{O}_v$. $\square$

1.6. Algebraic extensions

Stupid lemma

Let K be complete w.r.t. disc. val. v and let $f(X) = a_n X^n + \dots + a_0 \in K[X]$ be irreducible.

Then, $v(a_i) \geq \min(v(a_n), v(a_0)) \ \forall i$.

Pf Multiply by some power of π so that w.l.o.g. $v(a_i) \geq 0 \ \forall i$ and $v(a_i) = 0$ for some i.

Let $v(a_i) = 0$ and $v(a_{i-1}), \dots, v(a_0) > 0$.

$$\Rightarrow f(X) \equiv a_n X^n + \dots + a_i X^i$$

$$\equiv \underbrace{X^i}_{\bar{g}(X)} \underbrace{(a_n X^{n-i} + \dots + a_i)}_{\bar{h}(X)} \quad \text{mod } \mathfrak{p}$$

$\bar{h}(X) \leftarrow$ not divisible by X because $a_i \not\equiv 0 \text{ mod } \mathfrak{p}_v$.

$\Rightarrow \bar{g}(X), \bar{h}(X)$ rel. prime

$\overset{V3}{\Rightarrow} f(X) = g(X)h(X)$ for some pol. $g(X), h(X) \in \mathcal{O}_v[X]$ with $\deg(g) = \deg(\bar{g}) = i$.

$\Rightarrow f(X)$ is not irred. unless

$$\left.\begin{array}{ll} i = 0 & (\text{so } v(a_0) = 0) \\ i = n & (\text{so } v(a_n) = 0) \end{array}\right\} \Rightarrow \min(v(a_n), v(a_0)) = 0.$$

□

Thm Let K be complete w.r.t. the disc. val. v and let L be a field extension of degree n. Then, there is exactly one disc. val. v' on L that extends v (so that $v'|_K = v$):

$$v'(x) = \frac{1}{n} v(\mathrm{Nm}_{L|K}(x)) \quad \text{for } x \in L.$$

$$|x|' = \sqrt[n]{|\mathrm{Nm}_{L|K}(x)|}$$

Then, $\mathcal{O}_{v'} \subseteq L$ is the integral closure of $\mathcal{O}_v$ in L.

Also, L is complete w.r.t. v'.

Analogy The only extension of $|\cdot|$ from $K = \mathbb{R}$ to $L = \mathbb{C}$ is $|x| = \sqrt{|x\bar{x}|}$.

Pf of thm

v' is a disc. val. satisfying the stated conditions

For $x \in K$: $v'(x) = \frac{1}{n} v(\underbrace{\mathrm{Nm}_{L|K}(x)}_{x^n}) = v(x). \Rightarrow v'|_K = v.$

a) For $x \in L$: $v'(x) = \infty \Leftrightarrow \mathrm{Nm}_{L|K}(x) = 0 \Leftrightarrow x = 0.$

b) For $x, y \in L$: $v'(xy) = \frac{1}{n} v(\underbrace{\mathrm{Nm}(xy)}_{\mathrm{Nm}(x)\mathrm{Nm}(y)}) = v'(x) + v'(y).$

__Claim__: $x \in L$ integral over $\mathcal{O}_v \iff v'(x) \geq 0$

__Pf__ Let $f(X) = X^t + a_{t-1} X^{t-1} + \dots + a_0 \in K[X]$ be the min. pol. of x.

$$\Rightarrow \mathrm{Nm}_{K(x)|K}(x) = \pm a_0$$

$$\Rightarrow \mathrm{Nm}_{L|K}(x) = \mathrm{Nm}_{K(x)|K}(\underbrace{\mathrm{Nm}_{L|K(x)}(x)}_{x^{[L:K(x)]}}) = (\pm a_0)^{[L:K(x)]}.$$

"$\Rightarrow$" x integral $\Rightarrow f(X) \in \mathcal{O}_v[X] \Rightarrow a_0 \in \mathcal{O}_v$

$$\Rightarrow \underbrace{\mathrm{Nm}_{L|K}(x)}_{v(\dots)\geq 0} \in \mathcal{O}_v \Rightarrow v'(x) \geq 0.$$

"$\Leftarrow$" $v'(x) \geq 0 \Rightarrow v(a_0) \geq 0$

$$\underset{\underset{\text{Stupid lemma}}{\uparrow}}{\Rightarrow} v(a_i) \geq 0 \ \forall i \Rightarrow f(X) \in \mathcal{O}_v[X]$$

$\Rightarrow x$ integral. □

c) __Claim__ For $x, y \in L$: $v'(x+y) \geq \min(v'(x), v'(y))$.

__Pf__ W.l.o.g. $v'(x) \geq v'(y)$. $\Rightarrow v'\left(\frac{x}{y}\right) \geq 0$.

$\Rightarrow \frac{x}{y}$ integral $\Rightarrow \frac{x}{y} + 1$ integral

$\Rightarrow v'\left(\frac{x}{y} + 1\right) \geq 0$

$\Rightarrow v'(x+y) \geq v'(y) = \min(v'(x), v'(y))$. □

L is complete w.r.t. v' because it is a fin.-dim. normed vector space over a complete field.

(Choose a basis of L. Take any Cauchy sequence $a_1, a_2, \ldots \in L$. In any fixed coordinate, the sequence is a Cauchy seq. and hence converges in K. $\Rightarrow$ The seq. converges in L.)

Uniqueness of v'

Assume that v'' is another disc. val. extending v.

$\mathcal{O}_{v''}$ is a PID contain $\mathcal{O}_v$.

$\Downarrow$

integrally closed

$\Rightarrow \mathcal{O}_{v'} \subseteq \mathcal{O}_{v''}$ [Idea: Enlarging $\mathcal{O}_{v'}$ would kill primes but the local ring $\mathcal{O}_{v'}$ already has just one prime!]

$\mathfrak{p}_{v''} \cap \mathcal{O}_{v'}$ is a nonzero prime ideal of $\mathcal{O}_{v'}$.

$\Rightarrow \mathfrak{p}_{v''} \cap \mathcal{O}_{v'} = \mathfrak{p}_{v'}$

$\Rightarrow \mathfrak{p}_{v'} \subseteq \mathfrak{p}_{v''}$

If $v''(x) \geq 0$, then $v''(\frac{1}{x}) \leq 0$. $\Rightarrow \frac{1}{x} \notin \mathfrak{p}_{v''} \Rightarrow \frac{1}{x} \notin \mathfrak{p}_{v'}$

$\Rightarrow v'(\frac{1}{x}) \leq 0 \Rightarrow v'(x) \geq 0$.

$\Rightarrow \mathcal{O}_{v''} \subseteq \mathcal{O}_{v'} \Rightarrow \mathcal{O}_{v'} = \mathcal{O}_{v''}$

$\Rightarrow \mathfrak{p}_{v'} = \mathfrak{p}_{v''} \Rightarrow v' = \lambda \cdot v''$ for some $\lambda > 0$.

$\Rightarrow v' = v''$. $\leftarrow \boxed{v'|_K = v''|_K}$ □

Alternative proof of uniqueness (Thanks, Wyatt and Xeru!)

Apply the norm equivalence theorem to the finite-dimensional K-vector space L. If the norms $|x|' = \lambda^{-v'(x)}$ and $|x|'' = \lambda^{-v''(x)}$ arising from discrete valuations v', v'' differ by a bounded factor, we must have $v' = v''$. $\square$

Last time

Thm Let K be complete w.r.t. a disc. val. v and let L be a field ext. of degree n. Then, there is exactly one disc. val. v' on L that extends v: $v'(x) = \frac{1}{n} v(\mathrm{Nm}_{L/K}(x))$ for $x \in L$.

$\mathcal{O}_{v'} \subset L$ is the int. closure of $\mathcal{O}_v \subset K$.

L is complete w.r.t. v'.

Cor There is exactly one valuation v' on $\overline{K}$ extending v.

It is not discrete! The field $\overline{K}$ might not be complete w.r.t. v'! Still, $\mathcal{O}_{v'}$ is the int. closure and $\mathfrak{p}_{v'}$ is the only nonzero prime ideal in $\mathcal{O}_{v'}$.

Notation If K is complete w.r.t. a disc. val. v, we denote the corr. normalized valuation by v_K.

We $\mathcal{O}_K = \mathcal{O}_{v_K}$, $\mathfrak{p}_K = \mathfrak{p}_{v_K}$, $\pi_K = \pi_{v_K}$, ...

We also denote the ext. of v_K to $\overline{K}$ by v_K.

Cor If $f(x) \in K[X]$ is an irreducible pol. over a field K as above, then all roots of $f(x)$ in $\overline{K}$ have the same valuation, namely $\frac{1}{n} v(\text{const. coeff. of } f(x)) = \frac{1}{n} v(f(0))$.

Analogy If $f(x) \in \mathbb{R}[X]$ is an irreducible pol. ($\Rightarrow$ deg $= 1$ or 2), then all roots in $\mathbb{C}$ have the same abs. val. (complex conjugates if deg $= 2$).

Def Let $L|K$ as above and $\mathfrak{p}_K \mathcal{O}_L = \mathfrak{p}_L^e$.

The number $e(L|K) = e$ is the ramification indese of $L|K$.

The number $f(L|K) = f = [\kappa_L : \kappa_K]$ is the inertia degree of $L|K$.

Rmk $$e = \Big[\underset{\frac{1}{e}\mathbb{Z}}{\underset{\|}{v_K(L^\times)}} : \underset{\mathbb{Z}}{\underset{\|}{v_K(K^\times)}} \Big] = \Big[\underset{\mathbb{Z}}{\underset{\|}{v_L(L^\times)}} : \underset{e\mathbb{Z}}{\underset{\|}{v_L(K^\times)}} \Big].$$

Rmk $v_L(x) = e \cdot v_K(x) \ \forall x \in L$.

Rmk $v_K(\pi_L) = \frac{1}{e}$.

Rmk If $M|L|K$ are as above, then
$$e(M|K) = e(M|L)\, e(L|K)$$
$$f(M|K) = f(M|L)\, f(L|K).$$

Thm Let $L|K$ be an ext. of degree n as above.

$\Rightarrow n = e \cdot f$

Pf Follows from following thm! □

Thm Let $\omega_1, \dots, \omega_f \in \mathcal{O}_L$ be so that $\omega_1 \bmod \mathfrak{p}_L, \dots, \omega_f \bmod \mathfrak{p}_L$ form a basis of $\kappa_L | \kappa_K$. Then, $(\omega_i \pi_L^j)_{\substack{1 \le i \le f \\ 0 \le j < e}}$ is a basis of $\mathcal{O}_L | \mathcal{O}_K$ (and therefore of $L|K$).

Pf Write $x = \sum a_{ij} \omega_i \pi_L^j$ for $a_{ij} \in K$.

$$\Rightarrow x \equiv \sum_i a_{i0} \omega_i \quad \mod \pi_L .$$

$$(x \mod \mathfrak{p}_L) = \sum_i (a_{i0} \mod \mathfrak{p}_K) \cdot (\omega_i \mod \mathfrak{p}_L)$$

in κ_L.

since $\omega_1 \mod \mathfrak{p}_L, \dots, \omega_f \mod \mathfrak{p}_L$ form a basis of $\kappa_L | \kappa_K$, this uniquely determines $a_{i0} \mod \mathfrak{p}_K \; \forall i$.

$$x \equiv \sum a_{i0} \omega_i + \sum a_{i1} \omega_i \pi_L \quad \mod \mathfrak{p}_L^2$$

$$\frac{x - \sum (a_{i0} \mod \mathfrak{p}_K) \omega_i}{\pi_L} \equiv \sum a_{i1} \omega_i \pi_L \mod \mathfrak{p}_L$$

This uniquely determines $a_{i1} \mod \mathfrak{p}_K \; \forall i$.

$\vdots$

$a_{i,e-1} \mod \mathfrak{p}_K \; \forall i$.

$a_{i0} \mod \mathfrak{p}_K^2 \; \forall i$

$\vdots$

□

Def $L|K$ is <u>unramified</u> if $e = 1$ $(\Leftrightarrow f = n)$.

$L|K$ is <u>totally ramified</u> if $e = n$ $(\Leftrightarrow f = 1)$.

<u>Comparing the splitting behavior of a prime before and after completion</u>

Thm Let $\mathcal{O}_K$ be a Dedekind dom. and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Let $L|K$ be a separable field ext. of degree n and $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ with inertia degrees $f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$.

$$\Rightarrow L \otimes \underset{\substack{\uparrow \\ \text{completion} \\ \text{w.r.t. } v_\mathfrak{p}}}{\widehat{K}_\mathfrak{p}} \cong \underset{\substack{\uparrow \\ \text{completion} \\ \text{of } L \text{ w.r.t } v_{\mathfrak{P}_i}}}{\widehat{L}_{\mathfrak{P}_1}} \times \ldots \times \widehat{L}_{\mathfrak{P}_r}$$

$$\mathcal{O}_L \otimes \widehat{\mathcal{O}}_\mathfrak{p} \cong \widehat{\mathcal{O}}_{\mathfrak{P}_1} \times \ldots \times \widehat{\mathcal{O}}_{\mathfrak{P}_r}$$

$$e_i = e(\widehat{L}_{\mathfrak{P}_i} | \widehat{K}_\mathfrak{p}),$$

$$\mathcal{O}_L/\mathfrak{P}_i \cong \widehat{\mathcal{O}}_{\mathfrak{P}_i}/\mathfrak{P}_i\widehat{\mathcal{O}}_{\mathfrak{P}_i},$$

$$f_i = f(\widehat{L}_{\mathfrak{P}_i} | \widehat{K}_\mathfrak{p}).$$

Sketch of pf

$$\hat{\mathcal{O}}_{\mathfrak{q}} = \varprojlim \mathcal{O}_K/\mathfrak{q}^n .$$

$$\Rightarrow \mathcal{O}_L \otimes \hat{\mathcal{O}}_{\mathfrak{q}} = \varprojlim \mathcal{O}_L/\mathfrak{q}^n \mathcal{O}_L$$

$\mathcal{O}_L|\mathcal{O}_K$ fin. gen.
because $L|K$ is
separable

$$= \varprojlim \mathcal{O}_L/(\mathfrak{q}\mathcal{O}_L)^n$$

$$= \varprojlim \mathcal{O}_L/(\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r})^n$$

$$\underset{CRT}{=} \prod_i \varprojlim \mathcal{O}_L/\mathfrak{P}_i^{e_i n}$$

$$= \prod_i \varprojlim \mathcal{O}_L/\mathfrak{P}_i^n$$

$$= \prod_i \hat{\mathcal{O}}_{\mathfrak{P}_i} .$$

□

In terms of polynomials:

If $\mathfrak{p} \nmid [\mathcal{O}_L : \mathcal{O}_K[\alpha]]$ for some $\alpha \in \mathcal{O}_L$, then its min. pol. $f(X) \in \mathcal{O}_K[X]$ factors in $\widehat{\mathcal{O}}_{\mathfrak{p}}[X]$ as

$$f(X) = f_1(X) \cdots f_r(X)$$

with $f_i(X) \in \widehat{\mathcal{O}}_{\mathfrak{p}}[X]$ irred. of degree

$$[\widehat{L}_{\mathfrak{P}_i} : \widehat{K}_{\mathfrak{p}}] = e_i f_i \quad \left(\widehat{L}_{\mathfrak{P}_i} = \widehat{K}_{\mathfrak{p}}[X]/f_i(X)\right)$$

and each $f_i(X)$ factors mod $\mathfrak{p}$ as

$$f_i(X) = g_i(X)^{e_i} \text{ with } g_i(X) \in \kappa_{\mathfrak{p}}[X]$$

irreducible of degree f_i $\left(\kappa_{\mathfrak{P}_i} = \kappa_{\mathfrak{p}}[X]/g_i(X)\right)$.

1.7. Newton polygons

Let K be a field with val. v.

Thm Let $r_1, \dots, r_n \in K^\times$ with $v(r_1) \leq \dots \leq v(r_n)$.

Then, the coeff. of $(X-r_1)\cdots(X-r_n) = X^n + a_{n-1}X^{n-1} + \dots + a_0$ satisfy $v(a_{n-i}) \geq v(r_1) + \dots + v(r_i)$ for $i = 1, \dots, n$.

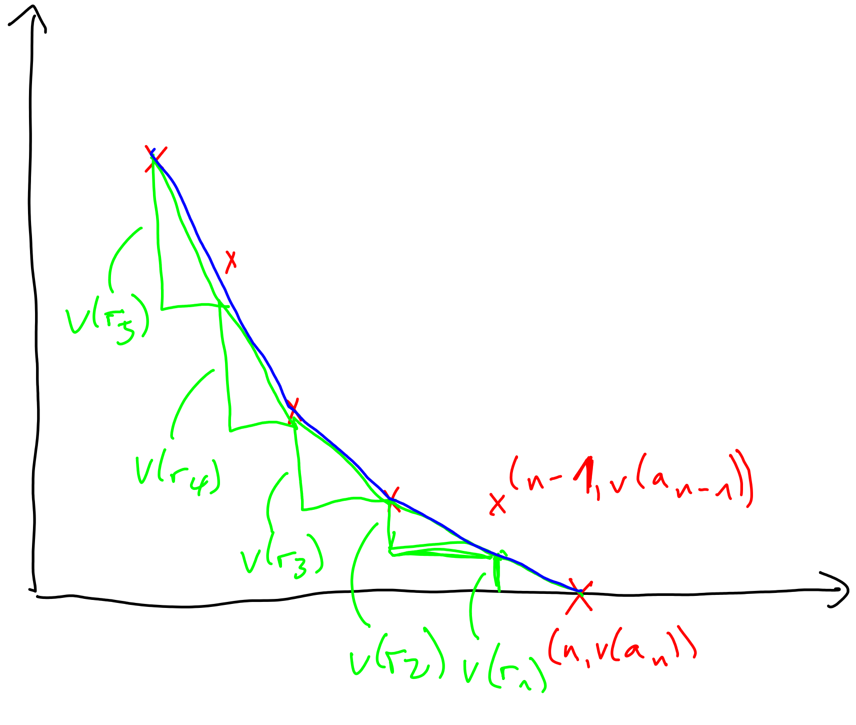
Equality holds (at least) if $v(r_i) < v(r_{i+1})$ or $i = n$.

Pf Expand the product $(X-r_1)\cdots(X-r_n)$.

$\rightsquigarrow$ $a_{n-i} = \pm$ the sum of all products of i of the numbers $r_1, \dots, r_n$.

Each prod. has val. $\geq v(r_1) + \dots + v(r_i)$.

This val. occurs in exactly one prod. if $v(r_i) < v(r_{i+1})$ of $i = n$. □



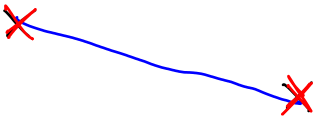
The points $(i, v(a_i))$ lie on or above this polygon.

There is a point at each corner of the polygon.

Def The Newton polygon of a pol. $f(X) = \sum_{i=0}^{n} a_i X^i$ (with $a_0, a_n \neq 0$) is the lower convex hull of the set of points $(i, v(a_i))$ $(i = 0, \dots, n)$.

Cor The val. of the roots of $f(X)$ in $\overline{K}$ are minus the slopes of the Newton polygon. (Width of line segment = number of roots with the corr. valuation).

Cor 1 If $f(X) \in K[X]$ is irreducible, its Newton polygon is just a single line segment.



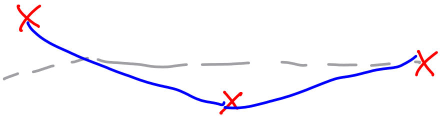
Pf All roots have the same valuation. □

Rmk More generally, $f(X)$ has at least one irreducible factor per line segment.

Cor of Cor 1 The stupid lemma:

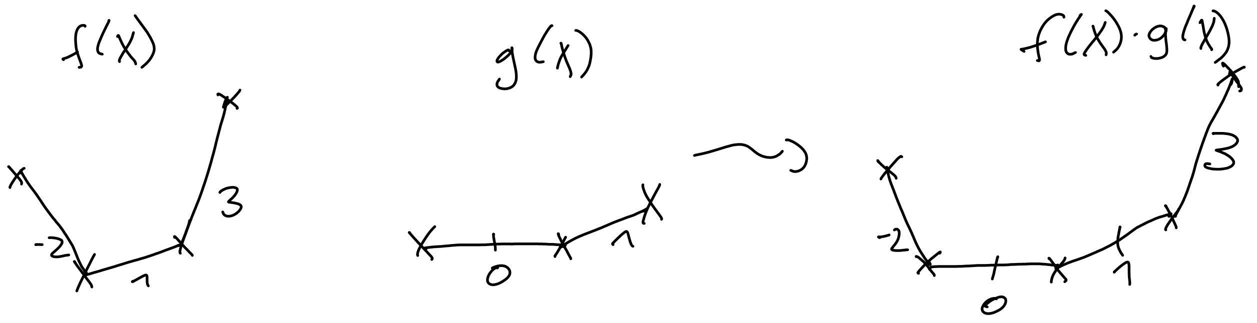
If $f(X)$ is irred., then $v(a_i) \geq \min(v(a_0), v(a_n))$ $\forall i$

Pf

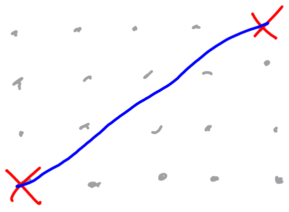


(not a single line segment) □

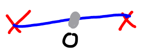
Cor 2 To find the Newton polygon of $f(X)\cdot g(X)$, glue the Newton pol. of $f(X)$, $g(X)$ together and sort the line segments. (Move up/down to make $v(a_0)$ correct.)



Cor of Cor 2 If $v = v_u$ is normalized and the Newton polygon is a line segment which contains no integer points except its endpoints, then $f(X)$ is irreducible.



Pf Can't have been glued together from two polygons whose corners lie at integer points. □

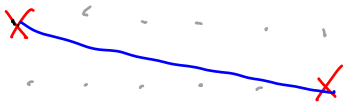
Warning Converse is false! (E.g. $X^2-2 \in \mathbb{Q}_3[X]$ is irred. (no roots mod 3)) 

Cor of Cor of Cor 2 (Eisenstein criterion)

If $\underbrace{\text{it is the line segment } [(0,1),(n,0)]}$, then $f(X)$ is irred.

$$\Uparrow$$

$$\boxed{v(a_0)=1,\ v(a_1),\dots,v(a_{n-1})\geq 1,\ v(a_n)=0}$$



Rmk Let $f(X) \in K[X]$ be irreducible with slope $-\frac{a}{b}$ $(\gcd(a,b)=1)$.

Let $\alpha \in \overline{K}$ be a root of $f(X)$. $(\Rightarrow v(\alpha) = \frac{a}{b})$ and

$L = K(\alpha) \cong K[X]/f(X)$. Then $b \mid e(L|K)$ because

$$\frac{a}{b} \in v_K(L^\times) = \frac{1}{e} \cdot \mathbb{Z}.$$

Warning We might have $b \neq e$.

For example, look at $X^2-3 \in \mathbb{Q}_2[X]$. $\rightsquigarrow$ slope $0 = \frac{0}{1}$

But $v_2(1-\sqrt{3}) = \frac{1}{2} v_2(N_{\mathbb{Q}_2(\sqrt{3})|\mathbb{Q}_2}(1-\sqrt{3}))$

$$= \frac{1}{2} v_2(1-3) = \frac{1}{2}, \text{ so } e=2.$$

Another proof that $f(\alpha)=0 \Rightarrow v(\alpha) = -$slope of a line seg.

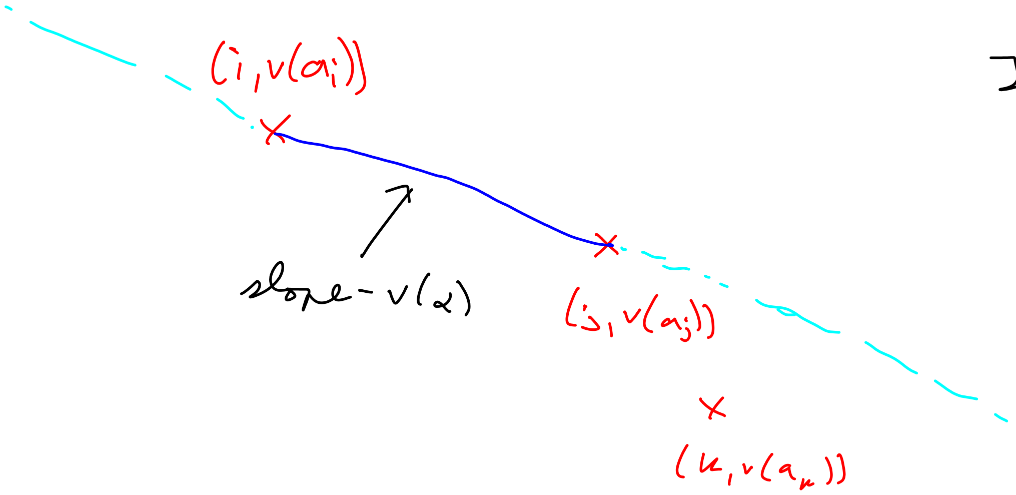
Write $f(X) = \sum_i a_i X^i$.

Then monomials have valuation $v(a_i\alpha^i) = v(a_i) + i \cdot v(\alpha)$.

If the min. val. t occured in just one monomial $a_i\alpha^i$, then $v(f(\alpha)) = t$, so $f(\alpha) \neq 0$. ↯

$\Rightarrow$ The min. val. occurs in at least two monomials $a_i\alpha^i$, $a_j\alpha^j$.

$$\Rightarrow v(a_j) - v(a_i) = -(j-i) \cdot v(\alpha).$$



If there were a third point $(k, v(a_k))$ below the line, then $v(a_k\alpha^k) < v(a_i\alpha^i)$. ↯ □

1.8. Classification of local fields

Thm The nonarchimedean local fields are:

- the fin. ext. K of $\mathbb{Q}_p$

- the fields $K = \mathbb{F}_q((T))$.

Pf Let $\kappa_K = \mathbb{F}_q$, $q = p^f$.

Case 1: $\mathrm{char}(K) = 0$

$\Rightarrow \mathbb{Q} \subseteq K$

$p = 0$ in $\mathbb{F}_q \Rightarrow v_K(p) \geq 1$.

$\Rightarrow v_K|_{\mathbb{Q}}$ is a multiple of the p-adic valuation on $\mathbb{Q}$

$\Rightarrow K$ is an ext. of $\mathbb{Q}_p$ with $f(K|\mathbb{Q}_p) = [\mathbb{F}_q : \mathbb{F}_p] = f < \infty$

$e(K|\mathbb{Q}_p) = v_K(p) < \infty$

of degree $n = e \cdot f < \infty$.

Case 2: $\mathrm{char}(K) \neq 0$

$\mathrm{char}(K) = 0$ in $K \Rightarrow \mathrm{char}(K) = 0$ in $\kappa_K = \mathbb{F}_q$

$\Rightarrow \mathrm{char}(K) = p$.

$\Rightarrow \mathbb{F}_p \subseteq K$.

$\mathbb{F}_q$ is the splitting field of the separable polynomial $X^q - X = \prod_{t \in \mathbb{F}_q} (X - t)$ over $\mathbb{F}_p$.

By Hensel's lemma, it splits completely in K,

$\Rightarrow \mathbb{F}_q \subseteq K$.

$\Rightarrow$ We can write any el. x of K in base π_K with digits in $\mathbb{F}_q$:

$$x = \sum_{i=-r}^{\infty} a_i \pi_K^i \quad (a_i \in \mathbb{F}_q). \Rightarrow K \cong \mathbb{F}_q((T)), \quad \pi_K \leftrightarrow T$$

□

2. Infinite Galois theory

Reference: Chapter 4.2 in Bosch: Algebra from the viewpoint of Galois theory

Def A Galois ext. $L|K$ is an algebraic field ext. which is normal and separable.

If an irred. pol. $f(x) \in K[X]$ has a root in L,

- normal: then it split completely in L
- separable: then all its roots in $\overline{K}$ are distinct (equivalently, $f'(x) \neq 0$).

Ex The separable closure K^{sep} of K is the maximal Galois extension of K.

2.1. Computing infinite Galois groups

Question What is $Gal(\overline{\mathbb{F}}_q | \mathbb{F}_q)$?

Thm Let $M|K$ be a Gal. ext. and let $\mathcal{L}$ be any set of finite Galois ext. $L \subseteq M$ of K such that $M = \bigcup_{L \in \mathcal{L}} L$.

Then,
$$Gal(M|K) \cong \varprojlim_{L \in \mathcal{L}} Gal(L|K), \qquad \sigma \longmapsto (\sigma|_L)_L .$$
the set of tuples $(\sigma_L)_L \in \prod_{L \in \mathcal{L}} Gal(L|K)$ such that

$$\sigma_{L_2}\big|_{L_1} = \sigma_{L_1} \quad \text{for all } L_1 \subseteq L_2 \quad (\text{in } \mathcal{L}).$$

__Pf__ The preimage of $(\sigma_L)_L \in \varprojlim \mathrm{Gal}(L|K)$ is

$$\sigma : M \to M$$
$$x \mapsto \sigma_L(x) \text{ for any } x \in L \in \mathcal{L}.$$

__Well-def:__ Assume $x \in L_1, L_2 \in \mathcal{L}$.

Look at the compositum $L_1 \cdot L_2$.

We have $L_1 \cdot L_2 = K(y)$ for some $y \in M$.

Let $y \in L_3 \in \mathcal{L}$. $\Rightarrow L_1, L_2 \subseteq L_1 \cdot L_2 \subseteq L_3$.

$$\Rightarrow \sigma_{L_1}(x) \underset{\substack{\uparrow \\ L_1 \subseteq L_3}}{=} \sigma_{L_3}(x) \underset{\substack{\uparrow \\ L_2 \subseteq L_3}}{=} \sigma_{L_2}(x)$$

__Field hom.:__ Let $x, y \in M$. Let $K(x,y) \subseteq L \in \mathcal{L}$.

$$\Rightarrow \sigma(x \pm y) = \sigma_L(x \pm y) = \sigma_L(x) \pm \sigma_L(y) = \sigma(x) \pm \sigma(y)$$

__Fixes K:__ Let $x \in K$. Take any $L \in \mathcal{L}$.

$$\Rightarrow \sigma(x) = \sigma_L(x) = x.$$ □

Ex The fin. ext. of $\mathbb{F}_q$ are $\mathbb{F}_{q^n}$ with $n \geq 1$.

$$\Rightarrow Gal(\overline{\mathbb{F}_q} \,|\, \mathbb{F}_q) \cong \varprojlim_{n \geq 1} Gal(\mathbb{F}_{q^n} \,|\, \mathbb{F}_q)$$

We have $Gal(\mathbb{F}_{q^n} \,|\, \mathbb{F}_q) \cong \mathbb{Z}/n\mathbb{Z}$

$$\varphi_q \longmapsto 1 \bmod n$$

where φ_q is the Frobenius automorphism $x \mapsto x^q$.

Note that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ if and only if $n | m$ (so $\mathbb{F}_{q^m} = \mathbb{F}_{(q^n)^{m/n}}$) and that in this case

$$\begin{tikzcd}
Gal(\mathbb{F}_{q^m} \,|\, \mathbb{F}_q) \arrow[rrr, phantom, "\cong"] \arrow[ddd, "\text{restriction}"'] & & & \mathbb{Z}/m\mathbb{Z} \arrow[ddd, "\text{reduction mod } n"] \\
& \varphi_q \arrow[r] \arrow[d, mapsto] & 1 \bmod m \arrow[d, mapsto] & \\
& \varphi_q \arrow[r] & 1 \bmod n & \\
Gal(\mathbb{F}_{q^n} \,|\, \mathbb{F}_q) \arrow[rrr, phantom, "\cong"] & & & \mathbb{Z}/n\mathbb{Z}
\end{tikzcd}$$

$$Gal(\overline{\mathbb{F}_q} \,|\, \mathbb{F}_q) = \varprojlim_{n \geq 1} \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$$

$$\uparrow$$

$$\boxed{\begin{array}{c} \text{set of } (a_n)_n \in \prod_n \mathbb{Z}/n\mathbb{Z} \\ \text{s.t. } a_n = a_m \bmod n \ \forall n | m \end{array}}$$

Ex $\mathbb{Q}(\zeta_\infty) = \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n)$ is a field (in fact a Gal. ext.)

because $\mathbb{Q}(\zeta_n)\cdot\mathbb{Q}(\zeta_m) \subseteq \mathbb{Q}(\zeta_{nm})$.

$$\Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) \cong \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q})$$

$$\begin{aligned}\mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) &\cong (\mathbb{Z}/n\mathbb{Z})^\times \\ \phi_k &\longrightarrow k \bmod n\end{aligned}$$

where ϕ_k is the automorphism $\zeta_n \longmapsto \zeta_n^k$.

Note that $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_m)$ if and only if $n \mid \mathrm{lcm}(m,2)$.

In particular, $\mathbb{Q}(\zeta_{2n}) \subseteq \mathbb{Q}(\zeta_{2m})$ if and only if $n \mid m$. (note that $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2n})$ for n odd).

In this case,

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}(\zeta_{2m})|\mathbb{Q}) \arrow[ddd, bend right, "\text{restriction}"'] & \cong & (\mathbb{Z}/2m\mathbb{Z})^\times \arrow[ddd, bend left, "\text{reduction mod } 2n"] \\
\phi_k \arrow[rr] \arrow[d, mapsto] & & k \bmod 2m \arrow[d, mapsto] \\
\phi_k \arrow[rr] & & k \bmod 2n \\
\mathrm{Gal}(\mathbb{Q}(\zeta_{2n})|\mathbb{Q}) & \cong & (\mathbb{Z}/2n\mathbb{Z})^\times
\end{tikzcd}$$

$$\begin{aligned}\Rightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) &= \varprojlim \mathrm{Gal}(\mathbb{Q}(\zeta_{2n})|\mathbb{Q}) \\ &= \varprojlim (\mathbb{Z}/2n\mathbb{Z})^\times \\ &= \varprojlim (\mathbb{Z}/n\mathbb{Z})^\times \\ &= \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times .\end{aligned}$$

2.2. Fundamental theorem

Fund. thm. finite of Galois theory

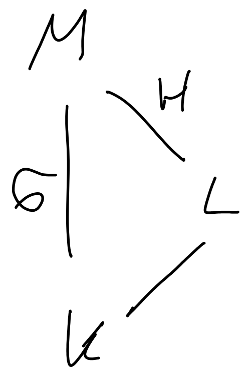
Let $M|K$ be a finite Gal. ext. with $G = \mathrm{Gal}(M|K)$.

Then, there is a bijection

$$\{\text{field } K \subseteq L \subseteq M\} \longleftrightarrow \{\text{subgroup } H \subseteq G\}$$

$$L \longmapsto \mathrm{Gal}(M|L) = \{\sigma \in G \mid \sigma(x) = x \ \forall x \in L\}$$

$$M^H = \{x \in M \mid \sigma(x) = x \ \forall \sigma \in H\} \longleftarrow\!\shortmid \quad H$$



$M|L$ is always Galois.

$L|K$ is Galois if and only if H is a normal subgroup of G. Then, H is the kernel of $G \longrightarrow \mathrm{Gal}(L|K)$,
$\sigma \mapsto \sigma|_L$

so $\mathrm{Gal}(L|K) \cong G/H$.

What goes wrong for infinite Galois extensions?

We might have $\mathrm{Gal}(M|M^H) \supsetneq H$.

Not every $H \leq G$ is of the form $\mathrm{Gal}(M|L)$ for some L.

Ese
$$\begin{array}{ccc} G = \mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q) & \cong & \hat{\mathbb{Z}} \\ \cup\!| & & \cup\!| \\ H = \langle \varphi_q \rangle & \cong & \mathbb{Z} \\ \varphi_q & \longrightarrow & 1 \end{array}$$

$$\begin{aligned} \overline{\mathbb{F}_q}^H &= \{x \in \overline{\mathbb{F}_q} \mid \varphi_q(x) = x\} \\ &= \{x \in \overline{\mathbb{F}_q} \mid x^q = x\} \\ &= \mathbb{F}_q \end{aligned}$$

$$\Rightarrow \mathrm{Gal}(\overline{\mathbb{F}_q}|\overline{\mathbb{F}_q}^H) = \mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q) = G \supsetneq H.$$

2.2. Fundamental theorem

Fund. thm. of infinite Galois theory

Let $M|K$ be a ~~finite~~ Gal. ext. with $G = \mathrm{Gal}(M|K)$.

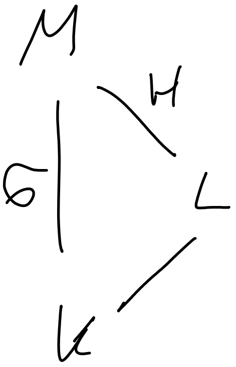
Then, there is a bijection

$$\{\text{field } K \subseteq L \subseteq M\} \longleftrightarrow \{\text{closed subgroup } H \subseteq G\}$$

$$L \longmapsto \mathrm{Gal}(M|L) = \{\sigma \in G \mid \sigma(x) = x \ \forall x \in L\}$$

(Krull top. is subspace top. from Krull top. on $G = \mathrm{Gal}(M|K)$)

$$M^H = \{x \in M \mid \sigma(x) = x \ \forall \sigma \in H\} \longleftarrow\!\shortmid \ H$$



$M|L$ is always Galois.

$L|K$ is Galois if and only if H is a normal subgroup of G. Then, H is the kernel of $G \longrightarrow \mathrm{Gal}(L|K)$, $\sigma \mapsto \sigma|_L$,

so $\mathrm{Gal}(L|K) \cong G/H$.

(Krull top. = quotient top.)

For any subgroup $H \subseteq G$, $\mathrm{Gal}(M|M^H) = \overline{H}$, the closure of H in G.

What goes wrong for infinite Galoisextensions?

We might have $Gal(M|M^H) \supsetneq H$.

Not every $H \leq G$ is of the form $Gal(M|L)$ for some L.

<u>Ex</u>

$$\begin{array}{ccc} G = Gal(\overline{\mathbb{F}}_q|\mathbb{F}_q) & \cong & \hat{\mathbb{Z}} \\ \cup\!| & & \cup\!| \\ H = \langle \varphi_q \rangle & \cong & \mathbb{Z} \\ \varphi_q & \longrightarrow & 1 \end{array}$$

$$\begin{aligned} \overline{\mathbb{F}}_q^{\,H} &= \{ x \in \overline{\mathbb{F}}_q \mid \varphi_q(x) = x \} \\ &= \{ x \in \overline{\mathbb{F}}_q \mid x^q = x \} \\ &= \mathbb{F}_q \end{aligned}$$

$$\Rightarrow Gal(\overline{\mathbb{F}}_q|\overline{\mathbb{F}}_q^{\,H}) = Gal(\overline{\mathbb{F}}_q|\mathbb{F}_q) = \underset{\overline{\mathbb{Z}}}{\overset{}{\underset{\|}{G}}} \supsetneq H. \quad \xleftarrow{} \boxed{\mathbb{Z} \text{ dense in } \hat{\mathbb{Z}}}$$

Note For $K \subseteq L \subseteq M$, we have

$$\mathrm{Gal}(M|L) = \{\sigma \in \mathrm{Gal}(M|K) \mid \sigma(x) = x \ \forall x \in L\}$$

$$= \bigcap_{x \in L} \mathrm{Gal}(M|K(x))$$

$$= \bigcap_{\substack{L' \subseteq L \\ \text{finite ext. of } K}} \mathrm{Gal}(M|L')$$

$$= \bigcap_{\substack{L' \subseteq L \\ \text{any ext. of } K}} \mathrm{Gal}(M|L').$$

Idea In topology, intersections of closed sets are closed.

⇝ Look for topology on $\mathrm{Gal}(M|K)$ s.t.

$H \subseteq G$ closed $\Leftrightarrow$ $H = \mathrm{Gal}(M|L)$ for some L.

Def The Krull topology on $G = \mathrm{Gal}(M|K)$ has the following base of open sets:

$$U_{\sigma, L} = \sigma \, \mathrm{Gal}(M|L) = \{\tau \in G \mid \tau|_L = \sigma\}$$

for $L \subseteq M$ finite Galois ext. of K, $\sigma \in \mathrm{Gal}(L|K)$.

Roughly: $\sigma, \tau \in G$ "close" if they agree on a "large" finite Galois ext. $L \subseteq M$ of K.

Ex If $M | K$ is a finite ext., we get the discrete top:

$U_{\sigma, M} = \{\sigma\}$, so any set is open.

Rmk The Krull top. on $\mathrm{Gal}(M|K) = \varprojlim_{L \in \mathcal{L}} \mathrm{Gal}(L|K)$

$$\subseteq \prod_{L \in \mathcal{L}} \mathrm{Gal}(L|K)$$

(where $\mathcal{L}$ consists of fin. Gal. ext. $L \subseteq M$ of K) agrees with the subspace top. of the prod. top. of the disc. top.

Rmk G is a topological group: $G \times G \to G$ and $G \to G$ $(x,y) \mapsto xy$ $x \mapsto x^{-1}$ are continuous.

Ex The isom. $\mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q) \cong \hat{\mathbb{Z}}$, $\mathrm{Gal}(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) \cong \hat{\mathbb{Z}}^\times$ defined earlier are homomorphisms.

Ese $\quad Gal(\overline{\mathbb{F}_q} \mid \mathbb{F}_q) = \hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$

Finite index closed subgroups: (= open) $\qquad H = n \cdot \hat{\mathbb{Z}}, \quad n \geq 1$

$$\rightsquigarrow$$

Fin. (Gal.) ext. of $\mathbb{F}_q$: $\qquad L = \mathbb{F}_{q^n}$

Closed subgroups: $H = \prod_p p^{e_p} \mathbb{Z}_p$ with $e_p = \{0, 1, \dots, \infty\}$ $\quad (p^\infty = 0)$

(Take any closed H, $e_p := \min\{ v_p(x_p) \mid x = (x_p)_p \in H \}$.

$$x \in H \Rightarrow x \cdot \mathbb{Z} \subseteq H \underset{\substack{\uparrow \\ H \text{ closed}}}{\Rightarrow} x \cdot \hat{\mathbb{Z}} \subseteq H \Rightarrow \underset{\substack{\| \\ p^{e_p}\mathbb{Z}_p}}{x_p \mathbb{Z}_p} \subseteq H$$

$$\Downarrow$$

$$\underset{\substack{\| \\ \dots = H}}{\prod_p p^{e_p} \mathbb{Z}_p} \subseteq H \Big\} \Big)$$

Gal. ext. of $\mathbb{F}_q$: $\displaystyle L = \bigcup_{\substack{n \geq 1: \\ H \subseteq Gal(\mathbb{F}_{q^n} | \mathbb{F}_q) \\ \| \\ n \cdot \hat{\mathbb{Z}}}} \mathbb{F}_{q^n} = \bigcup_{\substack{n \geq 1: \\ \forall p : v_p(n) \leq e_p}} \mathbb{F}_{q^n}$

$$\Big(\text{“} = \mathbb{F}_{q^N} \text{ with } N = \underbrace{\prod_p p^{e_p}}_{\text{not necessarily a number}} \text{”} \Big)$$

Pf of fund. thm. of infinite Galois theory

$M^{\mathrm{Gal}(M|L)} = L$ for any $K \subseteq L \subseteq M$

"$\supseteq$" clear

"$\subseteq$" Let $x \in M \setminus L$. Let L_x be a fin. Gal. ext. of L containing x. $\underset{\uparrow}{\Longrightarrow}$ $\exists\, \bar{\sigma} \in \mathrm{Gal}(L_x|L)$: $\bar{\sigma}(x) \neq x$.

fund. thm.
of fin. Gal. theory

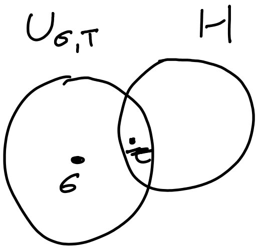
We know that $\mathrm{Gal}(C|A) \to \mathrm{Gal}(B|A)$ is surj. for any finite Gal. ext. $C|B$.

$\Rightarrow$ By Zorn's lemma, there is an ext. σ of $\bar{\sigma}$ to M. (The map $\mathrm{Gal}(M|L) \to \mathrm{Gal}(L_x|L)$ is surj.)

But $\sigma(x) \neq x$.

$\mathrm{Gal}(M|M^H) = \overline{H}$ for all $H \leq G$

"$\subseteq$" Let $\sigma \in \mathrm{Gal}(M|M^H)$. For any fin. Galois ext. $T \subseteq M$ of K, we have



$$\sigma|_T \in \mathrm{Gal}(T|T^H) = \text{"}H|_T\text{"} = \{\tau|_T : \tau \in H\}.$$

$\Rightarrow U_{\sigma,T} \cap H \neq \emptyset$ for all T

$\Rightarrow \sigma \in \overline{H}$.

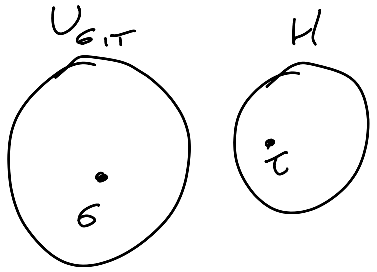
"$\supseteq$" Let $\sigma \notin \mathrm{Gal}(M|M^H)$. $\Rightarrow \exists\, x \in M^H : \sigma(x) \neq x$.

Let $T \subseteq M$ be a fin. Gal. ext. of K containing x.

$x \in M^H \Rightarrow \forall \tau \in H: \tau(x) = x$

Since $\sigma(x) \neq x$, we conclude that $\sigma|_T \neq \tau|_T \;\forall \tau \in H$.

$\Rightarrow U_{\sigma,T} \cap H = \emptyset$. $\Rightarrow \sigma \notin \overline{H}$.



<u>$\mathrm{Gal}(M|L) \subseteq \mathrm{Gal}(M|K)$ carries the subspace top.</u>

Let $\sigma \in \mathrm{Gal}(M|K)$, $T \subseteq M$ fin. Gal. ext.

$$U_{\sigma,T} \cap \mathrm{Gal}(M|L) = \{\tau \in G \mid \tau|_T = \sigma|_T,\ \tau|_L = \mathrm{id}_L\}$$

$$= \begin{cases} U_{\sigma', L\cdot T}, & \exists\, \sigma' \in \mathrm{Gal}(L\cdot T|K): \sigma'|_T = \sigma|_T,\ \sigma'|_L = \mathrm{id}_L \\ \emptyset, & \text{otherwise.} \end{cases}$$

$\vdots$

"$\square$"

Thm $G = \mathrm{Gal}(M|K)$ is Hausdorff, totally disconnected, compact.

Pf Hausdorff + tot. disconn.

Take any $\sigma \neq \sigma' \in G$.

$\Rightarrow \sigma|_L \neq \sigma'|_L$ for some finite Gal. ext. $L \subseteq M$ of K.

$\Rightarrow U_{\sigma,L} \cap U_{\sigma',L} = \emptyset$ (⇒ Hausdorff)

$U_{\sigma,L}$
σ
$U_{\sigma',L}$
σ'

In fact, $G \setminus U_{\sigma,L} = \bigcup_{\substack{\tau \in G: \\ \tau|_L \neq \sigma|_L}} U_{\tau,L}$ is open

(⇒ tot. disconnected)

compact

$$\underbrace{\mathrm{Gal}(M|K) = \varprojlim_{\substack{L \subseteq M \\ \text{fin. Gal. ext.} \\ \text{of } K}} \mathrm{Gal}(L|K)}_{\text{compact}} \underset{\substack{\uparrow \\ \text{closed}}}{\subseteq} \underbrace{\prod_{L \ldots} \underbrace{\mathrm{Gal}(L|K)}_{\substack{\text{finite} \\ \Downarrow \\ \text{compact}}}}_{\text{compact}}$$

□

Reminder: compact ⇒ ~~every sequence has a convergent subsequence~~

Hausdorff ⇒ limits are unique (if they exist), all finite subsets are closed.

Thm If G is a compact top. group, $H \subseteq G$ is any subgroup:

H open $\Leftrightarrow$ H closed and $[G:H] < \infty$.

Pf G is the disjoint union of the left cosets of H. □

2.3. Dedekind domains

Let $\mathcal{O}_K$ be a Ded. dom., $L|K$ any Gal. ext., $\mathcal{O}_L$ the integral closure of $\mathcal{O}_K$ in L. (Might not be a Ded. dom. if $L|K$ is infinite!)

Let $\mathfrak{p}$ be a prime in $\mathcal{O}_K$.

Thm $Gal(L|K)$ acts transitively on $\{\mathfrak{P}$ max. id. of $\mathcal{O}_L$ lying above (=containing) $\mathfrak{p}\}$.

$$\begin{tikzcd}
L & \mathcal{O}_L & \mathfrak{P} & \cdots \\
K \arrow[u, dash, "G"] & \mathcal{O}_K \arrow[u, dash] & \mathfrak{p} \arrow[u, dash] \arrow[u, dash, shift right] \arrow[ur, dash] \arrow[ur, dash, shift left] &
\end{tikzcd}$$

Def Decomposition group $D(\mathfrak{P}|\mathfrak{p}) = Stab(\mathfrak{P}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$

Thm $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ is normal.

Cor If $\kappa(\mathfrak{p})$ is a perfect (e.g. finite) field, then $\kappa(\mathfrak{P})|\kappa(\mathfrak{p})$ is Galois.

Thm $D(\mathfrak{P}|\mathfrak{p}) \longrightarrow Gal(\kappa(\mathfrak{P})|\kappa(\mathfrak{p}))$ is surjective.

Def Inertia group $= ker(\ldots) = \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) \mid \sigma(x) \equiv x \bmod \mathfrak{P} \; \forall x \in \mathcal{O}_L\}$

Rmk $\mathfrak{P}|\mathfrak{q}$ is unramified if and only $I(\mathfrak{P}|\mathfrak{q}) = 1$.

Def If $\mathfrak{P}|\mathfrak{q}$ is unramified and $\kappa(\mathfrak{q}) = \mathbb{F}_q$, write

$$\begin{array}{ccc} D(\mathfrak{P}|\mathfrak{q}) & \xrightarrow{\sim} & \mathrm{Gal}(\kappa(\mathfrak{P})|\kappa(\mathfrak{q})) \\ \mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) & \longrightarrow & \varphi_q : x \mapsto x^q \end{array}$$

(Frobenius)

Rmk

$$\begin{array}{ccc} D(\sigma\mathfrak{P}|\mathfrak{q}) & = & \sigma\, D(\mathfrak{P}|\mathfrak{q})\, \sigma^{-1} \\ I & & I \\ \mathrm{Frob} & & \mathrm{Frob} \end{array}$$

Cor $\mathrm{Frob}(\mathfrak{q}) = \{\mathrm{Frob}(\mathfrak{P}|\mathfrak{q}) : \mathfrak{P} \ni \mathfrak{q}\}$ is a conj. class in G

Lemma D, I are closed subgroups of G.

Pf

$$D(\mathfrak{P}|\mathfrak{q}) = \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

$$= \{\sigma \in G \mid \underbrace{\sigma(\mathfrak{P} \cap F) = \mathfrak{P} \cap F}_{\text{only depends on } \sigma|_F} \ \forall F \subseteq L \text{ fin. Gal. ext. of } K\}$$

$$= \bigcap_F \text{closed set}$$

is closed

$I = \_\_\_$ □

Rmk If G is abelian, $D(\mathfrak{R}|\mathfrak{q}), \dots$ only depend on $\mathfrak{q}$ (and L). $\rightsquigarrow$ $D_{L|K}(\mathfrak{q})$, $I_{L|K}(\mathfrak{q})$, $\mathrm{Frob}_{L|K}(\mathfrak{q})$

Rmk If K is complete w.r.t. a disc. val. v, $\mathcal{O}_K \overset{\mathcal{O}_v}{=}$ and $\mathcal{O}_L$ have just one max. id. $\rightsquigarrow$ $\underbrace{D(L|K)}_{\substack{\shortparallel \\ \mathrm{Gal}(L|K)}}$, $I(L|K)$, $\mathrm{Frob}(L|K)$.

Rmk

$$\begin{tikzcd}
M \arrow[d, dash, "H"] \arrow[dd, dash, bend right=60, "G"'] & \mathcal{O}_M \arrow[d, dash] & P \arrow[d, dash] \\
L \arrow[d, dash] & \mathcal{O}_L \arrow[d, dash] & \mathfrak{R} \arrow[d, dash] \\
K & \mathcal{O}_K & \mathfrak{q}
\end{tikzcd}$$

$$D(P|\mathfrak{R}) = D(P|\mathfrak{q}) \cap H$$

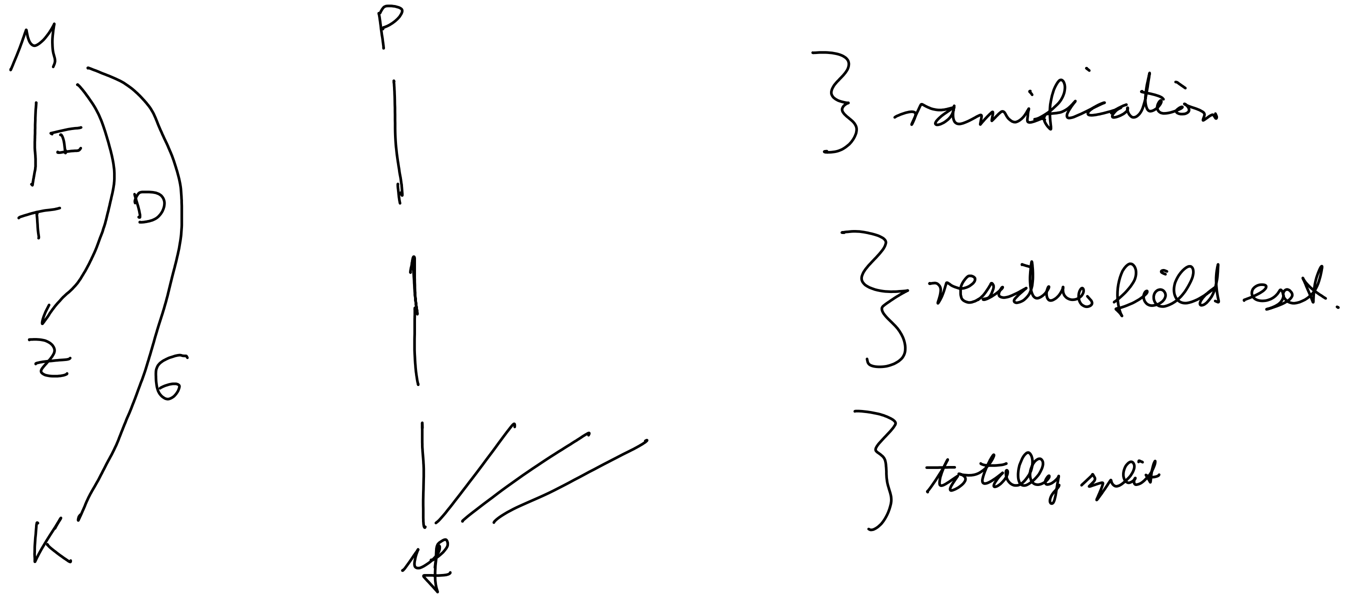
$I \qquad\qquad I$

If $L|K$ is Galois, then

$D(\mathfrak{R}|\mathfrak{q}) =$ image of $D(P|\mathfrak{q})$ under the restriction $G \to G/H$

$I \qquad\qquad\qquad\qquad I$

In particular, $\mathfrak{R}|\mathfrak{q}$ unramified $\iff$ $I(P|\mathfrak{q}) \subseteq H$.



Ex $L=\mathbb{Q}(\zeta_\infty)$, $K=\mathbb{Q}$

$$I_{\mathbb{Q}(\zeta_\infty)|\mathbb{Q}}(p) \subseteq Gal(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) = \hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$$

If $p \nmid m$, then $\mathbb{Q}(\zeta_m)|\mathbb{Q}$ is unram. at p.

$$\Rightarrow I(p) \subseteq Gal(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}(\zeta_m))$$
$$= \{x \in \hat{\mathbb{Z}}^\times \mid \underbrace{x \equiv 1 \bmod m}_{\Leftrightarrow\ \zeta_m^x = \zeta_m}\}$$

$$\Rightarrow I(p) \subseteq \mathbb{Z}_p^\times$$

For any $k \geq 0$, $\mathbb{Q}(\zeta_{p^k})|\mathbb{Q}$ is totally ramified at p.

$\Rightarrow$ The restriction of the restriction map

$$\underset{\hat{\mathbb{Z}}^\times}{\underset{\parallel}{Gal(\mathbb{Q}(\zeta_\infty)|\mathbb{Q})}} \twoheadrightarrow \underset{(\mathbb{Z}/p^k\mathbb{Z})^\times}{\underset{\parallel}{Gal(\mathbb{Q}(\zeta_{p^k})|\mathbb{Q})}}$$

to $I(p)$ is surjective.

$\Rightarrow I(p) \cap U \neq \emptyset \qquad \forall$ open $\emptyset \neq U \subseteq \mathbb{Z}_p^\times$

$$\underset{\substack{\uparrow \\ I(p) \text{ closed}}}{\Rightarrow} \boxed{I(p) = \mathbb{Z}_p^\times}.$$

max. ext. $Z_p \subseteq \mathbb{Q}(\zeta_\infty)$ unram. at p:

$$Z_p = \bigcup_{\substack{m \geq 1: \\ p \nmid m}} \mathbb{Q}(\zeta_m) \qquad (\text{field fixed by } \mathbb{Z}_p^\times)$$

$$\mathrm{Frob}_{Z_p|\mathbb{Q}}(p) = \underset{\substack{\shortparallel \\ (p,p,\dots)}}{p} \in \underset{\substack{\bigcap\!\!\!| \\ \hat{\mathbb{Z}}^\times}}{\prod_{\ell \neq p} \mathbb{Z}_\ell^\times} = \mathrm{Gal}(Z_p|\mathbb{Q})$$

($\zeta_m \mapsto \zeta_m^p \Rightarrow$ induces Frobenius aut. $x \mapsto x^p$ in the residue field extension).

Ex Let K be a local field with residue field $\mathbb{F}_q$.

$\Rightarrow$ The max. unram. ext. of K is

$$\bigcup_{n \geq 1} K(\zeta_{q^n - 1}) = \bigcup_{\substack{m \geq 1: \\ \gcd(m,q)=1}} K(\zeta_m).$$

Pf See problem 2 on problem set 3. $\square$

3. Chebotarev density theorem

Thm 3.1 Let K be a number field and $n \geq 1$. Then, the following are equivalent:

a) $\forall\, p \equiv p' \bmod n$ prime numbers:

p and p' split in the same way in $\mathcal{O}_K$

$\left(p\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r},\ p'\mathcal{O}_K = \mathfrak{P}_1'^{e_1} \cdots \mathfrak{P}_r'^{e_r},\right.$

$\left. \kappa(\mathfrak{P}_i) = \kappa(\mathfrak{P}_i')\ \forall i \right)$

b) $K \subseteq \mathbb{Q}(\zeta_n)$.

c) $\forall\, p \equiv p' \bmod n$ prime numbers:

If p splits completely in K, then p' splits completely in K.

Pf a) $\Rightarrow$ c) clear

b) $\Rightarrow$ a) Case 1: $p, p' \nmid n$

$\Rightarrow p, p'$ unram. in $\mathbb{Q}(\zeta_n)$

— " — — $\overset{\cup|}{K}$

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\zeta_n)|\mathbb{Q}) &= (\mathbb{Z}/n\mathbb{Z})^\times \\ \mathrm{Frob}(p) &= p \bmod n \\ &\quad\ \ \| \\ \mathrm{Frob}(p') &= p \bmod n \end{aligned}$$

$\Rightarrow \mathrm{Frob}_{\mathbb{Q}(\zeta_n)}(p) = \mathrm{Frob}_{\mathbb{Q}(\zeta_n)}(p')$

$\Rightarrow \mathrm{Frob}_K(p) = \mathrm{Frob}_K(p')$

$\Rightarrow D_K(p) = D_K(p')$

$\Rightarrow p, p'$ split in the same way in K.

Case 2: $p \mid n$ or $p' \mid n$

Since $p \equiv p' \bmod n$, this implies $p = p'$. $\square$

c) $\Rightarrow$ b) today's goal!

Chebotarev density theorem (Чеботарёв, Чоботарьов)

Let K be a number field and $L|K$ a finite Galois extension with Galois group G. Let C be a conjugacy class in G. Then, the density of primes $\mathfrak{q} \subset \mathcal{O}_K$ with $\mathrm{Frob}_{L|K}(\mathfrak{q}) = C$, when ordered by norm $N(\mathfrak{q})$,

is $\frac{\#C}{\#G}$. More precisely:

$$\lim_{X \to \infty} \frac{\#\{\mathfrak{q} : N(\mathfrak{q}) \le X,\ \mathrm{Frob}_{L|K}(C)\}}{\#\{\mathfrak{q} : N(\mathfrak{q}) \le X\}} = \frac{\#C}{\#G}.$$

(Frob only makes sense for unram. $\mathfrak{q}$, but the finitely many ramified primes don't matter as $X \to \infty$.)

Ex ($\mathbb{Q}(\zeta_n)|\mathbb{Q}$) (Dirichlet's theorem on primes in arithmetic progressions)

$\Rightarrow$ For any $c \in (\mathbb{Z}/n\mathbb{Z})^\times$, the density of prime numbers p s.t. $p \equiv c \bmod n$ is

$$\frac{1}{\#(\mathbb{Z}/n\mathbb{Z})^\times} = \frac{1}{\varphi(n)}.$$

(All invertible residues mod n occur "equally often".)

Ex ($G = S_3$) in L in $F = L^{\langle(23)\rangle}$

$C_1 = \{id\}$ $\quad \mathfrak{q} = \mathfrak{q}_1 \cdots \mathfrak{q}_6 = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$

$\Rightarrow D = \{id\}$ for $\frac{1}{6}$ of $\mathfrak{q}$

$C_2 = \{(12), (13), (23)\}$

$\Rightarrow D =$ group of order 2 $\quad \mathfrak{q} = \mathfrak{q}_1\mathfrak{q}_2\mathfrak{q}_3 = \underset{\substack{\uparrow \\ f=1}}{\mathfrak{p}_1} \; \underset{\substack{\uparrow \\ f=2}}{\mathfrak{p}_2}$

for $\frac{1}{2}$ of $\mathfrak{q}$

$C_3 = \{(123), (132)\}$ $\quad \mathfrak{q} = \mathfrak{q}_1\mathfrak{q}_2 = \underset{\substack{\uparrow \\ f_1=3}}{\mathfrak{p}_1}$

$\Rightarrow D = \langle(123)\rangle$

for $\frac{1}{3}$ of $\mathfrak{q}$

Pf of Chebotarev density theorem

cf. last chapter of Neukirch: Alg. Number Theory

Pf of c) $\Rightarrow$ b) in Thm 1

p splits completely in K if and only if p splits completely in the Galois closure of $K|\mathbb{Q}$.

(See problem 1 on problem set 4.)

$\Rightarrow$ We can assume that K is a Galois extension of $\mathbb{Q}$.

An (unram.) prime p splits completely in K if and only if $\mathrm{Frob}_{K|\mathbb{Q}}(p) = \{id\}$.

Let L be the compositum of K and $\mathbb{Q}(\zeta_n)$.

$$\begin{tikzcd}
 & L \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & \mathbb{Q}(\zeta_n) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & Gal(L|\mathbb{Q}) \arrow[dl] \arrow[dr] & \\
Gal(K|\mathbb{Q}) & & Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \arrow[d, phantom, "\shortparallel"] \\
 & & (\mathbb{Z}/n\mathbb{Z})^\times
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathrm{Frob}_{L|\mathbb{Q}}(\mathfrak{P}|p) \arrow[dl] \arrow[dr] & \\
\mathrm{Frob}_{K|\mathbb{Q}}(\mathfrak{P}\cap K|p) & & \mathrm{Frob}(\mathfrak{P}\cap\mathbb{Q}(\zeta_n)|p)
\end{tikzcd}$$

Assume $K \not\subseteq \mathbb{Q}(\zeta_n)$. $\Rightarrow Gal(L|K) \not\supseteq Gal(L|\mathbb{Q}(\zeta_n))$.

$$\begin{tikzcd}[column sep=small]
\Rightarrow \exists \sigma \in Gal(L|\mathbb{Q}): & \sigma \notin Gal(L|K) \arrow[d, Leftrightarrow] , & \sigma \in Gal(L|\mathbb{Q}(\zeta_n)) \arrow[d, Leftrightarrow] \\
 & \sigma|_K \neq id & \sigma|_{\mathbb{Q}(\zeta_n)} = id.
\end{tikzcd}$$

$$\begin{tikzcd}
 & id \arrow[dl] \arrow[dr] & \\
id & & id \arrow[d, phantom, "\shortparallel"] \\
 & & 1 \bmod p
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \sigma \arrow[dl] \arrow[dr] & \\
\neq id & & id \arrow[d, phantom, "\shortparallel"] \\
 & & 1 \bmod n
\end{tikzcd}$$

By Chebotarev's density theorem, there exist p, p' such that $\mathrm{Frob}_L(p) = \mathrm{id}$, $\mathrm{Frob}_L(p') =$ conjugacy class containing.

$\Downarrow$ p splits completely in K $\quad$ $\Downarrow$ $p \equiv 1 \bmod n$ $\quad$ $\Downarrow$ p' doesn't split completely in K $\quad$ $\Downarrow$ $p' \equiv 1 \bmod n$.

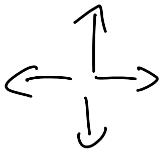
↯.

□

Ex of Thm 1 $\mathbb{Q}(\sqrt{n}) \subseteq \mathbb{Q}(\zeta_{|4n|})$, so the splitting behavior of p in $\mathbb{Q}(\sqrt{n})$ is determined by $p \bmod 4n$.

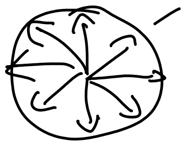
Pf It suffices to show this for primes $n = \ell$ and $n = -1$.

Case $n = -1$:



$\sqrt{-1} = i = \zeta_4$

Case $n = \ell = 2$:



$$\zeta_8 = \frac{\sqrt{2} + i \cdot \sqrt{2}}{2}$$

$$\zeta_8 + \zeta_8^{-1} = \sqrt{2}.$$

Case $n = \ell$ odd:

Quadr. subext. of $\mathbb{Q}(\zeta_\ell) \longleftrightarrow$ index two subgroups $H \subseteq \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)|\mathbb{Q}) = (\mathbb{Z}/\ell\mathbb{Z})^\times$

$\exists$ only one such subgroup (because $(\mathbb{Z}/\ell\mathbb{Z})^\times = \mathbb{F}_\ell^\times$ is cyclic):

$H = \{x \in (\mathbb{Z}/\ell\mathbb{Z})^\times \text{ quadr. res.}\}$

Look at $\alpha = \sum_{x \in (\mathbb{Z}/l\mathbb{Z})^\times} \left(\frac{x}{l}\right) \zeta_l^x$ (Gaußsum).

$$\phi_y(\alpha) = \sum_x \left(\frac{x}{l}\right) \zeta_l^{xy} = \sum_x \left(\frac{x/y}{l}\right) \zeta_l^x = \left(\frac{y}{l}\right) \sum_x \left(\frac{x}{l}\right) \zeta_l^x$$

$$= \left(\frac{y}{l}\right) \cdot \alpha = \pm \alpha.$$

(In part., $\phi_y(\alpha^2) = \alpha^2 \ \forall y$, so $\alpha^2 \in \mathbb{Q}$.
That's why we look at the Gaußsum!)

$$\alpha^2 = \sum_{x_1, x_2} \left(\frac{x_1 x_2}{l}\right) \zeta_l^{x_1 + x_2}$$

$$= \sum_{x_1, x_2} \left(\frac{x_2 / x_1}{l}\right) \zeta_l^{x_1 + x_2}$$

$$= \sum_{x_1, t} \left(\frac{t}{l}\right) \zeta_l^{x_1(1+t)}$$

$$= \sum_{t \in \mathbb{F}_l^\times} \left(\frac{t}{l}\right) \underbrace{\sum_{x_1 \in \mathbb{F}_l^\times} \zeta_l^{x_1(1+t)}}_{\substack{-1 \text{ if } t \neq -1 \\ l-1 \text{ if } t = -1}}$$

$$= \left(\frac{-1}{l}\right) \cdot l - \sum_t \left(\frac{t}{l}\right)$$

$$= \left(\frac{-1}{l}\right) \cdot l = \pm l.$$

$$\Rightarrow \sqrt{c} \text{ or } \sqrt{-c} \in \mathbb{Q}(\zeta_c)$$

$$\underset{\substack{\uparrow \\ \sqrt{-1} \in \mathbb{Q}(\zeta_4)}}{\Rightarrow} \sqrt{c} \in \mathbb{Q}(\zeta_{4c}) . \qquad \square$$

Last week

Gal$(L|K)$ compact

compact $\Rightarrow$ ~~sequentially compact~~

(correct for countable products of compact spaces)

Wyatt: Example where Gal$(L|K)$ is not sequentially compact

$K = \mathbb{R}(T)$

$L = K(\{\sqrt{T-\lambda} \mid \lambda \in \mathbb{R}\})$.

$$\Rightarrow \text{Gal}(L|K) = \underbrace{\prod_{\lambda \in \mathbb{R}} \mathbb{Z}/2\mathbb{Z}}_{\text{not sequentially compact}} \text{ with prod. topology}$$

For any finite, local, global field K, Gal$(K^{sep}|K)$ is sequentially compact, because there are only countably many finite Galois extensions of K.

<u>Preview</u>

How to tell whether $K \subseteq \mathbb{Q}(\zeta_\infty)$?

<u>Surprise:</u>

<u>Kronecker-Weber Theorem</u>

$\mathbb{Q}(\zeta_\infty)$ is the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$.

Equivalently: A fin. field ext. $K \mid \mathbb{Q}$ is abelian if and only if $K \subseteq \mathbb{Q}(\zeta_n)$ for some $n \geq 1$.
The smallest such n (= gcd of all such n) is called the <u>conductor</u> of K.

<u>Ex</u> $K = \mathbb{Q}(\sqrt{a})$ is an abelian ext.

Its conductor is $|\underset{\uparrow}{\operatorname{disc}}(K)|$.
discriminant of K

<u>Local Kronecker-Weber Theorem</u>

$$\mathbb{Q}_p(\zeta_\infty) = \bigcup_{n \geq 1} \mathbb{Q}_p(\zeta_n) \text{ is the max. abelian ext. of } \mathbb{Q}_p.$$

Slightly dangerous notation:
The primitive n-th roots of unity might not be Galois conjugate over $\mathbb{Q}_p$.
But they all generate the same field ext. of $\mathbb{Q}_p$.

<u>Question</u> What are the max. ab. ext. of other number fields / local fields K? What is $\mathrm{Gal}(K^{ab} \mid K)$? How to compute the conductor of an abelian extension?

1.9. Normalised absolute values

Def Let K be a local field.

$|x|_K = q_K^{-v_K(x)}$ if K is nonarch. with res. field $\mathbb{F}_{q_K}$, normalised disc. val. v_K.

$|x|_{\mathbb{R}} = |x|$, the usual abs. value if $K = \mathbb{R}$

$|x|_{\mathbb{C}} = |x|^2 = |x \cdot \bar{x}|$ if $K = \mathbb{C}$

$\uparrow$ Doesn't satisfy the triangle inequality.

Lemma 1.6.1 For any (fin.) ext. $L|K$ of local fields,

$$|x|_L = |Nm_{L|K}(x)|_K \qquad \forall x \in L.$$

Pf L, K nonarch.:

$$q_L = q_K^f, \quad v_L(x) = e \cdot v_K(x) = e \cdot \frac{1}{n} \cdot v_K(Nm_{L|K}(x)),$$

$n = e \cdot f$.

$L = \mathbb{C}, K = \mathbb{R}$ clear. □

4. Global fields

Def A global field K is

a) a fin. ext. of $\mathbb{Q}$ (number field)

b) a fin. (separable) ext. of $\mathbb{F}_p(T)$ ((global) function field).

4.1. Places

For any disc. val. v on K, we get a local field $\hat{K}_v$ with ring of integers $\hat{\mathcal{O}}_v$. There's a natural embedding $K \hookrightarrow \hat{K}_v$.

Change of notation: $K_v := \hat{K}_v$, $\mathcal{O}_v := \hat{\mathcal{O}}_v$.

If K is a number field, we also have real embeddings $K \hookrightarrow \mathbb{R}$, pairs of complex embeddings $K \hookrightarrow \mathbb{C}$.

Def A place v of K is

- a (norm.) disc. val. v, leading to an emb. $K \hookrightarrow K_v$ } finite (nonarch.) place
- an embedding $K \hookrightarrow \mathbb{R}$ $(K_v := \mathbb{R})$ } infinite (arch.) place.
- a pair of complex conj. emb. $K \hookrightarrow \mathbb{C}$ $(K_v := \mathbb{C})$

Rmk The places are the equivalence classes of multiplicative valuations ~~on~~ K (cf. Neukirch, II.3, III.1)

Eg The places of $\mathbb{Q}$ are the prime numbers $v = p$ and $v = \infty$.
↑
(the real embedding)

Def If $L|K$ is an ext of global fields, v is a place of K, w is a place of L, we write $w|v$ if $K \hookrightarrow K_v$ "is" the restriction of $L \hookrightarrow L_w$ to K.

The cases are:

- $v = v_{\mathfrak{q}}$, $w = v_{\mathfrak{P}}$, $\quad \mathfrak{P} | \mathfrak{q}$
  $\mathfrak{q} \subseteq \mathcal{O}_K$, $\mathfrak{P} \subseteq \mathcal{O}_L$
- $v : K \hookrightarrow \substack{\mathbb{R}\\ \mathbb{C}}$, $w : L \hookrightarrow \substack{\mathbb{R}\\ \mathbb{C}}$, $w|_K = v$

Ex The places of $\mathbb{Q}(\sqrt{2})$ are the primes and ∞_1, ∞_2
$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\uparrow$ real emb.

$\infty_1, \infty_2 | \infty$.

Lemma For any fin. separable ~~ext~~. $L|K$ of global fields and any place v of K,

$$\prod_{w|v} |x|_w = |N_{L|K}(x)|_v.$$

Pf $L|K$ is separable $\Rightarrow L \otimes_K K_v \cong \prod_{w|v} L_w$.

$$\prod_{w|v} |x|_w \overset{\boxed{\text{Lemma 1.6.1}}}{=} \prod_{w|v} |N_{L_w|K_v}(x)|_v = \Big|\prod_{w|v} N_{L_w|K_v}(x)\Big|_v$$

$$= \Big|N_{L\otimes_K K_v|K_v}(x)\Big|_v = |N_{L|K}(x)|_v. \quad \square$$

Thm (Product Formula) Let K be a global field.

$$\Rightarrow \prod_v |x|_v = 1 \qquad \forall x \in K^\times.$$

Pf for $K = \mathbb{Q}$

$$x = \pm \prod_p p^{a_p}. \implies |x|_p = p^{-a_p} \quad \forall p$$

$$|x|_\infty = \prod_p p^{a_p}$$

$$\prod_v |x|_v = 1.$$

□

Pf for $K = \mathbb{F}_q(T)$

$$x = \lambda \cdot \prod_{\substack{f(T) \text{ monic} \\ \text{irred.}}} f(T)^{a_f} \qquad (\lambda \in \mathbb{F}_q^\times)$$

$\implies |x|_f = q^{-\deg(f) \cdot a_f}$ (res. field $\mathbb{F}_q[T]/f(T)$ has size $q^{\deg(f)}$).

$|x|_\infty = q^{\deg(x)} = q^{\sum_f \deg(f) \cdot a_f}$ (res. field $\mathbb{F}_q[\frac{1}{T}]/(\frac{1}{T}) = \mathbb{F}_q$).

□

Pf for general K

Say K is a fin. ext. of $\mathbb{Q}$.

$$\implies \prod_{w \text{ pl. of } K} |x|_w = \prod_{v \text{ pl. of } \mathbb{Q}} \prod_{w|v} |x|_w \underset{\text{Lemma}}{\overset{\uparrow}{=}} \prod_v |\mathrm{Nm}_{K|\mathbb{Q}}(x)|_v = 1.$$

Same for fin. ext. of $\mathbb{F}_q(T)$.

□

4.2. Adèles

Motivation Let $f(x_1, \dots, x_n) \in \mathbb{Q}[x_1, \dots, x_n]$.
$\rightsquigarrow V = \{(x_1, \dots, x_n) : f(x_1, \dots, x_n) = 0\}$.

Assume $V(\mathbb{Q}) \neq \emptyset$.
$\Rightarrow V(\mathbb{Q}_p) \neq \emptyset \ \forall p$, $V(\mathbb{R}) \neq \emptyset$

$\Leftrightarrow V(\prod_p \mathbb{Q}_p \times \mathbb{R}) \neq \emptyset$.

Note that any $x \in \mathbb{Q}$ lies in $\mathbb{Z}_p$ for all but finitely many p (those not dividing the denominator of x).

Def The adèle ring $\mathbb{A}_K$ is the ring of tuples $(x_v)_v \in \prod_v K_v$ such that $x_v \in \mathcal{O}_v$ for all but finitely many nonarch. places v.

Rmk $K \subset \mathbb{A}_K$.
$x \mapsto (x)_v$.
In part., if $V(K) \neq \emptyset$, then $V(\mathbb{A}_K) \neq \emptyset$.

Def Define a topology on $\mathbb{A}_K$ with open base consisting of sets of the form $\prod_v U_v$, where all $U_v \subseteq K_v$ are open, and $U_v = \mathcal{O}_v$ for all but finitely many nonarch. places v.

Rmk $\mathbb{A}_K$ is a topological ring:
$+ : \mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$, $\times : \mathbb{A}_K \times \mathbb{A}_K \to \mathbb{A}_K$
are continuous.

Rmk $K \subseteq \mathbb{A}_K$ is discrete.

Pf It suffices to prove that for any $x \in K$, there is an open set $U \subseteq \mathbb{A}_K$ such that $K \cap U = \{x\}$.

W.l.o.g. $x = 0$.

Fix a nonempty finite set S of places containing all arch. places.

Take $$U = \prod_{v \notin S} \underbrace{\{x \in K_v \mid |x|_v \leq 1\}}_{\overset{\shortparallel}{\mathcal{O}_v}} \times \prod_{v \in S} \underbrace{\{x \in K_v \mid |x|_v < 1\}}_{\text{open}}.$$

By the product formula, U contains no element of K other than 0. $\square$

Rmk $K \subseteq \mathbb{A}_K$ is closed.

Rmk $\mathbb{A}_K / K$ is compact.

4.3. Adèles in extension land

Let $L|K$ be a separable ext. of global fields.

$$\begin{tikzcd}
L \arrow[d, dash] & w_1 \arrow[dr, dash] & w_2 \arrow[d, dash] & w_3 \arrow[dl, dash] & & \cdot \arrow[d, dash] & \cdot \arrow[dl, dash] & \cdot \arrow[d, dash] & \cdots \\
K & & v & & & \cdot & & \cdot &
\end{tikzcd}$$

$$\overbrace{L_{w_1}\times L_{w_2}\times L_{w_3}}^{\cong K_v \otimes_K L}$$

$$\begin{tikzcd}
L \arrow[d, dash] & L_{w_1} & L_{w_2} & L_{w_3} & \cdots \\
K & K_v \arrow[u, bend left] \arrow[ur, bend right] \arrow[urr, bend right] & & &
\end{tikzcd}$$

$\Rightarrow$ Thm 4.3.1 $\quad \mathbb{A}_L \overset{\text{as rings}}{\cong} \mathbb{A}_K \otimes_K L$

$$\begin{tikzcd}
\mathbb{A}_L \arrow[dr, phantom, "\cong"', "\text{as top. groups}"] & \mathbb{A}_K \otimes_K L \arrow[d, phantom, "\cong"] \\
& \underbrace{\mathbb{A}_K \times \dots \times \mathbb{A}_K}_{[L:K]}
\end{tikzcd}$$

Rmk $\quad \mathbb{A}_K \subseteq \mathbb{A}_L \quad$ is cont.

Rmk If $\sigma \in \mathrm{Gal}(L|K)$, we get an automorphism σ of $\underset{\overset{\shortparallel}{\mathbb{A}_L}}{\mathbb{A}_K \otimes_K L}$: $\;x \otimes y \longmapsto x \otimes \sigma(y)$.

Explicitly, $\sigma(x_w)_w = (\sigma\, x_{w\circ\sigma})_w$

$$= (\sigma\, x_{\sigma^{-1}w})_w .$$

Def Trace $\mathrm{Tr}_{L|K} : \mathbb{A}_L \longrightarrow \mathbb{A}_K$
$$(x_w)_w \longmapsto \Big(\sum_{w|v} \mathrm{Tr}_{L_w|K_v}(x_w)\Big)_v \quad \Big(= \sum_{\sigma\in \mathrm{Gal}} \sigma x \text{ if } L|K \text{ Galois}\Big)$$

Norm $\mathrm{Nm}_{L|K} : \mathbb{A}_L \longrightarrow \mathbb{A}_K$
$$(x_w)_w \longmapsto \Big(\prod_{w|v} \mathrm{Nm}_{L_w|K_v}(x_w)\Big)_v \Big(= \prod_{\sigma} \sigma x \text{ if } L|K \text{ Galois}\Big)$$

4.4. Approximation theorems

Let K be a global field.

Weak approximation theorem

$\Uparrow$ Let S be a finite set of places of K. Then, the map $K \longrightarrow \prod_{v \in S} K_v$ has dense image.

Strong approximation theorem (away from S)

Let S be a nonempty set of places of K. Let

$$\mathbb{A}_K^S := \{ (x_v)_{v \notin S} \in \prod_{v \notin S} K_v \mid x_v \in \mathcal{O}_v \text{ for almost all } v \} = \prod_{v \notin S}{}' K_v.$$

(restricted product)

Then, the map $K \hookrightarrow \mathbb{A}_K^S$ has dense image.

Note It suffices to prove this for every 1-element set S.

Exe $K = \mathbb{Q}$, $S = \{\infty\}$.

Open base of $\mathbb{A}_K^S$: $U = \prod_p U_p$, $y_p + p^{e_p}\mathbb{Z}_p \subseteq U_p \subseteq \mathbb{Q}_p$ open $\forall p$

$(y_p \in \mathbb{Q}_p,\ e_p \in \mathbb{Z})$

$U_p = \mathbb{Z}_p$ for a.a. p

Goal: $\exists\, x \in \mathbb{Q}$: $x \in y_p + p^{e_p}\mathbb{Z}_p$ for fin. many p

$x \in \mathbb{Z}_p$ for all other p.

Multiplying by powers of p, we can make $y_p \in \mathbb{Z}_p$, $e_p \geq 0$.

Use the Chinese remainder theorem.

Ex $K=\mathbb{Q}$, $S=\{2\}$.

Open base of $\mathbb{A}_K^S$: $U=\prod_{p\neq 2} U_p \times U_\infty$, $y_p+p^{e_p}\mathbb{Z}_p \subseteq U_p \subseteq \mathbb{Q}_p \ \forall p\neq 2$

$U_p=\mathbb{Z}_p$ for a.a. $p\neq 2$

$(r,s)\subseteq U_\infty \subseteq \mathbb{R}$ open

Goal: $\exists\, x\in\mathbb{Q}$: $x\in y_p+p^{e_p}\mathbb{Z}_p$ for fin. many $p\neq 2$.

$x\in\mathbb{Z}_p$ for all other $p\neq 2$

$x\in(r,s)$.

Multiplying by powers of $p\neq 2$, we can make $y_p\in\mathbb{Z}_p$, $e_p\geq 0$. $\forall p\neq 2$.

Multiplying by a large power of 2, we can make $s-r>\prod_{p\neq 2}p^{e_p}$.

Use the Chinese remainder theorem.

Pf See Cassels-Fröhlich (Alg. Number Theory): Chapter II.15. □

More generally, one studies the following properties:

Def A variety V defined over K *satisfies weak approximation at S* if $V(K)\longrightarrow V(\prod_{v\in S}K_v)$ has dense image.

Def Say K is a number field. A variety V defined over $\mathcal{O}_K$ *satisfies strong approximation away from S* if $V(K)\hookrightarrow V(\mathbb{A}_K^S)$ has dense image.

Rmk We showed that the affine line $\mathbb{A}^1$ satisfies strong approximation.

4.5. Cocompactness

Thm 4.5.1 $\mathbb{A}_K/K$ is compact for any global field K.

Rmk By Thm 4.3.1., it suffices to show this for $K=\mathbb{Q}, \mathbb{F}_p(T)$.

Lemma Let $\mathcal{O}_K$ be the integral closure of $\left\{\begin{matrix}\mathbb{Z}\\ \mathbb{F}_p[T]\end{matrix}\right\}$ in K.

Then, $$\mathbb{A}_K/K \cong \left(\prod_{v\nmid\infty}\mathcal{O}_v \times \prod_{v\mid\infty} K_v\right)\Big/\mathcal{O}_K.$$

Pf "$\mapsto$" strong approximation

"$\mapsfrom$" $\{x\in K \mid x\in\mathcal{O}_v \ \forall v\nmid\infty\} = \mathcal{O}_K$. □

Pf of 4.5.1 for $K=\mathbb{Q}$

$$\begin{tikzcd} \mathbb{A}_\mathbb{Q}/\mathbb{Q} \cong \left(\prod_p \mathbb{Z}_p \times \mathbb{R}\right)/\mathbb{Z} \\ \prod_p \mathbb{Z}_p \times [0,1] \text{ compact} \arrow[u, two heads] \end{tikzcd}$$ □

Pf of 4.5.1 for any number field K

$$\begin{tikzcd} \mathbb{A}_K/K \cong \left(\prod_{\mathfrak{p}} \mathcal{O}_\mathfrak{p} \times (K\otimes_\mathbb{Q}\mathbb{R})\right)\Big/\mathcal{O}_K \\ \prod_{\mathfrak{p}}\mathcal{O}_\mathfrak{p} \times \left([0,1]\cdot\omega_1 + \dots + [0,1]\cdot\omega_n\right) \text{ compact,} \arrow[u, two heads] \end{tikzcd}$$

where $\omega_1,\dots,\omega_n$ is an integral basis of K. □

Pf of 4.5.1 for $K=\mathbb{F}_p(T)$

$$\begin{tikzcd} \mathbb{A}_{\mathbb{F}_p(T)}/\mathbb{F}_p(T) \cong \left(\prod_f \mathcal{O}_f \times \mathbb{F}_p((\tfrac{1}{T}))\right)/\mathbb{F}_p[T] \\ \prod_f \mathcal{O}_f \times \{f\in\mathbb{F}_p((\tfrac{1}{T})) \mid v_\infty(f)\geq 0\} \text{ compact} \arrow[u, two heads] \end{tikzcd}$$ □

4.6. Idèles

Group of idèles $\mathbb{A}_K^\times$.

Trouble $\mathbb{A}_K^\times \longrightarrow \mathbb{A}_K^\times$, $x \longmapsto x^{-1}$ is not continuous w.r.t. the subspace topology! ⇝ Using the subspace top. doesn't yield a top. group!

Pf $U := \left(\prod_{v \text{ nonarch}} \mathcal{O}_v \times \prod_{v \text{ arch.}} K_v \right) \cap \mathbb{A}_K^\times$ open w.r.t. subsp. top.

$$\| $$

$$\{ (x_v)_v \in \mathbb{A}_K^\times \mid v(x_v) \geq 0 \ \forall v \text{ nonarch} \}.$$

$$U^{-1} = \{ (x_v)_v \in \mathbb{A}_K^\times \mid v(x_v) \leq 0 \ \forall v \text{ nonarch} \}.$$

doesn't contain any nonempty open subset of $\mathbb{A}_K$.

$$\left(\prod U_v, \quad U_v = \mathcal{O}_v \text{ for a.a. } v \right). \qquad \square$$

Exc $\mathbb{A}_K^\times \cong \{ (x,y) \in \mathbb{A}_K \times \mathbb{A}_K \mid xy = 1 \}$ as groups

$x \longmapsto (x, x^{-1})$

Use the subspace top. on the RHS $\subseteq \mathbb{A}_K \times \mathbb{A}_K$.

⇝ $\mathbb{A}_K^\times$ is automatically a topological group!

Rmk Open base for top. on $\mathbb{A}_K^\times$:

$\prod_v U_v$, where $U_v \subseteq K_v^\times$ open $\forall v$,

$U_v = \mathcal{O}_v^\times$ for a.a. (nonarch.) v.

Rmk $K^\times \subseteq \mathbb{A}_K^\times$ is discrete and closed.

Def The idèle class group of K is $\mathbb{A}_K^\times / K^\times$.

We have a content map $c : \mathbb{A}_K^\times \longrightarrow \mathbb{R}^{>0}$

$$(x_v)_v \longmapsto \prod_v |x_v|_v$$

fin. prod. because $x_v \in \mathcal{O}_v^\times$ and therefore $|x_v|_v = 1$ for a.a. v

Rmk $c(\mathbb{A}_K^\times) = \begin{cases} \mathbb{R}^{>0}, & K \text{ number field} \\ q^{\mathbb{Z}} (?), & K \text{ function field with residue field } \mathbb{F}_q \end{cases}$

is an infinite subset of $\mathbb{R}^{>0}$.

Def $J_K^1 := \ker(c) = \{ (x_v)_v \in \mathbb{A}_K^\times \mid \prod_v |x_v|_v = 1 \}$.

Rmk Product formula: $K^\times \subseteq J_K^\times$.

$\Rightarrow \mathbb{A}_K^\times / K^\times$ is not compact (image of $\mathbb{A}_K^\times / K^\times \xrightarrow{c} \mathbb{R}^{>0}$ isn't compact)

Thm $J_K^1 / K^\times$ is compact.

Pf See Cassels-Fröhlich: Chapter II.16. $\square$

Ex $K = \mathbb{Q}$.

$$J_{\mathbb{Q}}^1 / \mathbb{Q}^\times \cong \prod_p \mathbb{Z}_p^\times = \hat{\mathbb{Z}}^\times .$$

$$[(x_2, x_3, \dots, x_\infty)] \longmapsto (x_2, x_3, \dots)$$

$|x_2|_2 |x_3|_3 \cdots |x_\infty|_\infty = 1$

multiply by appropriate power of p to make $x_p \in \mathbb{Z}_p^\times$ ($\Leftrightarrow |x_p|_p = 1$)

multiply by ± 1 to make $x_\infty > 0$

$\Rightarrow x_\infty = 1$

Thm Let K be a number field.

$$\Rightarrow \mathbb{A}_K^\times \Big/ K^\times \cdot \Big(\prod_{v\nmid\infty} \mathcal{O}_v^\times \times \prod_{v|\infty} K_v^\times\Big) \cong Cl_K$$

(the ideal class group)

Pf
$$\text{LHS} \cong \prod_{\mathfrak{p}}{}' \left(K_\mathfrak{p}^\times / \mathcal{O}_\mathfrak{p}^\times\right) \Big/ K^\times \cong \Big(\prod_{\mathfrak{p}}{}' \mathbb{Z}\Big) \Big/ K^\times$$

$$[(x_\mathfrak{p})_\mathfrak{p}] \longmapsto [(v_\mathfrak{p}(x_\mathfrak{p}))_\mathfrak{p}]$$

$$\cong \Big(\prod_{\mathfrak{p}}{}' \mathfrak{p}^{\mathbb{Z}}\Big) \Big/ K^\times \cong (\text{frac. ideals of } K)/K^\times.$$

$\square$

Cor We get an exact sequence

$$1 \longrightarrow \Big(\prod_{v\nmid\infty} \mathcal{O}_v^\times \times \prod_{v|\infty} K_v^\times\Big) \Big/ \mathcal{O}_K^\times \longrightarrow \mathbb{A}_K^\times / K^\times \longrightarrow Cl_K \longrightarrow 1.$$

5. Class field theory

5.1. Artin reciprocity maps

Def $\left\{\begin{matrix}\text{finite}\\ \text{local}\\ \text{global}\end{matrix}\right\}$ field $K \rightsquigarrow$ topological group $C_K := \left\{\begin{matrix}\mathbb{Z} \text{ (disc. top.)}\\ K^\times\\ \mathbb{A}_K^\times/K^\times\end{matrix}\right\}$

$L|K$ finite Gal. ext. $\rightsquigarrow$ continuous action of $\mathrm{Gal}(L|K)$ on C_L
(trivial action for finite fields)

$L|K$ finite ext. $\rightsquigarrow$ cont. hom. $\mathrm{Nm}_{L|K}: C_L \longrightarrow C_K$
(mult. by $[L:K]$ for finite fields)

Thm For any K as above, there is a continuous group hom.
(Artin reciprocity map) (to be constructed later)

$$\theta_K : C_K \longrightarrow \mathrm{Gal}(K^{ab}|K)$$

satisfying a list of properties (to follow).

Prop 1 (Fin. ab. ext) We get bijections

$$\left\{\begin{matrix}U \subseteq C_K \text{ open subgr.}\\ \text{of fin. index}\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}V \subseteq \mathrm{Gal}(K^{ab}|K) \text{ open}\\ \text{(fin. index)}\end{matrix}\right\} \xleftrightarrow{\text{fund. thm. of Galois theory}} \{L|K \text{ fin. ab. ext.}\}$$

$$U = \theta_K^{-1}(V) = \boxed{\mathrm{Nm}_{L|K}(C_L)} \qquad V = \overline{\theta_K(U)} = \mathrm{Gal}(K^{ab}|L) \qquad L = (K^{ab})^V = (K^{ab})^{\theta_K(U)}$$

For any fin. ab. ext. $L|K$, we get an isom.

$$C_K/\mathrm{Nm}_{L|K}(C_L) \xrightarrow[\sim]{\theta_{L|K}} \mathrm{Gal}(L|K).$$

Cor $\mathrm{Gal}(K^{ab}|K)\left(= \varprojlim_{\substack{L|K \text{ fin.}\\ \text{ab. ext.}}} \mathrm{Gal}(L|K)\right) \cong \varprojlim_{\substack{U \subseteq C_K\\ \text{open subgr.}\\ \text{of fin. index}}} C_K/U =: \underset{\uparrow}{\hat{C}_K}$

profinite completion of C_K

Cor $\Theta_K(C_K)$ is dense in $\mathrm{Gal}(K^{ab}|K)$.

Prop 2 (Functoriality)

For any fin. ext. $L|K$, we get a comm. diagram

$$\begin{tikzcd}
C_L \arrow[r, "\Theta_L"] \arrow[d, "\mathrm{Nm}_{L|K}"'] & \mathrm{Gal}(L^{ab}|L) \arrow[d, "\text{restriction}"] \\
C_K \arrow[r, "\Theta_K"'] & \mathrm{Gal}(K^{ab}|K)
\end{tikzcd}$$

$$\begin{tikzcd}
K^{ab} \arrow[r, dash] \arrow[d] & L^{ab} \arrow[d, dash] \\
K \arrow[r, dash] & L
\end{tikzcd}$$

Ex $K = \mathbb{F}_q$

$$\mathbb{Z} \xhookrightarrow{\Theta_{\mathbb{F}_q}} \hat{\mathbb{Z}} = \mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$$

$$1 \longmapsto 1 = \varphi_q \quad \text{(Frobenius aut.)}$$

$$\underset{\mathrm{Nm}_{\mathbb{F}_{q^n}|\mathbb{F}_q}(\mathbb{Z})}{\underset{\parallel}{\{U = n\mathbb{Z} \mid n \geq 1\}}} \longleftrightarrow \{V = n\hat{\mathbb{Z}} \mid n \geq 1\} \longleftrightarrow \{L = \mathbb{F}_{q^n} \mid n \geq 1\}$$

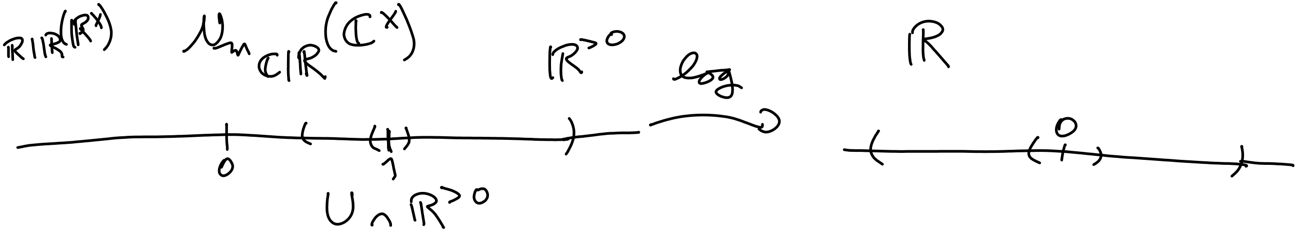
$$\mathbb{Z}/n\mathbb{Z} \xrightarrow[\sim]{\Theta_{\mathbb{F}_q}} \mathrm{Gal}(\mathbb{F}_{q^n}|\mathbb{F}_q)$$

$$1 \bmod n \longmapsto \varphi_q$$

Exe $K = \mathbb{R}$

$$\mathbb{R}^\times \xrightarrow{\theta_{\mathbb{R}}} \mathrm{Gal}(\mathbb{C}|\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$$

$$\{\underset{\mathrm{Nm}_{\mathbb{R}|\mathbb{R}}(\mathbb{R}^\times)}{\underset{\|}{\mathbb{R}^\times}}, \underset{\mathrm{Nm}_{\mathbb{C}|\mathbb{R}}(\mathbb{C}^\times)}{\underset{\|}{\mathbb{R}^{>0}}}\} \longleftrightarrow \{\mathbb{Z}/2\mathbb{Z}, 0\} \longleftrightarrow \{\mathbb{R}, \mathbb{C}\}$$



Exe $K = \mathbb{C}$

$$\mathbb{C}^\times \xrightarrow{\theta_{\mathbb{C}}} \mathrm{Gal}(\mathbb{C}|\mathbb{C}) = 1.$$

$$\{\underset{\mathrm{Nm}_{\mathbb{C}|\mathbb{C}}(\mathbb{C}^\times)}{\underset{\|}{\mathbb{C}^\times}}\} \longleftrightarrow \{1\} \longleftrightarrow \{\mathbb{C}\}$$

Exe K nonarch. local fields

$$C_K = K^\times = \mathcal{O}_K^\times \times \mathbb{Z}$$

$$\Rightarrow \hat{C}_K = \varprojlim_{\substack{U \subseteq K^\times \\ \text{open,} \\ \text{fin. index}}} K^\times/U = \varprojlim_{\substack{U \subseteq \mathcal{O}_K^\times \\ \text{open} \\ \text{(fin. index)}}} \mathcal{O}_K^\times/U \times \varprojlim_{\substack{U \subseteq \mathbb{Z} \\ \text{(open)} \\ \text{fin. index}}} \mathbb{Z}/U$$

$$= \widehat{\mathcal{O}_K^\times} \times \hat{\mathbb{Z}}$$

$$\underset{\substack{\uparrow \\ \boxed{\text{Lemma 5.1}}}}{=} \mathcal{O}_K^\times \times \hat{\mathbb{Z}}$$

$$\begin{tikzcd} \text{CFT} \Rightarrow \mathrm{Gal}(K^{ab}|K) \cong \hat{C}_K = \mathcal{O}_K^\times \times \hat{\mathbb{Z}} \\ K^\times = \mathcal{O}_K^\times \times \mathbb{Z} . \arrow[u, hook, "\theta_K"'] \end{tikzcd}$$

Ex $K = \mathbb{Q}_p$

Local Kronecker-Weber: $\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\zeta_\infty) = \bigcup_{n\geq 1} \mathbb{Q}_p(\zeta_n) = K_p \cdot \mathbb{Q}_p^{unram}$

$$\text{where } \underbrace{K_p}_{\text{a totally ramified ext.}} = \bigcup_{n\geq 1} \mathbb{Q}_p(\zeta_{p^n}), \quad \underbrace{\mathbb{Q}_p^{unram}}_{\text{max. (ab.) unram. ext.}} = \bigcup_{\substack{m\geq 1\\ p\nmid m}} \mathbb{Q}_p(\zeta_m) \underbrace{=}_{\forall m\not\equiv 0 \bmod p:\ \exists r\geq 1 : m \mid p^r-1} \bigcup_{r\geq 1} \mathbb{Q}_p(\zeta_{p^r-1})$$

$$\underbrace{K_p}_{\text{tot. ram.}} \cap \underbrace{\mathbb{Q}_p^{unram}}_{\text{unram.}} \overset{\Rightarrow}{=} \mathbb{Q}_p$$

$$\Rightarrow \mathrm{Gal}(\mathbb{Q}_p(\zeta_\infty)|\mathbb{Q}_p) = \mathrm{Gal}(K_p|\mathbb{Q}_p) \times \mathrm{Gal}(\mathbb{Q}_p^{unram}|\mathbb{Q}_p)$$

$$= \varprojlim_{n\geq 0} (\mathbb{Z}/p^n\mathbb{Z})^\times \times \mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)$$

$$= \mathbb{Z}_p^\times \times \hat{\mathbb{Z}} \qquad \checkmark$$

Prop 3 (Local-finite compatibility)

Let k be a nonarch. local field with residue field $\kappa = \mathbb{F}_q$. We get a comm. diagram

$$\begin{tikzcd}
k^\times \arrow[r, hook, "\theta_k"] \arrow[d, two heads, "v_k"'] & \mathrm{Gal}(k^{ab}|k) \arrow[d, two heads, "\text{reduction mod } \mathfrak{p}_{k^{ab}}"'] \arrow[r, phantom, "="] & D \arrow[d, two heads] \arrow[r, phantom, "="] & \mathrm{Gal}(k^{ab}|k) \arrow[d, two heads, "\text{restriction}"] \\
\mathbb{Z} \arrow[r, hook, "\theta_\kappa"'] & \mathrm{Gal}(\kappa^{ab}|\kappa) \arrow[r, phantom, "="] & D/I \arrow[r, phantom, "="] & \mathrm{Gal}(k^{unram}|k)
\end{tikzcd}$$

$$\begin{array}{lcl} \underline{\text{Cor}} \quad \mathrm{Gal}(k^{ab}|k) = \hat{C}_k = & \mathcal{O}_k^\times & \times \hat{\mathbb{Z}} \\ \qquad\quad \cup\!\vert & \cup\!\vert & \\ \rightsquigarrow \ I(k^{ab}|k) = & \mathcal{O}_k^\times & \end{array}$$

Prop 4 (Global-local compatibility)

Let K be a global field, and v be a place of K.

$$\begin{tikzcd}
\mathbb{A}_K^\times / K^\times \arrow[r, "\theta_K"] & \mathrm{Gal}(K^{ab}|K) \\
K_v^\times \arrow[u, hook, "\substack{\text{embedding}\\ \text{in } v\text{-coord.}}"] \arrow[r, "\theta_{K_v}"'] & \mathrm{Gal}(K_v^{ab}|K_v) = D(w|v) \arrow[u, hook]
\end{tikzcd}$$

for any ext. w of v from K to K^{ab} (well-def. subgroup of $\mathrm{Gal}(K^{ab}|K)$ (independent of choice of w) because all decomposition groups are conjugate and therefore identical in abelian extensions)

Some ideas for final papers

1. Witt vectors

$$\mathbb{Z}_p \rightsquigarrow \mathbb{F}_p$$

$$\mathbb{Z}_p \leftsquigarrow \mathbb{F}_p$$

$$\mathbb{Z}_q \leftsquigarrow \mathbb{F}_q$$

~~$\{0,1,\dots,p-1\}$~~

$\{0\} \cup \mu_{p-1}$

2. Complex multiplication

What is the max. ab. ext. of a given imaginary quadratic number field? (Has to do with elliptic curves!)

3. Tropical geometry

Newton polygons tell you what the valuations of the roots of a polynomial $\in K[X]$ are.

More generally, what are the valuations of the points on a variety V?

$\rightsquigarrow$ Fundamental theorem of tropical geometry

Transverse intersection theorem

4. Cubic and higher reciprocity laws

Know quadratic reciprocity.

How to generalise?

(...)

5. Hasse-Minkowski theorem

$\{f(x_1,\dots,x_n)=0\}$ for hom. degree 2 pol. f satisfies the Hasse principle.

6. Nonarch. local analysis

Haar measure on any local field

Lemma 5.1 Let G be a commutative compact topological group such $\bigcap\limits_{\substack{U \le G \\ \text{open} \\ \text{(fin. index)}}} U = 0$. Then $G = \underset{\substack{\uparrow \\ \text{profinite} \\ \text{completion}}}{\hat{G}}$.

Ex Let K be a number field.

$$\Rightarrow \hat{C}_K = C_K \Big/ \prod_{v \text{ real}} \mathbb{R}^{>0} \times \prod_{v \text{ complex}} \mathbb{C}^\times = C_K/(\text{comm. cp. of } C_K \text{ containing})$$

$$= \Big({\prod_{v \text{ nonarch}}}' K_v^\times \times \prod_{v \text{ real}} \underbrace{\mathbb{R}^\times / \mathbb{R}^{>0}}_{\{\pm 1\}} \Big) \Big/ K^\times$$

Pf Consider the map $f : C_K \longrightarrow \hat{C}_K = \varprojlim\limits_{\substack{U \le C_K \\ \text{open,} \\ \text{finite index}}} C_K/U$

Recall the continuous inclusion $i_v : K_v^\times \hookrightarrow C_K$.

For any U and any v, the set $i_v^{-1}(U) = $ "$U \cap K_v^\times$" $\subset K_v^\times$ is an open subgroup of $K_v^\times$.

$\Rightarrow$ For v real, $\mathbb{R}^{>0} \subseteq i_v^{-1}(U)$.

For v complex, $\mathbb{C}^\times = i_v^{-1}(U)$.

$\Rightarrow \prod\limits_{v \text{ real}} \mathbb{R}^{>0} \times \prod\limits_{v \text{ complex}} \mathbb{C}^\times \subseteq U \quad \forall U$

$\Rightarrow$ — " — $\subseteq \ker(f)$

In fact, — " — $= \bigcap\limits_U U = \ker(f)$.

We also have a continuous surjective map

$$\underbrace{J_K^1}_{\{(x_v)_v \in \mathbb{A}_K^\times \mid \prod_v |x_v|_v = 1\}} / K^\times \twoheadrightarrow \mathbb{A}_K^\times / K^\times \cdot \Big(\prod_{v \text{ real}} \mathbb{R}^{>0} \times \prod_{v \text{ complex}} \mathbb{C}^\times\Big).$$

LHS is compact (Thm. in section 4.6)

$\Rightarrow$ RHS is compact.

By Lemma 5.1, f is surjective. □

<u>Exe</u> Let K be a (global) function field.

$$\Rightarrow \underset{\substack{\uparrow \\ \text{not compact}}}{C_K} \longrightarrow \underset{\substack{\uparrow \\ \text{compact}}}{\widehat{C}_K} \text{ is injective, but not surjective.}$$

$$\boxed{\begin{array}{ccc} C_K & \longrightarrow & \mathbb{R}^{>0} \\ \shortparallel & & \\ \mathbb{A}_K^\times / K^\times & & \\ (x_v)_v & \longmapsto & \prod_v |x_v|_v \end{array}}$$

<u>Ex</u> $K = \mathbb{Q}$

Kronecker-Weber : $\mathbb{Q}^{ab} = \mathbb{Q}(\zeta_\infty) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_n)$

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) \arrow[r, phantom, "="] & \hat{\mathbb{Z}}^\times = \prod \mathbb{Z}_p^\times \arrow[rr, phantom, "="] & & \left(\prod_p{}' \mathbb{Q}_p^\times \times (\mathbb{R}^\times / \mathbb{R}^{>0}) \right) / \mathbb{Q}^\times \\
 & (\dots, p^{-1}, 1, p^{-1}, \dots) & p & \\
D(p) = \mathrm{Gal}(\mathbb{Q}_p(\zeta_\infty)|\mathbb{Q}_p) \arrow[uu, hook] \arrow[r, phantom, "="] & (0,1) \arrow[u, mapsto] & \mathbb{Z}_p^\times \times \hat{\mathbb{Z}} \arrow[u, hook] \arrow[r, phantom, "="] & \widehat{\mathbb{Q}_p^\times} \arrow[uu, hook]
\end{tikzcd}$$

$I(p) = \mathbb{Z}_p^\times$

5.2. Hilbert class field

Def Let $U := \prod_{v \text{ nonarch}} \mathcal{O}_v^\times \times \prod_{v \text{ arch.}} K_v^\times \subseteq \mathbb{A}_K^\times$

The corr. field $K' := (K^{ab})^{\Theta_K(U)}$ is called the Hilbert class field of K.

Ex If $K = \mathbb{Q}$, then $K' = \mathbb{Q}$ because

$$\prod \mathbb{Z}_p^\times \times \mathbb{R}^\times \longrightarrow \prod{}' \mathbb{Q}_p^\times \times \mathbb{R}^\times / \mathbb{Q}^\times$$ is surjective.

Thm K' is the maximal abelian unram. ext. of K in which every arch place (real) splits completely (into real places).

Pf The field corr. to $U' \subseteq C_K$ is

- unramified at v if and only if $I(v) = \mathcal{O}_v^\times \subseteq U'$
- completely split at v if and only if $D(v) = K_v^\times \subseteq U'$.

□

Rmk Some people (e.g. Milne) call $\mathbb{C}/\mathbb{R}$ ramified so they can say "K' is the max. unram. ext of K". But others (e.g. Neukirch) call $\mathbb{C}/\mathbb{R}$ unramified!

Rmk $\mathbb{Q}$ has no unramified field extensions (not even nonabelian ones).

Pf $K|\mathbb{Q}$ unramified $\Longleftrightarrow$ $D := \mathrm{disc}(K) = \pm 1$

Assume $n := [K:\mathbb{Q}] \geq 2$.

Minkowski's theorem implies that there exists some $0 \neq a \in \mathcal{O}_K$ such that

$$|\mathrm{Nm}_{K|\mathbb{Q}}(a)| \leq \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{n/2} \cdot \sqrt{|D|}$$

$$= \frac{n!}{n^n} \cdot \left(\frac{4}{\pi}\right)^{n/2} < 1. \quad ↯ \qquad \square$$

Thm If K is a number field, then $\mathrm{Gal}(K'|K) \cong \mathcal{Cl}_K$.

Pf $$\mathrm{Gal}(K'|K) \cong (\mathbb{A}_K^\times / K^\times)/U = \mathbb{A}_K^\times / K^\times \Big(\prod_{v \text{ nonarch}} \mathcal{O}_v^\times \times \prod_{v \text{ arch}} K_v^\times\Big)$$

$$\underset{\boxed{\text{Thm in section 4.6}}}{\cong} \mathcal{Cl}_K. \qquad \square$$

Exe $K = \mathbb{Q}(\sqrt{-15}) \rightsquigarrow K' = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$

$$\mathcal{Cl}_K = \left\{\langle 1 \rangle, \left\langle \left(2, \frac{1+\sqrt{-15}}{2}\right)\right\rangle\right\} \cong \mathbb{Z}/2\mathbb{Z}$$

$$= \mathrm{Gal}(K'|K).$$

Rmk

$$\begin{tikzcd} \vdots \arrow[d, dash, "\mathrm{unram.}"', "Cl_{K''}"] & \vdots \\ K'' \arrow[d, dash, "\mathrm{unram.}"', "Cl_{K'}"] & \leftarrow \text{Hilbert class field of } K' \\ K' \arrow[d, dash, "\mathrm{unram.}"', "Cl_{K}"] & \\ K & \end{tikzcd}$$

Theorem (Golod-Shafarevich)

Sometimes, this tower is infinite ($Cl_{K'''\cdots'} \neq 1$ after every step).

Ex K imaginary quadratic extension of $\mathbb{Q}$ with disc(K) divisible by ≥ 6 different primenumbers.

Cor Sometimes, K has an infinite (nonabelian) unramified extension.

[Reference: Cassels-Fröhlich.]

Thm (Principal ideal theorem)

Let K be a number field. Then, every ideal of K becomes principal in K'.

In other words, $Cl_K \longrightarrow Cl_{K'}$ is trivial.

Ex $K = \mathbb{Q}(\sqrt{-15})$

$$\left(2, \frac{1+\sqrt{-15}}{2}\right) = \left(\frac{1+\sqrt{5}}{2}\right).$$

The thm follows from:

Prop 5 (Cofunctoriality)

For any fin. separable ext. $L|K$ of $\left\{\begin{matrix}\text{fin.}\\ \text{local}\\ \text{global}\end{matrix}\right\}$ fields,

we get a comm. diagram

$$\begin{tikzcd}
C_K \arrow[r, "\theta_K"] \arrow[d] & \mathrm{Gal}(K^{ab}|K) = G^{ab} \arrow[d, "V"] \\
C_L \arrow[r, "\theta_L"'] & \mathrm{Gal}(L^{ab}|L) = H^{ab}
\end{tikzcd}$$

where $V: G^{ab} \to H^{ab}$ is the transfer (Verlagerung) map defined as follows. $(G = \mathrm{Gal}(K^{sep}|K),\ H = \mathrm{Gal}(K^{sep}|L))$

Def Let G be a compact top. group and let $H \leq G$ be an open (index n) subgroup. Let $g_1, \dots, g_n \in G$ be representatives of the cosets in $H \backslash G$. Then, define $V : G^{ab} \longrightarrow H^{ab}$: For any $t \in G$, let $V(t) = \prod_{i=1}^{n} [h_i] \in H^{ab}$, where we write $g_i t = h_i g_{\pi(i)}$ with $h_i \in H$, $\pi \in S_n$ some permutation.

Rmk V is a continuous hom. and does not depend on the choice of $g_1, \dots, g_n$.

Pf of the principal ideal theorem

~~$G K'' \neq$~~

$$\begin{tikzcd}
K'' \arrow[d, dash, "Cl_{K'}"] \arrow[dd, bend left=60, "G"] \\
K' \arrow[d, dash, "Cl_K"] \\
K
\end{tikzcd}$$

K'' is a Galois extension of K (e.g. because $U' \subseteq \mathbb{A}_{K'}$ is invariant under the action of $Gal(K'|K)$, or because any $Gal(K'|K)$-conjugate of K'' is again an unram. abelian ext. of K' and therefore equal to K'').

$G := Gal(K''|K)$. $K''|K$ unram, $K'|K$ max. unram. ab. ext.

$K'|K$ is the max. abelian subext. of $K''|K$.

$\Rightarrow Gal(K''|K') = [G, G] \leq G$

$$\begin{tikzcd}
Cl_K \arrow[r, phantom, "\cong"] \arrow[d] & Gal(K'|K) \arrow[d, "V"] \\
Cl_{K'} \arrow[r, phantom, "\cong"] & Gal(K''|K')
\end{tikzcd}$$

The result follows from a theorem in group theory:

Thm Let G be any finite group and $H = [G,G] \subseteq G$. Then $V : G^{ab} \longrightarrow H^{ab}$ is the trivial map.

Pf Maybe later (reinterpreting V in terms of group homology). "$\square$"

Last time: Hilbert class field of a number field

<u>What about function fields K?</u>

- The image of $U = \prod_v \mathcal{O}_v^\times$ in $\mathbb{A}_K^\times / K^\times$ has ~~finite~~/infinite index in $\mathbb{A}_K^\times / K^\times$.

$$\boxed{\mathbb{A}_K^\times \Big/ \prod_v \mathcal{O}_v^\times \times K^\times \cong \Big({\prod_v}' \underbrace{K_v^\times / \mathcal{O}_v^\times}_{\mathbb{Z}} \Big) \Big/ K^\times}$$

It is contained in the kernel of the content map

$$c : \mathbb{A}_K^\times / K^\times \longrightarrow \mathbb{R}^{>0}, \qquad (x_v)_v \longmapsto \prod_v |x_v|_v$$

, which has infinite image.

- K has an infinite unramified abelian extension.

$\overline{\mathbb{F}}_q(T) \,|\, \mathbb{F}_q(T)$ is the max. (abelian) unram. ext.

Pf Unram.: Every irred. $f(T) \in \mathbb{F}_q[T]$ split into distinct (linear) factors over $\overline{\mathbb{F}}_q$.

Same for the place at ∞, replacing T by $\frac{1}{T}$.

Max. unram.: Assume $K \,|\, \overline{\mathbb{F}}_q(T)$ is a deg. n unram. ext.

$\rightsquigarrow$ proj. curves $C \longrightarrow \mathbb{P}^1_{\mathbb{F}_1}$ unram. covering of degree n

Riemann-Hurwitz: $\underset{2 \geq}{\chi(C)} = n \cdot \underbrace{\chi(\mathbb{P}^1)}_{2} = 2n$

$\Rightarrow n = 1 \Rightarrow K = \overline{\mathbb{F}}_q(T)$.

5.3. Kummer theory

Thm (Hilbert 90)

Let $L|K$ be a Galois ext. with $\mathrm{Gal}(L|K) \cong \mathbb{Z}/n\mathbb{Z}$ generated by σ. Let $a \in L^\times$. Then,

$$\mathrm{Nm}_{L|K}(a) = 1 \iff a = \frac{b}{\sigma(b)} \text{ for some } b \in L^\times.$$

Pf "$\Leftarrow$" clear

"$\Rightarrow$" Let $t \in L$

and $b = t + a\sigma(t) + a\sigma(a)\sigma(t) + \dots + a\sigma(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}(t)$

$$a\sigma(b) = a\sigma(t) + a\sigma(a)\sigma(t) + \dots + \dots + \underbrace{a\sigma(a)\cdots\sigma^{n-1}(a)}_{\mathrm{Nm}(a)=1}\underbrace{\sigma^n(t)}_{t}$$

$\Rightarrow a\sigma(b) = b.$

It remains to choose $t \in L$ so that $b \neq 0$.

But the function $L \longrightarrow L$

$$t \longmapsto t + a\sigma(t) + \dots + a\sigma(a)\cdots\sigma^{n-2}(a)\sigma^{n-1}(t)$$

is nonzero because the automorphisms $\mathrm{id}, \sigma, \dots, \sigma^{n-1}$ of L are linearly independent. □

Cor (Kummer theory)

Let K be a field containing n distinct n-th roots of unity (char $K \nmid n$ and $\zeta_n \in K$). Then, each Gal. ext. $L|K$ with $\mathrm{Gal}(L|K) \cong \mathbb{Z}/n\mathbb{Z}$ is of the form

$L = K(\sqrt[n]{c})$ for some $c \in K^\times$.

Ex If $\mathrm{char}(K) \neq 2$, the $\mathbb{Z}/2\mathbb{Z}$-ext. are of the form $K(\sqrt{c})$.

Pf $\mathrm{Nm}_{L|K}(\underset{\underset{K}{\cap}}{\zeta_n}) = \zeta_n^n = 1. \underset{H90}{\Rightarrow} \exists\, b \in L^\times : \zeta_n = \frac{b}{\sigma(b)}.$

$$\Rightarrow 1 = \zeta_n^n = \frac{b^n}{\sigma(b^n)} \Rightarrow \sigma(b^n) = b^n \Rightarrow c := b^n \in K^\times.$$

On the other hand $\sigma^i(b) = \frac{b}{\zeta_n^i} \neq b$ for $i = 1, \dots, n-1$.

$\Rightarrow L = K(b)$. □

5.4. Hilbert symbols

Def Let K be a local field (nonarch. or arch.) containing n distinct n-th roots of unity. For any $a, b \in K^\times$, define the Hilbert symbol $(a,b)_n \in \mu_n = \{1, \zeta_n, \dots, \zeta_n^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z}$ by

$$\underbrace{\theta_K(a)}_{\in \mathrm{Gal}(K^{ab}|K)}(\sqrt[n]{b}) = (a,b)_n \cdot \sqrt[n]{b}.$$

Rmk $(a,b)_n$ is indep. of the choice of $\sqrt[n]{b}$ because

$$\theta_K(a)(\zeta_n^i) = \zeta_n^i.$$

Ex $K = \mathbb{R}$, $n = 2 \rightsquigarrow (a,b)_2 = \begin{cases} +1, & a > 0 \text{ or } b > 0 \\ -1, & a < 0 \text{ and } b < 0 \end{cases}$

Ex $K = \mathbb{C}$, any $n \rightsquigarrow (a,b)_n = 1$.

Rmk $(a,b)_n$ is multiplicatively bilinear:

i) $(a_1a_2, b)_n = (a_1,b)_n \cdot (a_2, b)$

ii) $(a, b_1b_2)_n = (a,b_1)_n \cdot (a, b_2)$.

Pf Clear from def. □

Rmk $(a,b)_n$ only depends on a, b up to n-th powers in $K^\times$:

i) $(a, b^n)_n = 1$

ii) $(a^n, b)_n = 1$.

Pf $(a,b^n)_n = (a,b)_n^n = 1$

$(a^n,b)_n$ // □

Cor We get a bilinear pairing $(\cdot,\cdot)_n : K^\times/K^{\times n} \times K^\times/K^{\times n} \to \mu_n$.

Rmk $K^\times/K^{\times n}$ is a finite group.

Pf $K^\times \cong \mathcal{O}_K^\times \times \mathbb{Z} \Rightarrow K^\times/K^{\times n} \cong \mathcal{O}_K^\times/\mathcal{O}_K^{\times n} \times \mathbb{Z}/n\mathbb{Z}$

Let $t \in U_K^{(r)} = 1 + \mathfrak{p}_K^r$ for $r \geq 2v_K(n)+1$.

$f(X) := X^n - t$.

$v_K(f(1)) = v_K(1-t) \geq r$

$v_K(f'(1)) = v_K(n)$

Hensel (v2) $\Rightarrow$ $f(X)$ has a root in $\mathcal{O}_K^\times$.

$\Rightarrow U_K^{(r)} \subseteq \mathcal{O}_K^{\times n}$.

But $\mathcal{O}_K^\times / U_K^{(r)}$ is finite. □

Rmk $(a,b)_n = 1 \iff a \in Nm_{L|K}(L^\times)$ where $L = K(\sqrt[n]{b})$.

Pf $(a,b)_n = 1 \iff \theta_K(a)(\sqrt[n]{b}) = \sqrt[n]{b} \iff \theta_K(a)|_L = id_L$

$\iff a \in Nm_{L|K}(L^\times)$.

Prop 1 in section 5.1 : $K^\times / Nm_{L|K}(L^\times) \xrightarrow[\sim]{\theta_K} Gal(L|K)$

$\square$

Cor $(x^n - b, b)_n = 1$ $\forall x \in K,\ b \in K^\times$ with $x^n - b \neq 0$.

Pf Let $L = K(\sqrt[n]{b})$.

If $[L:K] = n$, then

$$Nm_{L|K}(X - \sqrt[n]{b}) = \prod_{i=0}^{n-1}(X - \underbrace{\zeta_n^i \sqrt[n]{b}}_{\text{the conj. of } \sqrt[n]{b}}) = X^n - b.$$

Let $M = K[T]/(T^n - b) = \underbrace{L \times \dots \times L}_{n/[L:K]}$.

$Nm_{M|K}(X - T) = X^n - b$.

Let $X - T = (\alpha_1, \dots, \alpha_r) \in L \times \dots \times L$.

Then, $Nm_{M|K}(X - T) = \prod_j Nm_{L|K}(\alpha_j) = Nm_{L|K}(\prod_j \alpha_j)$.

In other words, if $[L:K] = \frac{n}{r}$, $b = c^r$, then

$$Nm_{L|K}\left(\prod_{j=0}^{r-1}(X - \zeta_n^j \sqrt[n]{b})\right) = \prod_{j=0}^{r-1} \prod_{k=0}^{\frac{n}{r}-1} (X - \zeta_n^j \zeta_n^{rk} \sqrt[n]{b})$$

$$= \prod_{i=0}^{n}(X - \zeta_n^i \sqrt[n]{b}) = X^n - b.$$

$\square$

Cor i) $(a,1-a)_n = 1 \quad \forall a \neq 0,1$

ii) $(a,-a)_n = 1 \quad \forall a \neq 0$.

Pf i) $x=1,\ b=1-a$

ii) $x=0,\ b=-a$ □

Rmk The Hilbert symbol is skew-symmetric:

$$(a,b)_n = (b,a)_n^{-1}.$$

Pf

$$\begin{aligned}(a,b)_n\cdot(b,a)_n &= (a,-a)_n\cdot(a,b)_n\cdot(b,a)\cdot(b,-b)_n\\ &= (a,-ab)_n\cdot(b,-ab)_n\\ &= (ab,-ab)_n\\ &= 1.\end{aligned}$$

□

Surprising Cor

$$a\in \mathrm{Nm}_{K(\sqrt[n]{b})|K}\left(K(\sqrt[n]{b})^\times\right) \iff b\in \mathrm{Nm}_{K(\sqrt[n]{a})|K}\left(K(\sqrt[n]{a})^\times\right).$$

Rmk The Hilbert symbol $(\cdot,\cdot)_n : K^\times/K^{\times n}\times K^\times/K^{\times n}\to \mu_n$

is nondegenerate:

$$(a,b)_n = 1 \ \forall b\in K^\times \iff a\in K^{\times n}$$

$$\Updownarrow$$

$$(b,a)_n = 1 \ \forall b\in K^\times$$

Pf "$\Leftarrow$" clear

"$\Rightarrow$" Assume $a\notin K^{\times n}$. $\Rightarrow L = K(\sqrt[n]{a})\neq K$.

$\Rightarrow \theta_K(b)|_L \neq \mathrm{id}_L$ for some $b\in K^\times$

$\Rightarrow (b,a)_n \neq 1$ for some $b\in K^\times$. □

Cor Let $b_1, \dots, b_r \in K^\times$ be representatives of the elements of $K^\times / K^{\times n}$ (or of generators).

Let $L = K(\sqrt[n]{b_1}, \dots, \sqrt[n]{b_r}) = K(\sqrt[n]{K^\times})$ (This is the max. ab. ext. of K s.t. $\sigma^n = id$ $\forall \sigma \in Gal(L|K)$.)

Then, $Nm_{L|K}(L^\times) = K^{\times n}$.

Pf $$Gal(K^{ab}|L) = \bigcap_{i=1}^{r} Gal(K^{ab}|K(\sqrt[n]{b_i}))$$

$$\underset{\substack{\uparrow \\ \text{Prop 1}}}{\Rightarrow} Nm_{L|K}(L^\times) = \bigcap_i Nm_{K(\sqrt[n]{b_i})|K}(K(\sqrt[n]{b_i})^\times)$$

$$= \bigcap_i \{ a \in K^\times \mid (a, b_i) = 1 \}$$

$$\underset{\substack{\uparrow \\ \text{nondegeneracy}}}{=} K^{\times n}.$$

□

Thm Let K be a nonarch. with residue field $\mathbb{F}_q$. Assume char $\mathbb{F}_q \nmid n$. ($\Leftrightarrow \mathfrak{p}_K \nmid n$).

Then, $$(a,b)_n \equiv \left((-1)^{v_K(a) v_K(b)} \cdot \frac{b^{v_K(a)}}{a^{v_K(b)}} \right)^{\frac{q-1}{n}} \mod \mathfrak{p}_K.$$

Rmk Since $\zeta_n \in K$ and char $\mathbb{F}_q \nmid n$, $\mathbb{F}_q$ contains n distinct n-th roots of unity. $\Rightarrow n \mid q-1$.

The congruence mod $\mathfrak{p}_K$ therefore uniquely determines the n-th root of unity $(a,b) \in K^\times$.

Exe If $\mathfrak{p}_K \nmid n$ and $a, b \in \mathcal{O}_v^\times$, then $(a,b)_n = 1$.

Exe The Legendre symbol

$$(\pi, u)_n \equiv u^{\frac{q-1}{n}} \mod \mathfrak{p}_K \text{ for } u \in \mathcal{O}_K^\times, \ \pi \in \mathcal{O}_K \text{ any uniformizer.}$$

Rmk $(\pi, u)_n = 1 \iff (u \mod \mathfrak{p}_K) \in \mathbb{F}_q^{\times n}$.

Pf $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$. □

Pf of Thm

Both sides are bilinear and skew-symmetric.

$\Rightarrow$ It suffices to consider the following cases:

i) $a = \pi$, $b = -\pi$ for π any uniformizer

ii) $a = \pi$, $b \in \mathcal{O}_K^\times$ —"—

iii) $a \in \mathcal{O}_K^\times$, $b \in \mathcal{O}_K^\times$

In fact, ii) $\Rightarrow$ iii) by bilinearity ($\pi' = a\pi$ is also a uniformizer).

i) $(\pi, -\pi)_n = 1$ proved earlier

ii) Local-finite compatibility (uniformizer $\mapsto$ Frobenius)

$$\begin{tikzcd}
K^\times \arrow[r, hook, "\theta_K"] \arrow[d, two heads, "v_K"'] & \mathrm{Gal}(K^{ab}|K) \arrow[d, two heads] \\
\mathbb{Z} \arrow[r, hook, "\theta_{\mathbb{F}_q}"'] & \mathrm{Gal}(\overline{\mathbb{F}}_q|\mathbb{F}_q)
\end{tikzcd}$$

$$\begin{tikzcd}
\pi \arrow[d, mapsto] & \\
1 \arrow[r, mapsto] & \varphi_q
\end{tikzcd}$$

$$\begin{array}{l}
\theta_K(\pi)(\sqrt[n]{b}) \equiv (\pi, b)_n \cdot \sqrt[n]{b} \mod \mathfrak{p}_L. \\
\qquad \rotatebox{90}{$\equiv$} \\
\varphi_q(\sqrt[n]{b}) \equiv \sqrt[n]{b}^{\,q}
\end{array}$$

$$\Longrightarrow \quad (\pi, b)_n \equiv \sqrt[n]{b}^{\,q-1} \equiv b^{\frac{q-1}{n}}. \qquad \square$$

$$\uparrow$$

$$\boxed{b \in \mathcal{O}_K^\times \Rightarrow \sqrt[n]{b} \not\equiv 0}$$

What if $q_K \mid n$?

Eg $K = \mathbb{Q}_2$, $n = 2$

$$(2^s a, 2^t b)_2 = (-1)^{s\cdot\frac{b^2-1}{8} + t\cdot\frac{a^2-1}{8} + \frac{a-1}{2}\cdot\frac{b-1}{2}}$$

for $a, b \in \mathbb{Z}_2^\times$, $s, t \in \mathbb{Z}$.

5.5. Hilbert's reciprocity law

Def Let K be a global field containing n distinct n-th roots of unity. For any $a, b \in K^\times$ and any place v, $\left(\frac{a,b}{v}\right)_n := (\underset{\overset{\cap}{K_v^\times}}{a}, \underset{\overset{\cap}{K_v^\times}}{b})_n$ (the Hilbert symbol in K_v.)

Thm (Hilbert's reciprocity law)

$$\prod_v \left(\frac{a,b}{v}\right)_n = 1. \qquad \forall a, b \in K^\times.$$

Pf global-local compatibility

$$\begin{tikzcd}
\mathbb{A}_K^\times/K^\times \arrow[r, "\theta_K"] & \mathrm{Gal}(K^{ab}|K) \\
\mathbb{A}_K^\times \arrow[u, two heads] & \\
K_v^\times \arrow[u, hook] \arrow[uu, bend right] \arrow[r, "\theta_{K_v}"'] & \mathrm{Gal}(K_v^{ab}|K_v) \arrow[uu]
\end{tikzcd}$$

$$\Theta_K(\underset{\underset{\mathbb{A}_K^\times}{\cap}}{(x_v)_v}) \overset{\boxed{\Theta_K \text{ cont. hom.}}}{=} \prod_v \Theta_K((\dots,1,x_v,1,\dots))$$

$$= \prod_v \underbrace{\Theta_{K_v}(x_v)}_{\in Gal(K_v^{ab}|K_v) \hookrightarrow Gal(K^{ab}|K)} \in Gal(K^{ab}|K)$$

$\Rightarrow$ For any $a \in K^\times$: $\underset{\underset{id}{\|}}{\Theta_K(a)} = \prod_v \Theta_{K_v}(a)$ $\quad \boxed{K^\times \subseteq \ker(\Theta_K)}$

$$1 = \frac{\Theta_K(a)(\sqrt[n]{b})}{\sqrt[n]{b}} = \prod_v \frac{\Theta_{K_v}(a)(\sqrt[n]{b})}{\sqrt[n]{b}} = \prod_v \left(\frac{a,b}{v}\right)_n .$$

□

Rmk For $K = \mathbb{Q}$, $n = 2$, this implies the quadratic reciprocity law!

Rmk $\left(\frac{a,b}{v}\right)_n = 1$ for all but finitely many v.

Pf $\operatorname{char}(K) \nmid n$. $\Rightarrow$ $\operatorname{char}(\underset{\underset{\text{res. field}}{\uparrow}}{\kappa_v}) \nmid n$ for a.a. v.

$a, b \in K^\times \Rightarrow a, b \in \mathcal{O}_v^\times$ for a.a. v

$\Rightarrow \left(\frac{a,b}{v}\right)_n = 1$ for a.a. v.

□

Application

The equation $y^2+z^2=(3-x^2)(x^2-2)$ does not satisfy the Hasse principle over $\mathbb{Q}$. (It has sol. in $\mathbb{A}_\mathbb{Q}$, but not in $\mathbb{Q}$.)

Pf sol. in $\mathbb{R}$: $(\sqrt{2},0,0)$

sol. in $\mathbb{Z}_2$: $(0,1,\sqrt{-7})$

sol. in $\mathbb{Z}_p$ $(2\nmid p)$: $x=1 \rightsquigarrow y^2+z^2=-2$ has sol. mod p

Hensel $\Rightarrow$ sol. in $\mathbb{Z}_p$.

no sol. in $\mathbb{Q}$: Let $(x,y,z)\in\mathbb{Q}^3$ be a sol.

$$\underbrace{\left(\frac{3-x^2,-1}{v}\right)_2}_{\in\{\pm1\}}\cdot\underbrace{\left(\frac{x^2-2,-1}{v}\right)_2}_{\in\{\pm1\}}\underset{\uparrow\ \text{bilinearity}}{=}\left(\frac{y^2+z^2,-1}{v}\right)_2\underset{\uparrow\ y^2+z^2\in \mathrm{Nm}_{\mathbb{Q}_v(i)|\mathbb{Q}_v}(\mathbb{Q}_v(i)^\times)}{=}1$$

$$\Rightarrow a_v:=\left(\frac{3-x^2,-1}{v}\right)_2=\left(\frac{x^2-2,-1}{v}\right)_2.$$

$$\| $$

$$\left(\frac{\frac{3}{x^2}-1,-1}{v}\right)_2 \quad (\text{if } x\neq 0)$$

Hilbert's reciprocity law: $\prod_v a_v=1$.

Let's compute all a_v.

$v=\infty$: $a_\infty=\left(\frac{3-x^2,-1}{\infty}\right)_2=1 \Leftrightarrow 3-x^2>0$

$a_\infty=\left(\frac{x^2-2,-1}{\infty}\right)_2=1 \Leftrightarrow x^2-2>0$

Since $3-x^2$, x^2-2 can't both be <0, we have $a_\infty=\boxed{1}$.

v = p odd:

Case $v_p(x) \geq 0$:

$$\Rightarrow 3 - x^2 \in \mathbb{Z}_p^\times \quad \text{or} \quad x^2 - 2 \in \mathbb{Z}_p^\times$$

$$\Rightarrow a_v = \left(\frac{3-x^2, -1}{v}\right)_2 = 1 \quad \text{or} \; a_v \left(\frac{x^2-2, -1}{v}\right)_2 = 1$$

$$\Rightarrow a_v = \boxed{1} \, .$$

Case $v_p(x) < 0$:

$$\Rightarrow \frac{3}{x^2} - 1 \in \mathbb{Z}_p^\times$$

$$\Rightarrow a_v = \left(\frac{\frac{3}{x^2} - 1, -1}{v}\right)_2 = \boxed{1}$$

v = 2:

Case $v_2(x) > 0$: $3 - x^2 \equiv 3 \equiv -1 \mod 4$

$$\Rightarrow a_v = \left(\frac{3-x^2, -1}{2}\right)_2 = \boxed{-1}$$

Case $v_2(x) = 0$: $x^2 - 2 \equiv -1 \mod 4$

$$\Rightarrow a_v = \left(\frac{x^2-2, -1}{2}\right)_2 = \boxed{-1}$$

Case $v_2(x) < 0$: $\frac{3}{x^2} - 1 \equiv -1 \mod 4$

$$\Rightarrow a_v = \left(\frac{\frac{3}{x^2} - 1, -1}{2}\right)_2 = \boxed{-1}$$

$$\Rightarrow \prod_v a_v = -1 \, . \quad ↯ \qquad \square$$

⇝ More general: Brauer-Manin obstructions

5.6. Conductors

Def Let $U_v^{(0)} = \mathcal{O}_v^\times$, $U_v^{(n)} = 1 + \mathfrak{p}_v^n$ $(n \geq 1)$.

$$K_v^\times \supseteq U_v^{(0)} \supseteq U_v^{(n)} \supseteq \dots$$

The conductor of a fin. abelian ext. $L|K$ of number fields corresponding to an open subgroup $U \leq \mathbb{A}_K^\times / K^\times$ of finite index is the ideal $\prod_{\mathfrak{p}} \mathfrak{p}^{e_\mathfrak{p}} \subseteq \mathcal{O}_K$, where $e_\mathfrak{p}$ is the smallest nonneg. integer such that $U_\mathfrak{p}^{(e_\mathfrak{p})} \subseteq U$.

$$\Big(\prod_{\mathfrak{p}} U_\mathfrak{p}^{(e_\mathfrak{p})} \subseteq U \Big)$$

Ex The conductor of (any subfield of) the Hilbert class field is 1.

Ex The conductor of an abelian ext. of $\mathbb{Q}$ is (the ideal generated by) the smallest $n \geq 1$ s.t. $K \subseteq \mathbb{Q}(\zeta_n)$.

Pf $\mathbb{Q}(\zeta_n)$ is the subfield

$$\begin{tikzcd}
\{x \in \hat{\mathbb{Z}}^\times \mid x \equiv 1 \bmod n\} \arrow[r, phantom, "\subseteq"] \arrow[d, equal, "n = \prod_p p^{e_p}"] & \hat{\mathbb{Z}}^\times = \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)|\mathbb{Q}) \arrow[dd, "\theta_\mathbb{Q}", "\wr"'] \\
\{(x_p)_p \in \prod_p \mathbb{Z}_p^\times \mid x \equiv 1 \bmod p^{e_p}\ \forall p\} \arrow[d, equal] & \\
\prod_p U_p^{(e_p)} \arrow[r, phantom, "\subseteq"] & \mathbb{A}_\mathbb{Q}^\times / \mathbb{Q}^\times \cdot \mathbb{R}^{>0}.
\end{tikzcd}$$

Question How to compute the conductor of a fin. ab. ext?

Question For a local field K, what are the abelian ext. $L^{(0)} \subseteq L^{(1)} \subseteq L^{(2)} \subseteq \ldots$

corr. to $K^\times \supseteq U_K^{(0)} \supseteq U_K^{(1)} \supseteq U_K^{(2)} \supseteq \ldots$

Ex $U_K^{(0)} = \mathcal{O}_K^\times = I$ inertia group

$L^{(0)} =$ max. unram. ext. of K.

$\rightsquigarrow$ higher ram. groups.

6. Higher ramification groups

6.1. Lower numbering

Def Let $\mathcal{O}_K$ be a Dedekind dom., $L|K$ a finite Galois ext.

The s-th ramification group (in lower numbering) of of $\mathfrak{P}$ of L over a prime $\mathfrak{p}$ of K is

$$I_s(\mathfrak{P}|\mathfrak{p}) = \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) \mid \forall a \in \mathcal{O}_L : \sigma(a) \equiv a \bmod \mathfrak{P}^{s+1}\}$$

$$= \{\sigma \in D(\mathfrak{P}|\mathfrak{p}) \mid i_{L|K}(\sigma) \geq s+1\}$$

where $i_{L|K}(\sigma) := \min\{v_{\mathfrak{P}}(\sigma(a)-a) \mid a \in \mathcal{O}_L\}$.

Rmk It is often denoted by $G_s(\mathfrak{P}|\mathfrak{p})$.

If $L|K$ is an ext. of local fields, write $I_s(L|K)$.

Ex $I_0(\mathfrak{P}|\mathfrak{p}) = I(\mathfrak{P}|\mathfrak{p})$ inertia group

Note $I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$

and $I_s = 1$ for suff. large s.

~~$\mathbb{C}|\mathbb{R}$ ramified?~~

Def $\mathfrak{P}|\mathfrak{p}$ is unramified if $I_0(\mathfrak{P}|\mathfrak{p})=1$.

$\mathfrak{P}|\mathfrak{p}$ is tamely ramified if $I_1(\mathfrak{P}|\mathfrak{p})=1$.

Lemma $I_s(\mathfrak{P}|\mathfrak{p})$ is a normal subgroup of $D(\mathfrak{P}|\mathfrak{p})$.

Lemma If $F|K$ is a subext. of $L|K$, then

$$\begin{tikzcd} L \arrow[d, dash] & \mathfrak{P} \arrow[d, dash] \\ F \arrow[d, dash] & P \arrow[d, dash] \\ K & \mathfrak{p} \end{tikzcd}$$

$$I_s(\mathfrak{P}|P) = I_s(\mathfrak{P}|\mathfrak{p}) \cap \mathrm{Gal}(L|F).$$

Rmk If K is a global field, then

$$\mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}}) = D(\mathfrak{P}|\mathfrak{p})$$

$$I_s(L_{\mathfrak{P}}|K_{\mathfrak{p}}) = I_s(\mathfrak{P}|\mathfrak{p}) \qquad \forall s \geq 0.$$

$\Rightarrow$ "Often, we can reduce to ext. of local fields."

Rmk If $\mathcal{O}_L = \mathcal{O}_K[a_1, \ldots, a_t]$, it suffices to consider only $a = a_1, \ldots, a_t$ in the def. of I_s and $i_{L|K}$.

Lemma $L|K$ fin. gal. ext. of local fields

$$\begin{aligned} I_s(L|K) &= \{\sigma \in \underline{\underline{I}}(L|K) \mid \sigma(\pi_L) \equiv \pi_L \bmod \mathfrak{P}_L^{s+1}\} \\ &= \{\sigma \in I(L|K) \mid \frac{\sigma(\pi_L)}{\pi_L} \equiv 1 \bmod \mathfrak{P}_L^{s}\} \\ &= \{\sigma \in I(L|K) \mid \frac{\sigma(\pi_L)}{\pi_L} \in U_L^{(s)}\} \end{aligned}$$

and $i_{L|K}(\sigma) = v_L(\sigma(\pi_L) - \pi_L)$ if $\sigma \in \underline{\underline{I}}(L|K)$.

Pf Let $F = L^{I(L|K)} = L \cap K^{unram}$ be the max. unram. subext.

$$\Rightarrow I_s(L|K) = I_s(L|F) = \{\sigma \in \underbrace{Gal(L|F)}_{I(L|K)} \mid \sigma(\pi_L) \equiv \pi_L \bmod \mathfrak{p}_L^{s+1}\}$$

$\mathcal{O}_L = \mathcal{O}_F[\pi_L]$ according to a Thm. in section 1.6.

$$\begin{tikzcd} L \arrow[d, dash, "\text{tot. ram.}"] \\ F \arrow[d, dash, "\text{unram.}"] \\ K \end{tikzcd}$$

□

Cor We obtain injective group hom.

$$I_0/I_1 \hookrightarrow \mathcal{O}_L^\times/U_L^{(1)} \cong \kappa_L^\times$$
$$[x] \mapsto x \bmod \mathfrak{p}_L$$

$$I_s/I_{s+1} \hookrightarrow U_L^{(s)}/U_L^{(s+1)} \cong \kappa_L \quad \text{for } s \geq 1.$$

$$[\sigma] \longmapsto \left[\frac{\sigma(\pi_L)}{\pi_L}\right] \qquad [1+\pi_L^s y] \mapsto y \bmod \mathfrak{p}_L$$

depends on choice of π_L

indep. of choice of π_L.

Pf Well-def.: $\frac{\sigma(\pi_L)}{\pi_L} \in \mathcal{O}_L^\times$. If $\sigma \in I_s$, then $\frac{\sigma(\pi_L)}{\pi_L} \in U_L^{(s)}$.

Indep. of π_L: Let $\sigma \in I_s$, $\alpha \in \mathcal{O}_L^\times$, then $v_L(\sigma(\alpha)-\alpha) \geq s+1$, ~~so~~ $v_L\left(\frac{\sigma(\alpha)}{\alpha} - 1\right) \geq s+1$, so $\frac{\sigma(\alpha)}{\alpha} \in U_L^{(s+1)}$.

Hence, $\frac{\sigma(\pi_L)}{\pi_L} U_L^{(s+1)} = \frac{\sigma(\alpha\pi_L)}{\alpha\pi_L} U_L^{(s+1)}$.

Group hom. If $\sigma, \tau \in I_s$, then

$$\frac{\sigma\tau(\pi_L)}{\pi_L} \cdot U_L^{(s+1)} = \frac{\tau(\pi_L)}{\pi_L} \cdot \frac{\sigma(\tau(\pi_L))}{\tau(\pi_L)} \cdot U_L^{(s+1)}$$

$$= \frac{\tau(\pi_L)}{\pi_L} \cdot \frac{\sigma(\pi_L)}{\pi_L} \cdot U_L^{(s+1)}$$

($\tau(\pi_L)$ is also a uniformizer)

Injective: $\sigma \in I_{s+1} \Leftrightarrow \frac{\sigma(\pi_L)}{\pi_L} \in U_L^{(s+1)}$. $\square$

Summary Let $k_L = \mathbb{F}_{q^f}$, $k_K = \mathbb{F}_q$, $q = p^r$.

$$\mathrm{Gal}(L|K) = D \underset{\substack{\uparrow \\ \text{quot.} \\ \mathbb{Z}/f\mathbb{Z}}}{\supseteq} I = I_0 \underset{\substack{\uparrow \\ \text{quot.} \\ \subseteq k_L^\times \\ = \mathbb{Z}/(q^f-1)\mathbb{Z} \\ \text{(size coprime} \\ \text{to } p)}}{\supseteq} I_1 \underset{\substack{\nwarrow \\ \text{quot.} \\ \subseteq k_L \\ = (\mathbb{Z}/p\mathbb{Z})^{rf} \\ \text{(size power} \\ \text{of } p)}}{\supseteq} I_2 \underset{\nearrow}{\supseteq} \underset{\nearrow}{\cdots}$$

Cor $\mathrm{Gal}(L|K)$ is solvable

Cor $I_1(L|K)$ is the unique p-Sylow subgroup of $I(L|K)$.

all p-Sylow subgroups are conjugate, but $I_1(L|K)$ is normal

Cor $L|K$ is tamely ramified if and only if $p \nmid |I(L|K)|$.

Lemma If $L|K$ is abelian, we even get injective group hom.

$$I_0/I_1 \hookrightarrow k_{\underline{\underline{K}}}^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$$

$$I_s/I_{s+1} \hookrightarrow k_{\underline{\underline{K}}} \cong (\mathbb{Z}/p\mathbb{Z})^r \qquad \text{for } s \geq 1.$$

$(k_K = \mathbb{F}_q, \quad q = p^r)$.

Pf Let $\sigma \in I_s$, $x = \dfrac{\sigma(\pi_L)}{\pi_L} \in U_L^{(s)}/U_L^{(s+1)}$.

Let $\tilde{\varphi}_q \in Gal(L|K)$ be a lift of the Frob. aut. φ_q.

$$\tilde{\varphi}_q(x) = \frac{\tilde{\varphi}_q\,\sigma(\pi_L)}{\tilde{\varphi}_q(\pi_L)} \underset{\substack{Gal(L|K)\\ \text{abelian}}}{=} \frac{\sigma\,\tilde{\varphi}_q(\pi_L)}{\tilde{\varphi}_q(\pi_L)} \underset{\substack{\tilde{\varphi}_q(\pi_L)\\ \text{is also a}\\ \text{uniformizer}}}{=} \frac{\sigma(\pi_L)}{\pi_L} = x \mod U_L^{(s+1)}$$

Case $s=0$: $\varphi_q(x \mod \mathfrak{p}_L) = (\tilde{\varphi}_q(x) \mod \mathfrak{p}_L)$

$\Rightarrow (x \mod \mathfrak{p}_L) \in \mathbb{F}_q^\times = \kappa_K^\times$. ✓

Case $s \geq 1$: Write $x = 1+\pi_L^s y$.

$\Rightarrow \tilde{\varphi}_q(1+\pi_L^s y) = 1+\pi_L^s y \mod U_L^{(s+1)}$.

$\Rightarrow \tilde{\varphi}_q(\pi_L^s y) \equiv \pi_L^s y \mod \mathfrak{p}_L^{s+1}$.

$$\Rightarrow \frac{\tilde{\varphi}_q(\pi_L^s)}{\pi_L^s} \cdot \underset{\substack{|||\\ \varphi_q(y)=y^q}}{\tilde{\varphi}_q(y)} \equiv y \mod \mathfrak{p}_L.$$

This congruence has at most q sol. $y \in \kappa_L$.

$$\Rightarrow |\underset{\subseteq \kappa_L = \mathbb{F}_{q^f} = (\mathbb{Z}/p\mathbb{Z})^{fr}}{\text{im}} \text{ of } I_s/I_{s+1} \text{ in } \kappa_L| \leq q = p^r.$$

$\Rightarrow \text{im} \subseteq (\mathbb{Z}/p\mathbb{Z})^r \cong \mathbb{F}_q$. □

6.2. Discriminant formula

Thm $L|K$ fin. Gal. ext. of local fields

$$\Rightarrow v_K(\mathrm{disc}(L|K)) = f(L|K) \cdot \sum_{\mathrm{id} \neq \sigma \in \mathrm{Gal}(L|K)} i_{L|K}(\sigma)$$

$$= f(L|K) \cdot \sum_{s=0}^{\infty} \left(|I_s(L|K)| - 1 \right).$$

Lemma $L|K$ fin. ext. of local fields.

$\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some $\alpha \in \mathcal{O}_L$.

Pf Let $\mathbb{F}_{q^f} | \mathbb{F}_q$ be the res. field ext.

$\Rightarrow \mathbb{F}_{q^f} = \mathbb{F}_q(\zeta_{q^f-1})$.

Hensel $\Rightarrow \zeta_{q^f-1} \in \mathcal{O}_L$

Let $\alpha = \zeta_{q^f-1} + \pi_L$.

$$\Rightarrow \beta := \alpha^{q^f} - \alpha = \cancel{\zeta_{q^f-1}^{q^f}} + \pi_L^{q^f} - \cancel{\zeta_{q^f-1}} - \pi_L$$

$$\equiv -\pi_L \mod \mathfrak{p}_L^2.$$

$\Rightarrow v_L(\beta) = 1$. $\Rightarrow \beta$ is a uniformizer in L.

$\Rightarrow \mathcal{O}_K[\alpha]$ contains a uniformizer and a generator $(\alpha \bmod \mathfrak{p}_L) = \zeta_{q^f-1}$ of $\kappa_L | \kappa_K$.

$\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\alpha]$. □

Thm in section 1.6

Pf of Thm Let $\mathcal{O}_L = \mathcal{O}_K[\alpha]$.

$$\Rightarrow \operatorname{disc}(L|K) = \pm \prod_{\substack{\sigma,\tau \in \operatorname{Gal}(L|K)\\ \sigma \neq \tau}} (\sigma(\alpha) - \tau(\alpha))$$

$$= \pm \prod_{\sigma} \sigma\Big(\prod_{\tau \neq id} (\alpha - \tau(\alpha))\Big).$$

$$\Rightarrow v_K(\operatorname{disc}(L|K)) = \frac{1}{e(L|K)} v_L(\operatorname{disc}(L|K))$$

$$= \frac{[L:K]}{e(L|K)} \sum_{\tau \neq id} v_L(\alpha - \tau(\alpha))$$

$$= f(L|K) \cdot \sum_{\tau \neq id} i_{L|K}(\tau) \qquad \square$$

Ex If $L|K$ is tamely ramified $(I_1 = 1)$, then

$$v_K(\operatorname{disc}(L|K)) = f(L|K) \cdot (e(L|K) - 1) = [L:K] - f(L|K).$$

6.3. Examples

Some totally ramified extensions: $L \mid K$

Ex $\mathbb{Q}_p(\sqrt{p}) \mid \mathbb{Q}_p \qquad (p \neq 2)$

$\mathbb{Z}_p[\sqrt{p}] \mid \mathbb{Z}_p$

$Gal = \{id, \sigma\} = \mathbb{Z}/2$

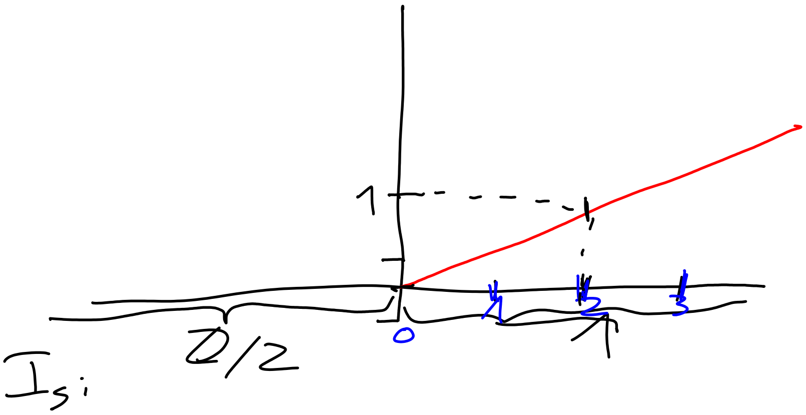
$$i(\sigma) = v_L(\underbrace{\sigma(\sqrt{p})}_{-\sqrt{p}} - \sqrt{p}) = v_L(-2\sqrt{p}) \overset{\text{tot. ram.}}{=} v_K(N_{L|K}(-2\sqrt{p})) = v_K(4p) = 1.$$

$I_0 = \mathbb{Z}/2 = I^0$

$I_1 = 1$

$I_2 = 1 \quad = I^1$

$\vdots$



Ex $\mathbb{Q}_2(\sqrt{p}) \mid \mathbb{Q}_2 \qquad (p \equiv 3 \bmod 4)$

$\mathbb{Z}_2[\sqrt{p}] \mid \mathbb{Z}_2$

$i(\sigma) = v_L(-2\sqrt{p}) = v_K(4p) = 2$

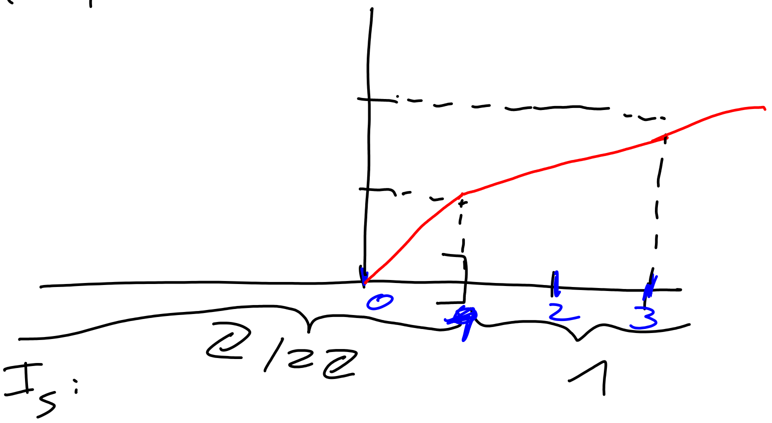
$I_0 = \mathbb{Z}/2 = I^0$

$I_1 = \mathbb{Z}/2 = I^1$

$I_2 = 1$

$I_3 = 1 \quad = I^2$

$\vdots$



Ex $\mathbb{Q}_2(\sqrt{2}) \mid \mathbb{Q}_2$

$\mathbb{Z}_2[\sqrt{2}] \mid \mathbb{Z}_2$

$i(\sigma) = v_K(8) = 3$

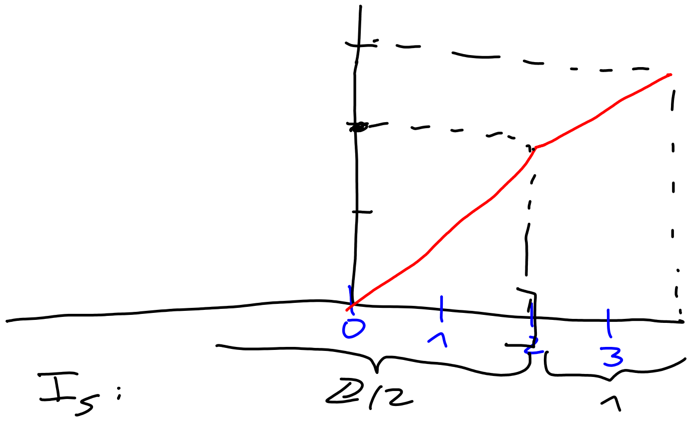
$I_0 = \mathbb{Z}/2 = I^0$

$I_1 = \mathbb{Z}/2 = I^1$

$I_2 = \mathbb{Z}/2 = I^2$

$I_3 = 1$

$\vdots$



Exe $K_n := \mathbb{Q}_p(\zeta_{p^n}) | \mathbb{Q}_p$ tot. ram. of degree $p^{n-1}(p-1) = \varphi(p^n)$.

$$\mathbb{Z}_p[\zeta_{p^n}] | \mathbb{Z}_p$$

$$\phi \longleftrightarrow r \bmod p^n$$

$$\begin{array}{ccc} \mathrm{Gal}(K_n | \mathbb{Q}_p) & = & (\mathbb{Z}/p^n\mathbb{Z})^\times \\ \cup\!| & & \cup\!| \\ \mathrm{Gal}(K_n | K_m) & = & \{ r \in (\mathbb{Z}/p^n\mathbb{Z})^\times \mid r \equiv 1 \bmod p^m \} \quad (m \leq n) \end{array}$$

$\zeta_{p^n} - 1$ is a uniformizer

Let $1 \neq r \in (\mathbb{Z}/p^n\mathbb{Z})^\times$.

$$i_{K_n|\mathbb{Q}_p}(\phi_r) = v_{K_n}\big(\phi_r(\zeta_{p^n}-1) - (\zeta_{p^n}-1)\big)$$

$$= v_{K_n}(\zeta_{p^n}^r - \zeta_{p^n})$$

$$\underset{\substack{\uparrow \\ \boxed{\zeta_{p^n} \in \mathcal{O}_{K_n}^\times}}}{=} v_{K_n}(\zeta_{p^n}^{r-1} - 1)$$

$$\underset{\substack{\uparrow \\ \boxed{\begin{array}{c} p^t = u(r-1), \\ u \in (\mathbb{Z}/p^n\mathbb{Z})^\times \end{array}}}}{=} v_{K_n}(\zeta_{p^n}^{p^t} - 1) \quad \text{if } t = v_p(r-1)$$

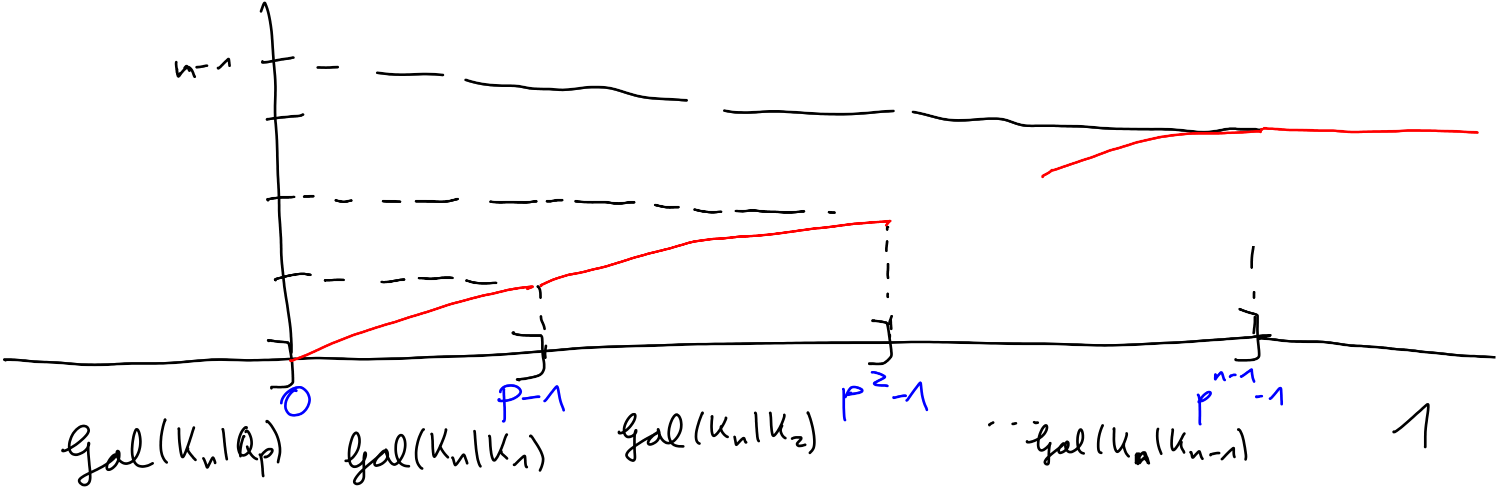
$= \text{largest } t \leq n$ s.t. $\phi_r \in \mathrm{Gal}(K_n|K_t)$

$$= v_{K_n}(\zeta_{p^{n-t}} - 1)$$

$$\underset{\substack{\uparrow \\ \boxed{\text{tot. ram.}}}}{=} \underbrace{[K_n : K_{n-t}]}_{p^t} \cdot \underbrace{v_{K_{n-t}}(\overbrace{\zeta_{p^{n-t}} - 1}^{\text{uniformizer in } K_{n-t}})}_{1}$$

$$= p^t$$

$\Rightarrow I_s(K_n|\mathbb{Q}_p) = \mathrm{Gal}(K_n|K_t)$, where t is the smallest $t \geq 0$ s.t. $s \leq p^t - 1$ or $t = n$.

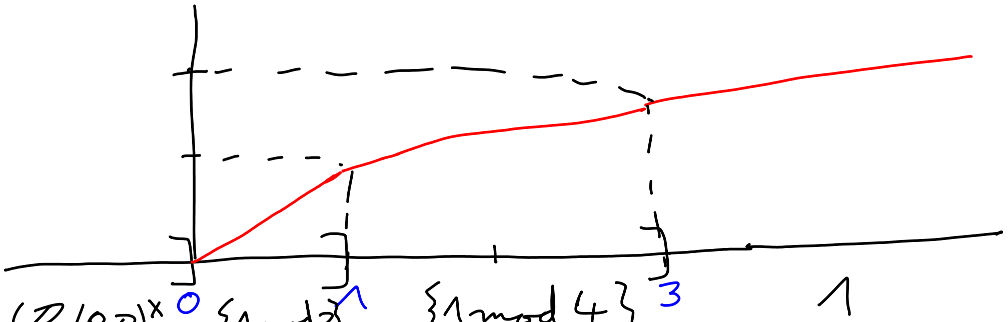


$I^t(K_n|\mathbb{Q}_p) = \mathrm{Gal}(K_n|K_t)$

Ex of Ex ($p^n = 8$)

$\mathbb{Q}_2(\sqrt{2}) = \mathbb{Q}_2(\zeta_8)^{\{\pm 1\}}$

$\boxed{\sqrt{2} = \zeta_8 + \zeta_8^{-1}}$



I_s: $(\mathbb{Z}/8\mathbb{Z})^\times = \{1 \bmod 2\}$ $\{1 \bmod 4\}$ 1

$I_s \bmod \{\pm 1\}$: $\underbrace{\qquad\qquad\qquad}_{\mathbb{Z}/2\mathbb{Z}}$ 1

$$\begin{tikzcd}
\mathbb{Q}_2(\zeta_8) \arrow[d, dash] \\
\mathbb{Q}_2(\sqrt{2}) \arrow[d, dash] \\
\mathbb{Q}_2
\end{tikzcd}$$

$I^0 = (\mathbb{Z}/8\mathbb{Z})^\times$ $\quad I^3 = 1$

$I^1 = (\mathbb{Z}/8\mathbb{Z})^\times$

$I^2 = \{1 \bmod 4\}$

6.4. Upper numbering

Def $\eta_{L|K}(s) := \int_0^s \frac{dx}{[I_0 : I_x]} = \frac{1}{|I_0|} \cdot \sum_{\sigma \in \mathrm{Gal}(L|K)} \min(\overbrace{i_{L|K}(\sigma), s+1}^{\mathbb{Z}}) - 1$

For $s = 0$: $i_{L|K}(\sigma) \geq 1 \iff \sigma \in I_0$

$\frac{d}{ds}$ agrees: $i_{L|K}(\sigma) \geq s+1 \iff \sigma \in I_s$

The <u>t-th ramification group (in upper numbering)</u> is $I^t(L|K) = I_{\eta_{L|K}^{-1}(t)}(L|K)$.

Thm (Herbrand)

If $F|K$ is a Galois subext., then $I^t(F|K)$ is the image of $I^t(L|K)$ under the restriction map $Gal(L|K) \twoheadrightarrow Gal(F|K)$.

$$\begin{tikzcd}
L \arrow[d, dash, "Gal."'] \arrow[dd, dash, bend left, "Gal."] \\
F \arrow[d, dash, "Gal"'] \\
K
\end{tikzcd}$$

Pf Neukirch, chapter II.10. □

Cor The following def. is consistent:

Def For any Gal. ext. $L|K$, let

$$I^t(L|K) = \{\sigma \in Gal(L|K) \mid \forall \underset{\substack{\cap\\ L}}{F}|K \text{ finite gal. ext.}: \sigma|_F \in I^t(L|K)\}.$$

Ex

$$\begin{array}{ccccc}
Gal(\mathbb{Q}_p(\zeta_\infty)|\mathbb{Q}_p) & \cong & \widehat{\mathbb{Q}_p^\times} \leftarrow \text{profinite completion} & \cong & \mathbb{Z}_p^\times \times \hat{\mathbb{Z}} \\
\rotatebox{90}{$\subseteq$} & & & & \rotatebox{90}{$\subseteq$} \\
Gal(\mathbb{Q}_p(\zeta_\infty)|\mathbb{Q}_p^{unram}(\zeta_{pt})) & \cong & U^{(t)}_{\mathbb{Q}_p} & & \\
\| & & & & \\
I^t(\mathbb{Q}_p(\zeta_\infty)|\mathbb{Q}_p) & & & &
\end{array}$$

$$\begin{array}{ccc}
I^0(\mathbb{Q}_p(\zeta_\infty)|\mathbb{Q}_p) & \cong & U^{(0)} = \mathbb{Z}_p^\times \\
\rotatebox{90}{$\subseteq$} & & \rotatebox{90}{$\subseteq$} \\
I^1(\mathbb{Q}_p(\zeta_\infty)|\mathbb{Q}_p) & \cong & U^{(1)} = 1 + p\mathbb{Z}_p \\
\rotatebox{90}{$\subseteq$} & & \rotatebox{90}{$\subseteq$} \\
I^2(\mathbb{Q}_p(\zeta_\infty)|\mathbb{Q}_p) & \cong & U^{(2)} = 1 + p^2\mathbb{Z}_p \\
\rotatebox{90}{$\subseteq$} & & \rotatebox{90}{$\subseteq$} \\
\ldots & & \ldots
\end{array}$$

6. 5. Abelian extensions

Thm (Hasse-Arf) If $L|K$ is abelian, then the "corners" of $\eta_{L|K}$ have integer coordinates.

In other words, $\forall t \in \mathbb{R}^{>0} \setminus \mathbb{Z} \; \exists \varepsilon > 0 : I^t(L|K) = I^{t+\varepsilon}(L|K)$

"I^t only changes at integers t."

Pf Serre, Local field, chapter V. □

Connection with CFT:

Property 6 of Artin reciprocity Let K be a local field.

Then, $U_K^{(t)} = \theta_K^{-1}(I^t(K^{ab}|K))$ for any $t \in \mathbb{Z}^{\geq 0}$.

$$\begin{tikzcd}
K^\times \arrow[r, "\theta_K"] & Gal(K^{ab}|K) \\
\cup & \cup \\
\mathcal{O}_K^\times = U_K^{(0)} \arrow[r] & I^0 \\
\cup & \cup \\
U_K^{(1)} \arrow[r] & I^1 \\
\cup & \cup \\
I_K^{(2)} \arrow[r] & I^2 \\
\cup & \cup \\
\vdots & \vdots
\end{tikzcd}$$

Cor $I^t(K^{ab}|K) / I^{t+1}(K^{ab}|K) \cong U_K^{(t)} / U_K^{(t+1)}$

$$\cong \begin{cases} k_K^\times, & t = 0 \\ k_K, & t \geq 1. \end{cases}$$

for any $t \in \mathbb{Z}^{\geq 0}$.

Rmk Hasse-Arf $\Longrightarrow$ Local Kronecker-Weber

Pf Let $K|\mathbb{Q}_p$ be a finite abelian ext.

Let $I^t(K|\mathbb{Q}_p)=1$.

Let $K' = K \cap \mathbb{Q}_p^{unram}$ $\left(\subseteq \mathbb{Q}_p(\zeta_\infty)\right)$.

$$\begin{tikzcd} K \arrow[d, dash, "\text{tot. ram.}"] \\ K' \arrow[d, dash, "\text{unram}"] \\ \mathbb{Q}_p \end{tikzcd}$$

Goal: $K \subseteq K'(\zeta_{p^t})$.

Recall that $I^t(\mathbb{Q}_p(\zeta_{p^t})|\mathbb{Q}_p)=1$.

$\rightsquigarrow$ W.l.o.g. $K \supseteq K'(\zeta_{p^t})$.

replace K by $K(\zeta_{p^t}) = K\cdot K'(\zeta_{p^t})$

$$[K:K'] = |I(K|\mathbb{Q}_p)| = |I^0/I^1(K|\mathbb{Q}_p)|\cdot|I^1/I^2|\cdots|I^{t-1}/I^t|$$

Lemma in 6.1

$$\begin{aligned}
&\leq |\mathbb{F}_p^\times|\cdot \quad |\mathbb{F}_p| \cdots |\mathbb{F}_p| \\
&= |I^0/I^1(\mathbb{Q}_p(\zeta_{p^t})|\mathbb{Q}_p)|\cdot|I^1/I^2|\cdots|I^{t-1}/I^t| \\
&= |I(\mathbb{Q}_p(\zeta_{p^t})|\mathbb{Q}_p)| \\
&\overset{K'|\mathbb{Q}_p \text{ unram!}}{=} |I(K'(\zeta_{p^t})|K')| \\
&= [K'(\zeta_{p^t}):K']
\end{aligned}$$

$$\Rightarrow K = K'(\zeta_{p^t}) \subseteq \mathbb{Q}_p(\zeta_\infty). \qquad \square$$

More generally:

<u>Thm</u> ~~Let~~ Let $K_0 \subseteq K_1 \subseteq K_2 \subseteq \dots$ be abelian ext. of a local field K with residue field $\mathbb{F}_q$ such that

$$K_0 = K^{unram}, \quad I^n(K_n|K)=1,$$

$$[K_{n+1}:K_n] = \begin{cases} q-1, & n=0 \\ q, & n\geq 1 \end{cases}.$$

Then, $K^{ab} = \bigcup_{n\geq 0} K_n$.

<u>Construction</u>

The following construction turns out to work:

Let $f(X)\in \mathcal{O}_K[X]$ be an Eisenstein polynomial of degree $q-1$ and let $e(X) = X\cdot f(X)$. Let

α_1 be a root of $f(X)$,

α_2 —"— $f(e(X))$,

α_3 —"— $f(e(e(X)))$,

$\vdots$

Let $K_{\pi,n} = K(\alpha_n)$ depends only on the uniformiser $\pi = f(0)$ and n, and we can take $K_n = K^{unram}\cdot K_{\pi,n}$
$= K^{unram}(\alpha_n)$.

$$\Rightarrow K^{ab} = \bigcup_{n\geq 0} K_n.$$

<u>Ex</u> If $K=\mathbb{Q}_p$ with $e(X) = \underset{X^p+pX^{p-1}+\dots+pX}{\underset{\parallel}{(X+1)^p-1}}$, we get $\alpha_n = \zeta_{p^n}-1$,

$K_{p,n} = \mathbb{Q}_p(\zeta_{p^n})$, $K_n = \mathbb{Q}_p^{unram}(\zeta_{p^n})$.

<u>Rmk</u> Hasse-Arf ⇒ Global Kronecker-Weber

<u>Pf</u> Let $K|\mathbb{Q}$ be a finite abelian ext.

Write $I^t(p) = I^t(\mathfrak{P}|p)$ for any prime $\mathfrak{P}|p$ of K.

(Independent of $\mathfrak{P}$ because $I^t(\sigma\mathfrak{P}|p) = \sigma I^t(\mathfrak{P}|p)\sigma^{-1}$ and $K|\mathbb{Q}$ is abelian.)

For any prime p, let $a_p \geq 0$ be minimal s.t. $I^{a_p}(p) = 1$.

In particular, $a_p = 0 \iff p$ unramified in K.

Goal: $K \subseteq \mathbb{Q}(\zeta_n)$, where $n = \prod_p p^{a_p}$.

W.l.o.g. $K \supseteq \mathbb{Q}(\zeta_n)$. (Replacing K by $K \cdot \mathbb{Q}(\zeta_n)$ and noting $I^{a_p}_{\mathbb{Q}(\zeta_n)}(p) = 1$.)

$\Rightarrow [K:\mathbb{Q}] \geq [\mathbb{Q}(\zeta_n):\mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$.

Look at the ext. $K_\mathfrak{P}|\mathbb{Q}_p$ of local fields.

Since $I^{a_p}(K_\mathfrak{P}|\mathbb{Q}_p) = 1$, we have

$$K_\mathfrak{P} \subseteq (\mathbb{Q}_p^{ab})^{I^{a_p}} = \mathbb{Q}_p^{unram}(\zeta_{p^{a_p}}).$$

$$\Rightarrow I(p) = I(\mathfrak{P}|p) = I(K_\mathfrak{P}|\mathbb{Q}_p) = I(\mathbb{Q}_p(\zeta_{p^{a_p}})|\mathbb{Q}_p) = (\mathbb{Z}/p^{a_p}\mathbb{Z})^\times.$$

$$\Rightarrow |I(p)| = |(\mathbb{Z}/p^{a_p}\mathbb{Z})^\times| \quad \forall p.$$

$$\Rightarrow |\underbrace{\text{subgr. of } \mathrm{Gal}(K|\mathbb{Q}) \text{ gen. by all } I(p)}_{= \mathrm{Gal}(K|\mathbb{Q}) \text{ by problem 1 on pset 7 (essentially because } \mathbb{Q} \text{ has no unram. ext.)}}| \leq \prod_p |(\mathbb{Z}/p^{a_p}\mathbb{Z})^\times| = |(\mathbb{Z}/n\mathbb{Z})^\times|.$$

$\Rightarrow [K:\mathbb{Q}] \leq |(\mathbb{Z}/n\mathbb{Z})^\times|$

$\Rightarrow K = \mathbb{Q}(\zeta_n)$. □

6.6. Tamely ramified extensions

We can extend the def. of "tamely ramified" to infinite ext.:

Def A Gal. ext. $L|K$ of (nonarch.) local fields is tamely ramified if $I^{\varepsilon}(L|K)=1$ $\forall \varepsilon>0$.

$$\begin{tikzcd}
L \arrow[dd, dash] \arrow[dr, dash, "\text{t.r.}"'] & \\
& F \arrow[dl, dash, "\text{t.r}"] \\
K &
\end{tikzcd}$$

Rmk Any Gal. ext. $L|K$ has a unique max. tamely ramified subext.: $L^{\bigcup_{\varepsilon>0} I^{\varepsilon}(L|K)}$

Thm The max. tamely ramified ext. of a local field K with residue field $\mathbb{F}_q$ is

$$K^{tame} = \bigcup_{\substack{m\geq 1\\ \gcd(m,q)=1}} K^{unram}(\pi_K^{1/m}) = \bigcup_{\substack{m\geq 1\\ \gcd(m,q)=1}} K(\zeta_m, \pi_K^{1/m})$$

$$= \bigcup_{t\geq 0} K(\zeta_{q^t-1}, \pi_K^{1/(q^t-1)}),$$

the splitting field of all polynomials $X^m-\pi_K$ with $\gcd(m,q)=1$.

Rmk For any $\alpha\in(K^{tame})^{\times}$, $m\geq 1$ s.t. $\gcd(m,q)=1$, $X^m-\alpha$ has m distinct roots in K^{tame}.

Pf HW. $\square$

Pf of Thm

$K^{tame}|K$ is tamely ramified

$$\begin{tikzcd}
K(\zeta_m, \pi_K^{1/m}) \arrow[d, dash, "\text{deg. } m \text{ (totally ram.)}"] \\
K(\zeta_m) \arrow[d, dash, "\text{unram.}"] \\
K
\end{tikzcd}$$

$\Big\}$ $e = m$ relatively prime to q

$\Rightarrow p \nmid e$

$\Rightarrow \quad I_1 = 1. \Rightarrow$ tamely ram.

$\uparrow$

I_1 is the p-Sylow subgroup of I

$L|K$ fin. tamely ram. ext. $\Rightarrow L \subseteq K^{tame}$

Let $L' = L \cap K^{unram}$.

$$\begin{tikzcd}
L \arrow[d, dash, "\text{tot. ram.}"] \\
L' \arrow[d, dash, "\text{unram.}"] \\
K
\end{tikzcd}$$

$\Rightarrow L = L'(\pi_L)$.

tamely ram. $\Rightarrow e(L|K) = e(L|L') = [L:L']$ relatively prime to q.

Let $f(X) = X^e + a_{e-1}X^{e-1} + \dots + a_0 \in L'[X]$ be the min. pol. of π_L over L'. It is an Eisenstein polynomial:

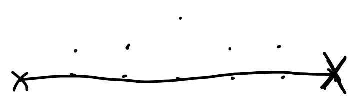
$$\begin{array}{ccccc}
v_{L'}(a_0) = 1, & & v_{L'}(a_1) \geq 1 & , \dots, & v_{L'}(a_{e-1}) \geq 1 \\
\boxed{L'|K \text{ unram.}} \longrightarrow \| & & \| & & \| \\
v_K(a_0) & & v_K(a_1) & & v_K(a_{e-1})
\end{array}$$

Problem: $f(X) \equiv X^e \mod \mathfrak{p}_{L'} \Rightarrow$ can't apply Hensel's lemma directly.

Solution: "Tilt" using the substitution $Y = \pi_K^{1/e} X$.

$$g(Y) := \pi_K^{-1} f(\pi_K^{1/e} X).$$

$g(Y)$:



$$g(Y) \equiv Y^e \quad + \underbrace{\frac{a_0}{\pi_K}}_{\not\equiv 0} \mod \mathfrak{p}_K$$

$g(Y)$ has e roots in the residue field $\mathbb{F}_q$ of $K^{unram} \subseteq K^{tame}$.

$$g'(Y) \equiv e Y^{e-1} \mod \mathfrak{p}_K$$

$$g'(\alpha) \equiv e\alpha^{e-1} \not\equiv 0 \mod \mathfrak{p}_K$$

$\Rightarrow g(Y)$ has e distinct roots mod $\mathfrak{p}_K$.

Hensel in fin. unram. ext. of K $\Rightarrow$ $g(Y)$ has e distinct roots in $\mathcal{O}_{K^{tame}}$.

$\Rightarrow \dfrac{\pi_L}{\pi_K^{1/e}} \in K^{tame} \Rightarrow \pi_L \in K^{tame}$

$\Rightarrow L \subseteq K^{tame}$. □

Thm Let $\tau(\pi_K^{1/m}) = \zeta_m \pi_K^{1/m}$, $\tau(\zeta_m) = \zeta_m$

$\Phi_q(\pi_K^{1/m}) = \pi_K^{1/m}$, $\Phi_q(\zeta_m) = \zeta_m^q$.

$$\begin{tikzcd} K(\zeta_m, \pi_K^{1/m}) \arrow[d, dash, "\langle\tau\rangle"'] \\ K(\zeta_m) \arrow[d, dash, "\langle\Phi_q\rangle"'] \\ K \end{tikzcd}$$

Then subgroup of $\mathrm{Gal}(K^{tame}|K)$ generated by τ, Φ_q is dense. It is a semidirect product $\underbrace{\langle\tau\rangle}_{\cong \mathbb{Z}} \rtimes \underbrace{\langle\Phi_q\rangle}_{\cong \mathbb{Z}}$ with $\Phi_q \tau \Phi_q^{-1} = \tau^q$.

Thm The max. tamely ramified abelian ext. of K is

$$K^{\text{tame, ab}} = K^{\text{unram}}\left(\pi_K^{1/(q-1)}\right),$$

$$\begin{aligned} \mathrm{Gal}(K^{\text{tame, ab}}) &\cong \mathbb{Z}/(q-1)\mathbb{Z} \rtimes \hat{\mathbb{Z}} \\ &= \mathbb{Z}/(q-1)\mathbb{Z} \times \hat{\mathbb{Z}} \end{aligned}$$

$$\left(\cong \mathcal{O}_K^\times / U_K^{(1)} \times \hat{\mathbb{Z}}\right.$$

$$\cong \widehat{K}^\times / U_K^{(1)}$$ as predicted by CFT.)

7. Lubin-Tate theory

How to prove that the construction of K^{ab} in 6.5 works?

Reminder: Why is $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$?

Any aut. of $\mathbb{Q}(\zeta_n)$ induces an aut. of the group ($\mathbb{Z}$-module) $\mathbb{Q}(\zeta_n)^\times \supseteq \langle \zeta_n \rangle \cong \mathbb{Z}/n\mathbb{Z}$ and the group aut. determines the aut. of $\mathbb{Q}(\zeta_n)$.

$$\Rightarrow Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \subseteq Aut_{\mathbb{Z}\text{-mod.}}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z}/n\mathbb{Z})^\times.$$

Try to generalize ...

- K = quadr. imag. number field

  Replace $\mathbb{Q}(\zeta_n)^\times$ by $E(L)$ for fin. ab. ext. $L|K$.

  $\langle \zeta_n \rangle \rightsquigarrow$ fin. subgr. ($\mathcal{O}_K$-modules)

  (<u>complex multiplication</u>)

- K nonarch. local field

  $\rightsquigarrow$ construct the group law using power series for the group operation

  (<u>Lubin-Tate theory</u>).

7.1. Formal groups

Def A formal group over a (comm.) ring R is a power series $F(X,Y) \in R[[X,Y]]$ such that:

i) $F(X,Y) = X+Y+(\text{deg.} \geq 2 \text{ terms})$ ($\approx$ addition close to 0)

ii) $F(X,Y) = F(Y,X)$ (commutative)

iii) $\underbrace{F(X,F(Y,Z))}_{\text{only makes sense because } F(0,0)=0} = F(F(X,Y),Z)$ (associative)

Exe $\mathbb{G}_a(X,Y) = X+Y$ (additive formal group)

Exe $\mathbb{G}_m(X,Y) = (X+1)(Y+1)-1 = X+Y+XY$ (multiplicative formal group)

so $\mathbb{G}_m(X-1,Y-1) = XY-1$. (moved the mult. id 1 to 0).

Rmk The axioms imply $F(X,0) = X$ (identity) and $\exists\, i(X) \in R[[X]]$: $i(X) = -X + (\text{deg.} \geq 2 \text{ terms})$, $F(X,i(X)) = 0$. (inverse).

Cor $F(X,Y) = X+Y+XY \cdot (\text{some power series in } X,Y)$.

Pf If $F(X,Y)-X-Y = (\text{deg.} \geq 2 \text{ terms})$ had a monomial of the form X^i or Y^i, then $F(X,0) \neq X$ or $F(0,Y) \neq Y$. $\square$

Def A hom. $f: F \to G$ of formal groups over R is a power series $f \in R[[X]]$ with $f(0)=0$ and $f(F(X,Y)) = G(f(X), f(Y))$.

Def lemma $\mathrm{End}_R(F) = \{ f: F \to F \text{ hom.} \}$ is a ring with

addition $(f+g)(X) = F(f(X), g(X))$. ⚠

multiplication $(f \circ g)(X) = f(g(X))$.

7.2. Formal modules

Def A formal R-module F is a formal group F over R together with a ring hom. $R \to \mathrm{End}_R(F)$

$$a \mapsto [a]_F(X)$$

satisfying

$$[a]_F(X) = aX + (\text{deg.} \geq 2) \quad \forall a \in R$$

($\approx$ mult. by a close to 0).

Def A hom. $f: F \to G$ of formal R-modules is a hom. of formal groups s.t.

$$f([a]_F(X)) = [a]_G(f(X)) \quad \forall a \in R.$$

Ex $[a]_{G_a}(X) = aX$ (trivial additive R-module).

7.3. Lubin-Tate modules

Let K be a nonarch. local field with res. field $\mathbb{F}_q$.

Def A Lubin-Tate series for a uniformizer π is a power series $e \in \mathcal{O}_K[[X]]$ s.t.

i) $e(X) = \pi X + (\deg. \geq 2)$

ii) $e(X) \equiv X^q \mod \mathfrak{p}_K$.

Ex $e(X) = X^q + \pi X$.

Ex $f(X) = X^{q-1} + \dots + \pi$ monic Eisenstein pol. of degree $q-1$.

$\Rightarrow e(X) = X \cdot f(X)$ is a L-T series for π.

Ex $K = \mathbb{Q}_p$, $\pi = p$

$\leadsto e(X) = (X+1)^p - 1 = X^p + pX^{p-1} + \dots + pX$.

Thm A Let $e(X)$ be a L-T series for π. There is a unique formal $\mathcal{O}_K$-module F_e (the Lubin-Tate module for e) s.t. $[\pi]_{F_e}(X) = e(X)$.

Ex $K = \mathbb{Q}_p$, $\pi = p$, $e(X) = (X+1)^p - 1$.

$\leadsto F_e(X,Y) = \mathbb{G}_m(X,Y) = (X+1)(Y+1) - 1$

$[a]_F(X) = (X+1)^a - 1 = \sum_{i=1}^{\infty} \binom{a}{i} X^i$ for $a \in \mathbb{Z}_p$

$$\left(\binom{a}{i} = \frac{a \cdots (a-i+1)}{i!} \right)$$

Thm B If $e(X), \tilde{e}(X)$ are L-T series for the same π, then $F_e, F_{\tilde{e}}$ are isomorphic formal $\mathcal{O}_K$-modules.

$\rightsquigarrow F_\pi := F_e$.

The Thm follows from the following Lemma.

Lemma Let $e(X), \tilde{e}(X)$ be L-T series for π and let $a_1, \dots, a_r \in \mathcal{O}_K$. Then, there is exactly one power series $\phi \in \mathcal{O}_K[[X_1, \dots, X_r]]$ s.t.

- $\phi(X_1, \dots, X_r) = a_1 X_1 + \dots + a_r X_r + (\deg. \geq 2)$
- $e(\phi(X_1, \dots, X_r)) = \phi(\tilde{e}(X_1), \dots, \tilde{e}(X_r))$.

Pf of Thm A using the lemma

There is a unique $F_e(X,Y) = X + Y + (\deg. \geq 2)$ s.t.
$$e(F_e(X,Y)) = F_e(e(X), e(Y)).$$

There is a unique $[a]_{F_e}(X) = aX + (\deg. \geq 2)$ s.t.
$$e([a]_{F_e}(X)) = [a]_{F_e}(e(X)).$$

We need to show:

$$F_e(X,Y) = F_e(Y,X)$$
$$F_e(X, F_e(Y,Z)) = F_e(F_e(X,Y), Z)$$
$$[a]_{F_e}(F_e(X,Y)) = F_e([a]_{F_e}(X), [a]_{F_e}(Y))$$
$$[a+b]_{F_e}(X) = F_e([a]_{F_e}(X), [b]_{F_e}(X))$$
$$[ab]_{F_e}(X) = [a]_{F_e}([b]_{F_e}(X))$$
$$[1]_{F_e}(X) = X$$
$$[\pi]_{F_e}(X) = e(X).$$

The statements follow from the uniqueness claim in the lemma. For example:

- $F_e(X, F_e(Y,Z))$ and $F_e(F_e(X,Y),Z)$ are both the power series $\phi(X,Y,Z) = X+Y+Z+(\deg.\geq 2)$ such that $e(\phi(X,Y,Z)) = \phi(e(X),e(Y),e(Z))$.

- $[a]_{F_e}(F_e(X,Y))$ and $F_e([a]_{F_e}(X),[a]_{F_e}(Y))$ are both the power series $\phi(X,Y) = aX+aY+(\deg.\geq 2)$ such that $e(\phi(X,Y)) = \phi(e(X),e(Y))$.

...

□

Pf of Thm B

similar. □

Pf of Lemma Write $X=(X_1,\dots,X_r)$, $e(X)=(e(X_1),\dots,e(X_r))$.

Write $\phi(X) = \phi_1(X)+\phi_2(X)+\dots$ with $\phi_n(X)\in\mathcal{O}_K[X]$ homogeneous of degree n. We inductively construct ϕ_n so that $e(\phi_1(X)+\dots+\phi_n(X)) = \phi_1(\tilde{e}(X))+\dots+\phi_n(\hat{e}(X))+(\deg.\geq n+1)$, starting with $\phi_1(X) = a_1X_1+\dots+a_rX_r$.

(Note that
$$\begin{aligned} e(\phi_1(X)) &\underset{i)}{=} \pi\,\phi_1(X)+(\deg.\geq 2 \text{ in } \phi_1(X)) \\ &= \pi(a_1X_1+\dots+a_rX_r)+(\deg.\geq 2) \\ &\underset{i)}{=} a_1\hat{e}(X_1)+\dots+a_r\hat{e}(X_r)+(\deg.\geq 2) \\ &= \phi_1(\tilde{e}(X))+(\deg.\geq 2).\,) \end{aligned}$$

Assume we have constructed $\phi_1,\dots,\phi_{n-1}$.

For any ϕ_n (hom. deg. n), we

$$e(\phi_1(X)+\dots+\phi_n(X)) \underset{i)}{=} e(\phi_1(X)+\dots+\phi_{n-1}(X)) + \pi\,\phi_n(X) + (\deg.\geq n+1)$$

$$\phi_1(\tilde{e}(X)) + \dots + \phi_n(\underbrace{\hat{e}(X)}_{\pi X + (\deg.\geq 2)}) = \phi_1(\tilde{e}(X)) + \dots + \phi_{n-1}(\tilde{e}(X)) + \pi^n \phi_n(X) + (\deg.\geq n+1)$$

This forces us to take $\phi_n :=$ hom. deg. n part of

$$\frac{e(\phi_1(X)+\dots+\phi_{n-1}(X)) - (\phi_1(\tilde{e}(X))+\dots+\phi_{n-1}(\hat{e}(X)))}{\pi^n-\pi}.$$

It remains to show that the coefficients lie in $\mathcal{O}_K$, in other words that the numerator is divisible by π. (Because $\pi^n-\pi$ is divisible by $\mathfrak{p}$ exactly once.)

But
$$\begin{aligned} e(\phi_1(X)+\dots+\phi_{n-1}(X)) &\underset{ii)}{\equiv} (\phi_1(X)+\dots+\phi_{n-1}(X))^q \\ &\equiv \phi_1(X)^q+\dots+\phi_{n-1}(X)^q \\ &\equiv \phi_1(X^q)+\dots+\phi_{n-1}(X^q) \\ &\underset{ii)}{\equiv} \phi_1(\tilde{e}(X))+\dots+\phi_{n-1}(\hat{e}(X)) \mod \mathfrak{p} \end{aligned}$$

$(\cdot)^q$ is a hom. mod $\mathfrak{p}$

$t\equiv t^q \mod \mathfrak{p}$ $\forall t\in\mathcal{O}_K$

□

7.4. Turning formal into ordinary groups/modules

Let K be a nonarch. local field.

If F is a formal group over $\mathcal{O}_K$, then for any $x, y \in \mathfrak{p}_K$,

$F(x,y) = x + y + (\text{deg.} \geq 2)$ converges in $\mathfrak{p}_K$.

$\rightsquigarrow$ We obtain a group operation $\underset{F}{+}$ on $\mathfrak{p}_K$ with the identity $0 \in \mathfrak{p}_K$. $\quad (x \underset{F}{+} y = F(x,y))$

If F is a formal $\mathcal{O}_K$-module, then for any $a \in \mathcal{O}_K$, $x \in \mathfrak{p}_K$,

$[a]_F(x) = ax + (\text{deg.} \geq 2)$ converges in $\mathfrak{p}_K$.

$\rightsquigarrow$ We obtain a scalar mult. operation $\underset{F}{\bullet}$ by el. of $\mathcal{O}_K$.

$(a \underset{F}{\bullet} x = [a]_F(x))$.

Similarly, formal hom. of formal groups/modules can be turned into actual (ordinary) hom. of ordinary groups/modules.

$\underline{\text{Ex}}$ $\quad x \underset{\mathbb{G}_a}{+} y = x + y \quad \rightsquigarrow$ group $(\mathfrak{p}_K, +)$

$a \underset{\mathbb{G}_a}{\bullet} x = ax$

$\underline{\text{Ex}}$ $\quad x \underset{\mathbb{G}_m}{+} y = (x+1)(y+1) - 1 \quad \rightsquigarrow$ group $\cong (\underset{\substack{\| \\ 1+\mathfrak{p}_K}}{U_K^{(1)}}, \cdot)$

In fact, the power series converge for any elements of $\mathfrak{p}_{\bar{K}}$.

(Reduce to finite extensions of K, which are all complete.)

7.5. Torsion

Choose a uniformizer and let F_π be the corresponding L-T module. (Determined by π up to isom. of formal $\mathcal{O}_K$-modules.)

Def Let $F_\pi(n) = \{\lambda \in \mathfrak{m}_{\overline{K}} \mid \underbrace{\pi^n \underset{F_\pi}{\cdot} \lambda}_{} = 0\}$

$$= \pi \underset{F}{\cdots} \pi \underset{F}{\cdot} \lambda = e^n(\lambda)$$

be the set of π^n-torsion elements for $n \geq 0$.

$$0 = F_\pi(0) \subseteq F_\pi(1) \subseteq F_\pi(2) \subseteq \dots$$

Let $F^1_\pi(n) = F_\pi(n) \setminus F_\pi(n-1)$ for $n \geq 1$.

Rmk $F_\pi(n) = "e^{-1}(F_\pi(n-1))"$, $F^1_\pi(n) = "e^{-1}(F^1_\pi(n-1))"$.

Ex $K = \mathbb{Q}_p$, $\pi = p$, $e(X) = (X+1)^p - 1$

$$\rightsquigarrow X \underset{F_\pi}{+} Y = (X+1)(Y+1) - 1$$

$$a \underset{F_\pi}{\cdot} X = (X+1)^a - 1$$

$$F_\pi(n) = \{\lambda \in \mathfrak{m}_{\overline{K}} \mid (\lambda+1)^{p^n} = 1\}$$

$$= \underset{\substack{\uparrow \\ p^n\text{-th roots of unity}}}{\mu_{p^n}} - 1$$

$$(F_\pi(n), \underset{F}{+}) \cong (\mu_{p^n}, \cdot) \text{ as groups}$$

$$F^1_\pi(n) = \underset{\substack{\uparrow \\ \text{primitive } p^n\text{-th roots of unity.}}}{\mu^1_{p^n}} - 1$$

__Lemma__ For any $n \geq 1$:

a) $|F^1_\pi(n)| = q^{n-1}(q-1)$

b) For any $\lambda_n \in F^1_\pi(n)$,

$K(\lambda_n)$ is a totally ramified separable degree $q^{n-1}(q-1)$ extension of K with uniformizer λ_n.

__Cor__ $|F_\pi(n)| = |F^1_\pi(n)| + |F^1_\pi(n-1)| + \dots + |F^1_\pi(1)| + |F_\pi(0)| = (q^{n-1}+\dots+1)(q-1)+1$
$= q^n$.

__Pf of Lemma__

Induction over n:

__$n=1$:__ $F^1_\pi(1) = \{ 0 \neq \lambda_1 \in \mathfrak{m}_{\bar{K}} \mid e(\lambda_1) = 0 \}$

$$\Updownarrow$$

$$\lambda_1^{q-1} + \pi = 0 \Leftrightarrow f(\lambda_1) = 0$$

$f(X) := X^{q-1} + \pi \in K[X]$ is an Eisenstein polynomial of degree $q-1$. $\Rightarrow$ For any root λ_1 of $f(X)$, the ext. $K(\lambda_1)|K$ is tot. ram. of degree $q-1$ with uniformizer λ_1. In particular, $\lambda_1 \in \mathfrak{m}_{\bar{K}}$, so $F^1_\pi(1)$ is the set of __all__ roots of $f(X)$.

$f'(X) = (q-1)X^{q-2}$ has no nonzero roots

$\Rightarrow f(X), f'(X)$ have no roots in common

$\Rightarrow f(X)$ is separable, has $q-1$ distinct roots

$\Rightarrow K(\lambda_1)|K$ is separable and $|F^1_\pi(1)| = q-1$.

__$n-1 \to n$:__ $F^1_\pi(n) = \{ \lambda_n \in \mathfrak{m}_{\bar{K}} \mid \underbrace{\lambda_{n-1} := e(\lambda_n) \in F^1_\pi(n-1)} \}$

$$\Updownarrow$$

$$\lambda_n^q + \pi\lambda_n = \lambda_{n-1} \Leftrightarrow f(\lambda_n) = 0.$$

Fix any $\lambda_{n-1} \in F^1_\pi(n-1)$.

$f(X) := X^q + \pi X - \lambda_{n-1} \in K(\lambda_{n-1})[X]$ is an Eisenstein polynomial of degree q.

$\Rightarrow$ For any root λ_n of $f(X)$, the ext. $K(\lambda_n)|K(\lambda_{n-1})$ is tot. ram. of degree q with uniformiser λ_n. In particular, $\lambda_n \in \mathfrak{m}_{\bar{K}}$, so $F'_\pi(n)$ is the set of <u>all</u> roots of $f(X)$.

Also, $K(\lambda_n)|K$ is by induction a tot. ram. ext. of degree $q \cdot q^{n-2}(q-1) = q^{n-1}(q-1)$.

$$f'(X) = q\,X^{q-1} + \pi$$

$$\Rightarrow q\,f(X) - X\,f'(X) = \underbrace{\pi(q-1)X - q\lambda_{n-1}}_{\underline{\text{linear}}\text{ pol. in } K(\lambda_1)[X]}.$$

$\Rightarrow$ All common roots of $f(X)$ and $f'(X)$ lie in $K(\lambda_{n-1})$.

But $f(X)$ has no roots in $K(\lambda_{n-1})$ because

$[K(\lambda_n) : K(\lambda_{n-1})] = q > 1$ for any root λ_n of $f(X)$.

$\Rightarrow$ $f(X)$ is separable, hence has q distinct roots.

$$\Rightarrow K(\lambda_n)|K(\lambda_{n-1}) \text{ separable}, \quad |F'_\pi(n)| = \underset{\text{(} q \text{ roots } \lambda_n \text{ of } f(X)\text{)}}{q} \cdot \underset{\text{(for each } \lambda_{n-1} \in F'_\pi(n-1)\text{)}}{q^{n-2}(q-1)}$$

$\Rightarrow$ $K(\lambda_n)|K$ separable by induction

□

Thm The $\mathcal{O}_K$- module $F_\pi(n)$ is isomorphic to $\mathcal{O}_K/\mathfrak{p}_K^n$.

Pf Let $\lambda_n \in F_\pi(n) \setminus F_\pi(n-1)$.

The kernel of the $\mathcal{O}_K$-mod. $\mathcal{O}_K \longrightarrow F_\pi(n)$

$$a \longmapsto a \cdot_{F_\pi} \lambda_n$$

is an ideal $\mathfrak{p}_K^m$ of $\mathcal{O}_K$. $(m \geq 0)$

The kernel contains π_K^r if and only if $\pi_K^r \cdot_{F_n} \lambda_n = 0$.

$$\Updownarrow$$

$$r \geq n$$

$\Rightarrow$ The kernel is $\mathfrak{p}_K^n$.

$\Rightarrow$ Injective hom. $\underbrace{\mathcal{O}_K/\mathfrak{p}_K^n}_{\text{size } q^n} \hookrightarrow \underbrace{F_\pi(n)}_{\text{size } q^n}$.

$\Rightarrow$ Surjective. $\square$

7.6. Maximal abelian extension

Def Let $K_{\pi,n} = K(F_\pi(n))$ be the smallest extension of K containing all elements of $F_\pi(n)$.

Rmk $K_{\pi,n}$ is independent of the choice of L-T series. (It might depend on the choice of π, though!)

Pf Let $e(X), \tilde{e}(X)$ be L-T series for π.

By Thm B from section 7.3, there are power series $f, f^{-1} \in \mathcal{O}_K[[X]]$ inducing an isomorphism

$$\begin{tikzcd} F_e \arrow[r, shift left, "f"] & F_{\tilde{e}} \arrow[l, shift left, "f^{-1}"] \end{tikzcd}$$

of formal $\mathcal{O}_K$-modules.

Let $\lambda \in F_e(n)$. $\Rightarrow f(\lambda) \in F_{\tilde{e}}(n)$.

$$\Rightarrow \lambda = \underset{\substack{\uparrow \\ \text{power series} \\ \text{with coeff. in } \mathcal{O}_K}}{f^{-1}}(f(\lambda)) \in K(F_{\tilde{e}}(n)).$$

$\Rightarrow K(F_e(n)) \subseteq K(F_{\tilde{e}}(n))$.

Similarly, ... ? ... . $\square$

Ex $K = \mathbb{Q}_p$, $\pi = p$ $\rightsquigarrow$ $K_{p,n} = \mathbb{Q}_p(\zeta_{p^n})$.

Thm a) $K_{\pi,n}|K$ is a totally ramified Galois ext. with

$$\mathrm{Gal}(K_{\pi,n}|K) \longrightarrow \mathrm{Aut}_{\mathcal{O}_K\text{-mod}}(\underbrace{F_\pi(n)}_{\mathcal{O}_K/\mathfrak{p}_K^n}) \cong (\mathcal{O}_K/\mathfrak{p}_K^n)^\times = \mathcal{O}_K^\times/U_K^{(n)}$$

$$\sigma \longmapsto \sigma|_{F_\pi(n)}$$

b) We have $K_{\pi,n} = K(\lambda_n)$ for any $\lambda_n \in F'_\pi(n)$.

Pf W.l.o.g. $e(X) = X^q + \pi X$.

$K_{\pi,n}$ is the splitting field of the degree q^n polynomial $e^n(X)$, which has q^n roots (all in $\mathfrak{p}_{\bar{K}}$) according to the Lemma in 6.5.

$\Rightarrow$ $K_{\pi,n}|K$ is Galois.

The map Gal $\to$ Aut is well-defined:

$\sigma|_{F_\pi}$ permutes el. of F_π $\left\{ \forall x \in F_\pi(n):\ e^n(x) = 0 \Rightarrow \sigma(\underset{\substack{\| \\ e^n(\sigma(x))}}{e^n(x)}) = 0 \Rightarrow \sigma(x) \in F_\pi(n) \right.$

$\sigma|_{F_\pi}$ hom. of $\mathcal{O}_K$-mod. $\left\{ \begin{array}{l} \forall x,y \in F_\pi(n):\ \sigma(F_\pi(x,y)) = F_\pi(\sigma(x),\sigma(y)) \text{ because } F_\pi \in \mathcal{O}_K[[X,Y]] \\ \forall a \in \mathcal{O}_K,\ x \in F_\pi(n):\ \sigma([a]_{F_\pi}(x)) = [a]_{F_\pi}(\sigma(x)) \text{ because } [a]_{F_\pi} \in \mathcal{O}_K[[X]] \end{array} \right.$

The map is injective because the elements of $F_\pi(n)$ generate $K_{\pi,n}$.

$$\Rightarrow [\underset{\substack{\text{IV} \\ [K(\lambda_n):K]}}{K_{\pi,n}} : K] = |\mathrm{Gal}| \leq |\mathrm{Aut}| = |(\mathcal{O}_K/\mathfrak{p}_K^n)^\times| = q^{n-1}(q-1)$$

$$[K(\lambda_n):K] \underset{\substack{\uparrow \\ \text{Lemma in 6.5.}}}{=} q^{n-1}(q-1)$$

$\Rightarrow$ $K_{\pi,n} = K(\lambda_n)$, which is tot. ram. of deg. $q^{n-1}(q-1)$, and the map is indeed an isomorphism. $\square$

Cor $K_\pi := \bigcup_{n\geq 0} K_{\pi,n}$ is a totally ramified Galois ext. of K with Galois group $\mathcal{O}_K^\times$.

Pf $$\mathrm{Gal}(K_\pi|K) = \varprojlim_{n\geq 0} \underbrace{\mathrm{Gal}(K_{\pi,n}|K)}_{(\mathcal{O}_K/\mathfrak{p}_K^n)^\times} ,$$

where the restriction map $\mathrm{Gal}(K_{\pi,n}|K) \twoheadrightarrow \mathrm{Gal}(K_{\pi,m}|K)$ $(n\geq m)$ is the quotient map $(\mathcal{O}_K/\mathfrak{p}_K^n)^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{p}_K^m)^\times$.

□

Thm
$$\begin{array}{ccc}
I^t(K_{\pi,n}|K) & = & \mathrm{Gal}(K_{\pi,n}|K_{\pi,t}) \\
\cap & & \| \\
\mathrm{Gal}(K_{\pi,n}|K) & & \\
\| & & \\
\mathcal{O}_K^\times/U_K^{(n)} & \supseteq & U_K^{(t)}/U_K^{(n)}
\end{array} \qquad \forall t\leq n$$

$$\begin{array}{ccc}
I^t(K_\pi|K) & = & \mathrm{Gal}(K_\pi|K_{\pi,t}) \\
\cap & & \| \\
\mathcal{O}_K^\times & \supseteq & U_K^{(t)}
\end{array} \qquad \forall t\geq 0$$

Pf Let $\underset{\mathrm{id}}{\overset{}{\sigma}}$ $\sigma \neq \mathrm{id}$ $\in \mathrm{Gal}(K_{\pi,n}|K)$ corr. to $a \in \mathcal{O}_K^\times/U_K^{(n)}$

(so $\sigma(\lambda_n) = a \underset{F_\pi}{\cdot} \lambda_n$).

Goal: $\underset{\text{compute}}{\wedge}$ $i_{K_{\pi,n}|K}(\sigma) = v_{K_{\pi,n}}(\sigma(\underset{\text{uniformizer}}{\underset{\uparrow}{\lambda_n}}) - \lambda_n)$

$= v_{K_{\pi,n}}(a \underset{F}{\cdot} \lambda_n - \lambda_n)$.

If $a \in U_K^{(1)}$, then

$i_{K_{\pi,n}|K}(\sigma) = 1$ because

$$a \underset{F}{\cdot} \lambda_n - \lambda_n = a\lambda_n - \lambda_n + (\text{deg.} \geq 2 \text{ terms in } \lambda_n)$$

$$\equiv \underbrace{(a-1)}_{\not\equiv 0 \bmod \lambda_n} \lambda_n \mod \lambda_n^2 .$$

If $a \in U_K^{(t)} \setminus U_K^{(t+1)}$, say $a = 1 + b \cdot \pi_K^t$, $b \in \mathcal{O}_K^\times$,

then $i_{K_{\pi,n}|K}(\sigma) = q^t$ because

$$a \underset{F}{\cdot} \lambda_n - \lambda_n = \lambda_n \underset{F}{+} \underbrace{(a-1)}_{b \cdot \pi_K^t} \underset{F}{\cdot} \lambda_n - \lambda_n$$

$$= \underbrace{\lambda_n \underset{F}{+} b \underset{F}{\cdot} \underbrace{e^t(\lambda_n)}_{\lambda_{n-t} \in F_\pi(n-t) \setminus F_\pi(n-t-1)}}_{\lambda'_{n-t} \in F_\pi(n-t) \setminus F_\pi(n-t-1)} - \lambda_n$$

Cor in 7.1

$$\equiv \cancel{\lambda_n} + \lambda'_{n-t} - \cancel{\lambda_n}$$

$$+ \lambda_n \cdot \lambda'_{n-t} \cdot (\text{power series in } \lambda_n, \lambda'_{n-t} \text{ with coefficients in } \mathcal{O}_K)$$

so $v_{K_{\pi,n}}(a \underset{F}{\cdot} \lambda_n - \lambda_n) = v_{K_{\pi,n}|K}(\lambda'_{n-t})$

$$= q^t \, v_{K_{\pi,n-t}}(\lambda'_{n-t}) = q^t .$$

Rest is exactly like for cyclotomic ext.

Cor The maximal abelian extension of K is

$$K^{ab} = K^{unram} \cdot K_\pi .$$

Pf See the Thm in 6.5. □

Rmk $Gal(K^{unram} \cdot K_\pi) = Gal(K^{unram}/K) \times Gal(K_\pi/K)$
$= \hat{\mathbb{Z}} \times \mathcal{O}_K^\times .$

Thm The map

$$K^\times = \mathbb{Z} \times \mathcal{O}_K^\times \longrightarrow \hat{\mathbb{Z}} \times \mathcal{O}_K^\times = Gal(K^{ab}/K)$$
$$a \cdot \pi^n \mapsto (n, a)$$

is independent of the choice of uniformiser.

Rmk It's the Artin reciprocity map.

Idea of pf If $e(X), \tilde{e}(X)$ are L-T series for $\pi, \tilde{\pi}$, then $F_e, F_{\tilde{e}}$ might not be isomorphic as formal $\mathcal{O}_K$-modules. But they become isomorphic over the completion of K^{unram}.

See Neukirch V, Thm 2.2, Cor. 2.3, Thm 5.5.

"□"

8. Group (co-)homology

8.1. G-modules

Def Let G be a finite group (written multiplicatively). A (left) G-module is an abelian group A (additively) with a left action of G on A s.t. $g(a+a') = ga + ga'$ $\forall g \in G, a, a' \in A$.

Rmk $g0 = 0$, $g(-a) = -ga$

Ex Any abelian group A with the trivial G-action: $ga = a$ $\forall g, a$.

(We equip $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, $\mathbb{Q}$ with the trivial G-action unless otherwise stated.)

Ex $L|K$ fin. Gal. ext., $G = \mathrm{Gal}(L|K)$

$\rightsquigarrow$ G-modules L, $L^\times$, $\mu_n(L^\times) = \{x \in L^\times \mid x^n = 1\}$

$\mathcal{O}_L | \mathcal{O}_K$ corr. ext. of Ded. dom. $\rightsquigarrow \mathcal{O}_L$, $\mathcal{O}_L^\times$

$L|K$ number fields $\rightsquigarrow J(L) = \{\text{frac. id. of } L\}$, $\mathcal{Cl}_L$

E elliptic curve over K $\rightsquigarrow E(L)$

⋮

Def A hom. of G-modules is a hom. $f: A \to B$ of groups s.t. $f(ga) = g f(a)$ $\forall g \in G, a \in A$.

Def Construct G-modules $A \times B$, A/B, ... (for $B \subseteq A$ any sub-G-module) in the obvious way.

Rmk A (left) G-mod. A is the same as a left $\mathbb{Z}[G]$-module, where $\mathbb{Z}[G]$ is the group ring of G: The ring of formal sums $\sum_{g\in G} a_g \cdot g$ with $a_g \in \mathbb{Z}$ $\forall g \in G$

$a_g = 0$ for $\underset{\uparrow}{a.a}$ $g \in G$.

(all but finitely many)

$$\sum_g a_g g + \sum_g b_g g = \sum_g (a_g + b_g) g$$

$$\left(\sum_g a_g g\right)\left(\sum_g b_g g\right) = \sum_{g,h} a_g b_h \, gh$$

$$= \sum_{i \in G} \underbrace{\left(\sum_{\substack{g,h\in G:\\ gh=i}} a_g b_h\right)}_{\in \mathbb{Z}} \cdot \underbrace{i}_{\in G}$$

We'll often consider the "norm element"

$$N = N_G = \sum_{g\in G} g \in \mathbb{Z}[G].$$

Def The group of invariants is

$$A^G = \{a \in A \mid ga = a \ \forall g \in G\}$$ (= biggest subgroup of A with trivial G-action).

The group of co-invariants is

$$A_G = A / \langle ga - a \mid g \in G, a \in A \rangle$$ (= biggest quotient group of A with trivial G-action).

Ex $\mathbb{Z}^G = \mathbb{Z}$, $\mathbb{Z}_G = \mathbb{Z}$, $N_G \cdot x = \sum_{g\in G} g\underbrace{x}_{} = |G|\cdot x$

$(x \in \mathbb{Z})$

$L^G = K$, $L_G \cong K$, $N_G \cdot x = \sum_{g\in G} gx = \mathrm{Tr}_{L|K}(x)$

by the normal basis theorem

$(x \in L)$

$(L^\times)^G = K^\times$, $N_G \cdot x = \prod_{g\in G} gx = \mathrm{Nm}_{L|K}(x)$

$(x \in L^\times)$

$J(L)^G \supseteq J(K)$

"$\neq$" iff $L|K$ is ramified at a prime

$\mathfrak{p} = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e$

$\Rightarrow \mathfrak{P}_1 \cdots \mathfrak{P}_r \in J(L)^G$
$\notin J(K)$

8.2. Motivation

Lemma If $0 \to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ is an exc. seq. of G-mod., we get exc. seq. $0 \to A^G \xrightarrow{i} B^G \xrightarrow{p} C^G$

and $A_G \xrightarrow{i} B_G \xrightarrow{p} C_G \to 0$

Pf straightforward. □

Ex $L|K$ gal. ext. of local fields (nonarchimedean)

$$1 \to \mathcal{O}_L^\times \to L^\times \xrightarrow{v_K} \tfrac{1}{e}\mathbb{Z} \to 0$$

$$1 \to \mathcal{O}_K^\times \to K^\times \xrightarrow{v_K} \tfrac{1}{e}\mathbb{Z}$$

surjective if and only if $e = 1$ ($L|K$ unramified)

Ex $G = \{e, \sigma\}$ cyclic group of order 2

$\tilde{\mathbb{Z}}$ = group $\mathbb{Z}$ with nontriv. G-action: $ex = x$, $\sigma x = -x$ $\forall x \in \mathbb{Z}$

triv. G-action because $1 = -1$ in $\mathbb{Z}/2\mathbb{Z}$

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

$$0 \to 0 \xrightarrow{\cdot 2} 0 \xrightarrow[\text{not surj.}]{} \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/2\mathbb{Z} \xrightarrow[\text{not inj.}]{\cdot 2} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

Questions

- How nonsurjective is $B^G \to C^G$?
- How to tell if a given element of C^G lies in the image of B^G?

Def Let $C^1(G,A) = \{(a_g)_{g\in G} \mid a_g \in A \; \forall g \in G\}$ (group of 1-cochains)

$\cup|$

$(*)$ $Z^1(G,A) = \{(a_g)_{g\in G} \mid a_{gh} = a_g + g a_h\}$ (group of 1-cocycles)

$gha - a = ga - a + g(ha - a)$

$\cup|$

$B^1(G,A) = \{(ga - a)_{g \in G} \mid a \in A\}$ (group of 1-coboundaries)

$H^1(G,A) = Z^1(G,A)/B^1(G,A)$ (first cohomology group)

Rmk (Functoriality in A)

Any hom. $A \to B$ of G-modules induces a hom. of $H^1(G,A) \to H^1(G,B)$ of groups.

($H^1(G, \cdot)$ is a functor $\{G\text{-mod.}\} \to \{\text{ab. gr.}\}$.)

Ex If G acts trivially on A, then

$$B^1(G,A)=0$$

$$\Rightarrow H^1(G,A)=Z^1(G,A)=\{(a_g)_{g\in G} \mid a_{gh}=a_g+\cancel{g}a_h \ \forall g,h\}$$

$$= \mathrm{Hom}_{group}(G,A)$$

$$\uparrow$$

$$\boxed{\begin{array}{l}(f_1+f_2)(g)=f_1(g)+f_2(g)\\ \text{for } f_1,f_2\in \mathrm{Hom}_{gr}(G,A)\end{array}}$$

Thm If $0\to A \xrightarrow{i} B \xrightarrow{p} C \to 0$ an ex. seq. of G-mod., we get an ex. seq. of groups

$$\begin{tikzcd}
0 \arrow[r] & A^G \arrow[r, "i"] & B^G \arrow[r, "p"] & C^G \arrow[dll, "\delta"'] \\
 & H^1(G,A) \arrow[r, "i"] & H^1(G,B) \arrow[r, "p"] & H^1(G,C)
\end{tikzcd}$$

Pf w.l.o.g. $A \underset{i}{\subseteq} B$ sub-G-module, $C \underset{p}{=} B/A$.

Def of δ: For any $c\in C^G$, choose $b\in B$ s.t. $(b \bmod A)=c$.

$$(gb-b \bmod A) = g(b \bmod A)-(b \bmod A)$$
$$= gc-c \underset{\substack{\uparrow\\ c\in C^G}}{=} 0 \qquad \forall g\in G.$$

$\Rightarrow gb-b\in A \ \forall g\in G$

$\Rightarrow (gb-b)_{g\in G}\in C^1(G,A)$

$\overset{(*)}{\Longrightarrow} (gb-b)_{g\in G}\in Z^1(G,A)$

b is unique mod A. $\Rightarrow (gb-b)_{g\in A}$ is unique mod $B^1(G,A)$.

$\rightsquigarrow \delta(c):=\left((gb-b)_{g\in G} \bmod B^1(G,A)\right)\in H^1(G,A)$

is a well-def. el. of $H^1(G,A)$ indep. of the choice of b.

δ hom.: clear

$b \in B^G \Rightarrow \delta(b \bmod A) = 0$: $\quad gb - b = 0 \ \forall g \in G$

$c \in C^G,\ \delta(c) = 0 \Rightarrow \exists\, b \in B^G : (b \bmod A) = c$:

$$\delta(c) = 0 \Rightarrow \exists\, b \in B : (b \bmod A) = c,\ (gb-b)_{g \in G} = 0$$

$$\Downarrow$$

$$b \in B^G$$

Rest is similarly easy diagram chasing... □

(This proof is the motivation for the def. of $H^1(G,A)$!)

Cor If $H^1(G,A) = 0$, then $B^G \to C^G$ is surjective.

$(0 \to A^G \to B^G \to C^G \to 0)$

depends only on A, not on B, C!

$c \in C^G \rightsquigarrow$ choose any b: $(b \bmod A) = c$

Q: $\exists\, a \in A$: $\underbrace{b + a \in B^G}$?

$$\forall g \in G : (gb - b) + (ga - a) = 0$$

$$\Updownarrow$$

$$(gb-b)_{g \in G} + (ga - a)_{g \in G} = 0$$

$\rightsquigarrow$ def. of 1-coboundaries

Def A free G-module is a free $\mathbb{Z}[G]$-module, i.e. $\bigoplus_{i\in I} \mathbb{Z}[G]$ for any set I.

A coinduced G-module is a module of the form

$$\mathrm{Hom}_{\text{group}}(\underset{\substack{\circlearrowleft \\ G}}{\mathbb{Z}[G]}, \underset{\substack{\uparrow \\ \text{gives group structure}}}{X}) \text{ for some abelian group } X.$$

$$\Vert$$

$$\underset{\text{(not necessarily hom.)}}{\{\text{map } G \to X\}} = \{(x_g)_{g\in G} \mid x_g \in X \ \forall g\}$$

$$= \Big\{ \sum_{g\in G} x_g g \;\Big|\; x_g \in X \ \forall g \Big\}$$

$$\Big(\text{action given by } h \sum_g x_g g = \sum_g x_g hg = \sum_g x_{h^{-1}g}\, g \Big)$$

An induced G-module is a module of the form

$$\underset{\substack{\circlearrowleft \\ G}}{\mathbb{Z}[G]} \otimes_{\mathbb{Z}} X \text{ for some abelian group } X.$$

$$\Vert$$

$$\{(x_g)_{g\in G} \mid x_g \in X \ \forall g,\ x_g = 0 \text{ for all but fin. many } g\}.$$

(same action as before)

Rmk For finite groups G, induced $=$ coinduced.

Ex $(\mathbb{Z}/2\mathbb{Z})[G]$ is an induced G-module, but not free.

8.3. Cohomology

[Reference: Milne's notes of CFT,
Neukirch's books on CFT, ...]

Thm/Def There is a unique family of *cohomology functors* $H^i(G,\cdot) : \{G\text{-mod.}\} \longrightarrow \{\text{ab. grp.}\}$ $(i\geq 1)$

satisfying the following axioms:

a) If $0\to A\to B\to C\to 0$ is an ex. seq. of G-mod., we obtain a long ex. seq.

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

b) If A is coinduced, then $H^i(G,A)=0$ $\forall i\geq 1$.

c) Any comm. diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

of short ex. seq. produces a comm. diagram of long ex. seq.

$$\begin{tikzcd}
0 \arrow[r] & A^G \arrow[r] \arrow[d] & B^G \arrow[r] \arrow[d] & C^G \arrow[r] \arrow[d] & H^1(G,A) \arrow[r] \arrow[d] & H^1(G,B) \arrow[r] \arrow[d] & \cdots \arrow[d] \\
0 \arrow[r] & A'^G \arrow[r] & B'^G \arrow[r] & C'^G \arrow[r] & H^1(G,A') \arrow[r] & H^1(G,B') \arrow[r] & \cdots
\end{tikzcd}$$

By convention, we set $H^0(G,A) = A^G$.

Sketch of pf

Uniqueness / construction 1

Consider the injective hom. of G-modules

$$\begin{aligned} A &\hookrightarrow \{\text{map } G \to A\} = A^* . \\ a &\longmapsto (g \mapsto g^{-1}a) \end{aligned}$$

We're ignoring the action of G on A, here!

It's a G-module hom.:

$$\begin{aligned} ha \longmapsto (g &\mapsto g^{-1}ha) \\ &= (hg \mapsto g^{-1}a) \\ &= h\cdot(g \mapsto g^{-1}a). \end{aligned}$$

The short exc. seq.

$$0 \to A \to A^* \to A^*/A \to 0$$

gives rise to

$$\begin{tikzcd} 0 \arrow[r] & A^G \arrow[r] & (A^*)^G \arrow[r] & (A^*/A)^G \arrow[dll] \\ & H^1(G,A) \arrow[r] & \underset{\overset{\| \, b)}{1}}{H^1(G,A^*)} \arrow[r] & H^1(G,A^*/A) \arrow[dll] \\ & H^2(G,A) \arrow[r] & \underset{\overset{\| \, b)}{1}}{H^2(G,A^*)} \arrow[r] & H^2(G,A^*/A) \arrow[dll] \\ & \cdots & & \end{tikzcd}$$

$\Rightarrow H^1(G,A) \cong \operatorname{coker}\left((A^*)^G \to (A^*/A)^G\right)$

$\Rightarrow H^1(G,A)$ uniquely determined $\forall A$.

$\Rightarrow H^2(G,A) \cong H^1(G,A^*/A)$

$\Rightarrow H^2(G,A)$ uniquely determined $\forall A$

$\vdots$

Axiom c) shows uniqueness for morphisms $H^i(G,A) \to H^i(G,B)$.

Construction 2

Choose a resolution of $\mathbb{Z}$ by free G-modules:

an ex. sequence

$$0 \leftarrow \mathbb{Z} \xleftarrow{d^0} P_0 \xleftarrow{d^1} P_1 \xleftarrow{d^2} P_2 \xleftarrow{d^3} \cdots$$

where each P_i is a free G-module.

The produces a cochain complex (composition of two consecutive maps is 0)

$$0 \xrightarrow{d^0} \mathrm{Hom}_G(P_0,A) \xrightarrow{d^1} \mathrm{Hom}_G(P_1,A) \xrightarrow{d^2} \mathrm{Hom}_G(P_2,A) \xrightarrow{d^3} \cdots$$

$$\begin{tikzcd} P_i \arrow[d, "f"'] & P_{i+1} \arrow[l, "d^{i+1}"'] \arrow[dl, dashed, "d^{i+1}(f)"] \\ A & \end{tikzcd}$$

It might not be exact, though!

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

Note: $H^0(G,A) = \ker(d^1) = \{ \underset{G\text{-mod.hom.}}{f : P_0 \to A} \mid f \circ d^1 = 0 \}$.

$$= \mathrm{Hom}_G(P_0/d^1(P_1), A)$$

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

$$f \longmapsto f(1)$$

$$(n \mapsto nx) \longleftarrow\!\!\shortmid \; x$$

Now, check the axioms:

b) Let A be coinduced:

$A = \{\text{map } G \to X\}$ for some ab. grp. X.

$$\mathrm{Hom}_G(P_i, A) = \mathrm{Hom}_{\text{group}}(P_i, X)$$

$$(p \mapsto a(p)) \longmapsto (p \mapsto a(p)(e))$$

$$(p \mapsto (g \mapsto x(g^{-1}p))) \longleftarrow\!\shortmid (p \mapsto x(p))$$

$$\begin{tikzcd}
\cdots & P_{i-1} \arrow[l] \arrow[rd, dashed, "g"'] & P_i \arrow[l, "d^i"'] \arrow[d, "f"'] & P_{i+1} \arrow[l, "d^{i+1}"'] \arrow[ld, "0"] \\
 & & X &
\end{tikzcd}$$

el. of $\ker(d^{i+1} : \mathrm{Hom}_G(P_i, A) \to \mathrm{Hom}_G(P_{i+1}$

Each P_i is a free $\mathbb{Z}[G]$-module and therefore a free $\mathbb{Z}$-module. $\Rightarrow \exists\, g$ s.t. $f = g \circ d^i$

$\Rightarrow f \in \mathrm{im}(d^i)$.

$\Rightarrow$ The cochain complex is exact.

$\Rightarrow H^i(G, A) = 0 \quad \forall i \geq 1$.

a) P_i free G-module: $P_i \cong \bigoplus_{i\in I} \mathbb{Z}(G)$

$\Rightarrow \mathrm{Hom}_G(P_i, A) \cong \prod_{i\in I} A$

$\Rightarrow$ If $0 \to A \to B \to C \to 0$ is an ex. seq. of G-mod.,

then

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_G(P_i, A) \arrow[r] \arrow[d, phantom, "\cong" rotate=90] & \mathrm{Hom}_G(P_i, B) \arrow[r] \arrow[d, phantom, "\cong" rotate=90] & \mathrm{Hom}_G(P_i, C) \arrow[r] \arrow[d, phantom, "\cong" rotate=90] & 0 \\
 & \prod_{i\in I} A & \prod_{i\in I} B & \prod_{i\in I} C &
\end{tikzcd}$$

is also an exact sequence.

Apply the snake lemma to

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_G(P_i, A) \arrow[r] \arrow[d] & \mathrm{Hom}_G(P_i, B) \arrow[r] \arrow[d] & \mathrm{Hom}_G(P_i, C) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Hom}_G(P_{i+1}, A) \arrow[r] & \mathrm{Hom}_G(P_{i+1}, B) \arrow[r] & \mathrm{Hom}_G(P_{i+1}, C) \arrow[r] & 0
\end{tikzcd}$$

This produces the long exact sequence . . .

"□"

8.4. Standard resolution

Here's a resolution of $\mathbb{Z}$ by free G-modules:

$$\begin{tikzcd}
0 & \mathbb{Z} \arrow[l] & \mathbb{Z}[G] \arrow[l, "d^0"'] \arrow[d, phantom, "\shortparallel"] & \mathbb{Z}[G^2] \arrow[l, "d^1"'] \arrow[d, phantom, "\shortparallel"] & \mathbb{Z}[G^3] \arrow[l, "d^2"'] \arrow[d, phantom, "\shortparallel"] & \cdots \arrow[l] \\
 & & P_0 & P_1 & P_2 &
\end{tikzcd}$$

Note: $P_i = \mathbb{Z}[G^{i+1}] = \Big\{ \sum_{g_0,\dots,g_i \in G} \underbrace{a_{g_0,\dots,g_i}}_{\in \mathbb{Z}} (g_0,\dots,g_i) \Big\}$

with G-action $g(g_0,\dots,g_i) = (gg_0,\dots,gg_i)$ is a free $\mathbb{Z}(G)$-module with $\mathbb{Z}[G]$-module basis

$\{(1, g_1,\dots,g_i) \mid g_1,\dots,g_i \in G\}$.

Rmk The P_i "correspond to" standard simplices in the definition of singular cohomology.

Let $d^i : P_i \longrightarrow P_{i-1}$

$$(g_0,\dots,g_i) \mapsto \sum_{j=0}^{i} (-1)^j \underset{\overset{\shortparallel}{(g_0,\dots,g_{j-1},g_{j+1},\dots,g_i)}}{(g_0,\dots,\hat{g}_j,\dots,g_i)}$$

It's easy to show $d^i \circ d^{i+1} = 0$ (so $\ker(d^i) \supseteq \operatorname{im}(d^{i+1})$).

To show $\ker(d^i) \subseteq \operatorname{im}(d^{i+1})$, use the chain homotopy maps $h^i : P_i \longrightarrow P_{i+1}$, $(g_0,\dots,g_i) \mapsto (1, g_0,\dots,g_i)$, which

satisfy $d^{i+1} \circ h^i + h^{i-1} \circ d^i = \mathrm{id}$.

If $a \in \ker(d^i)$, then

$$a = d^{i+1}(h^i(a)) + h^{i-1}(\underbrace{d^i(a)}_{0}) = d^{i+1}(h^i(a)) \in \operatorname{im}(d^{i+1}).$$

$$\begin{aligned}\tilde{C}^i(G,A) &:= \operatorname{Hom}_G(P_i, A) \\ &= \{ \underset{\text{map}}{\tilde{f} : G^{i+1} \to A} \mid \overset{\text{G-mod. hom. condition}}{\tilde{f}(gg_0,\dots,gg_i) = g\tilde{f}(g_0,\dots,g_i)} \\ &\qquad \forall g, g_0, \dots, g_i \in G \}\end{aligned}$$

(group of homogeneous i-cochains)

$d^i : \tilde{C}^{i-1}(G,A) \to \tilde{C}^i(G,A)$ is given by

$$(d^i \tilde{f})(g_0,\dots,g_i) = \sum_{j=0}^{i} (-1)^j \tilde{f}(g_0,\dots,\hat{g}_j,\dots,g_i).$$

$$\begin{array}{l} \tilde{C}^i(G,A) \\ \quad \rotatebox{90}{$\subseteq$} \\ \tilde{Z}^i(G,A) = \ker(d^{i+1}) \quad \text{(group of hom. } i\text{-cocycles)} \\ \quad \rotatebox{90}{$\subseteq$} \\ \tilde{B}^i(G,A) = \operatorname{im}(d^i) \quad \text{(group of hom. } i\text{-coboundaries)} \end{array}$$

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

In practice, inhomogeneous cochains tend to be more convenient:

$$C^i(G,A) := \{ (\underbrace{a_{g_1,\dots,g_i}}_{\in A})_{g_1,\dots,g_i \in G} \}$$

There's a group isomorphism

$$\tilde{C}^i(G,A) \cong C^i(G,A)$$
$$\tilde{f} \longleftrightarrow a$$

given by $a_{g_1,\dots,g_i} = \tilde{f}(1, g_1, g_1 g_2, \dots, g_1 \cdots g_i)$.

$$\begin{tikzcd}
0 \arrow[r] & \tilde{C}^0(G,A) \arrow[r, "d^1"'] \arrow[d, "\sim"] & \tilde{C}^1(G,A) \arrow[r, "d^2"'] \arrow[d, "\sim"] & \tilde{C}^2(G,A) \arrow[r, "d^3"'] \arrow[d, "\sim"] & \dots \\
0 \arrow[r] & C^0(G,A) \arrow[r] \arrow[d, phantom, sloped, "\cong"] & C^1(G,A) \arrow[r] & C^2(G,A) \arrow[r] & \dots \\
 & A & & &
\end{tikzcd}$$

$$d^1 : \overset{\overset{C^0(G,A)}{\parallel}}{A} \longrightarrow C^1(G,A)$$

$$a \longmapsto (ga - a)_{g \in G}$$

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

$$(a_g)_{g \in G} \mapsto (a_g + g a_h - a_{gh})_{g,h \in G}$$

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

$$(a_{g,h})_{g,h \in H} \mapsto (g a_{h,i} - a_{gh,i} + a_{g,hi} - a_{g,h})_{g,h,i \in G}$$

$$\vdots$$

$$C^i(G,A)$$

$$\cup\!|$$

$$Z^i(G,A) = \ker(d^{i+1}) \quad \underline{(\text{group of inhom. } i\text{-cocycles})}$$

$$\cup\!|$$

$$B^i(G,A) = \operatorname{im}(d^i) \quad \underline{(\text{group of inhom. } i\text{-coboundaries})}$$

$$H^i(G,A) = Z^i(G,A)/B^i(G,A)$$

$$\left.\begin{array}{l} \underline{\text{Ex}} \quad Z^0(G,A) = \{a \in A \mid \underset{\underset{ga=a}{\Updownarrow}}{ga - a = 0} \ \forall g \in G\} = A^G \\[2em] B^0(G,A) = 0 \end{array}\right\} \Rightarrow H^0(G,A) = A^G.$$

$$\left.\begin{array}{l} Z^1(G,A) = \{(a_g)_{g\in G} \mid a_{gh} = a_g + g a_h \ \forall g,h\} \\ B^1(G,A) = \{(ga-a)_{g\in G} \mid a \in A\} \end{array}\right\} \text{as before.}$$

8.5. Cyclic groups

Lemma Let $G \cong \mathbb{Z}/n\mathbb{Z}$ be generated by σ. Then,

$$\begin{tikzcd}
0 & \mathbb{Z} \arrow[l] & \mathbb{Z}[G] \arrow[l, "\varepsilon"'] & \mathbb{Z}[G] \arrow[l, "(\sigma-1)\cdot"'] & \mathbb{Z}[G] \arrow[l, "N_G\cdot"'] & \cdots \arrow[l, "(\sigma-1)\cdot"'] \\
 & \sum a_g & \sum_g a_g g \arrow[l, mapsto] & & &
\end{tikzcd}$$

$$(N_G = \sum_g g)$$

is a free resolution of G-modules.

Pf HW. $\square$

$$\begin{tikzcd}
\rightsquigarrow 0 \arrow[r] & \mathrm{Hom}_G(\mathbb{Z}[G], A) \arrow[r, "(\sigma-1)\cdot"] \arrow[d, equal, "\leftarrow \text{as groups}"] & \mathrm{Hom}_G(\mathbb{Z}[G], A) \arrow[r, "N_G\cdot"] \arrow[d, equal] & \mathrm{Hom}_G(\mathbb{Z}[G], A) \arrow[r, "(\sigma-1)\cdot"] \arrow[d, equal] & \cdots \\
 & A & A & A &
\end{tikzcd}$$

Cor $H^0(G,A) = \ker((\sigma-1)\cdot) = A^G$

$(\sigma-1)a = 0$
$\Leftrightarrow \sigma a = a$

map $A \xrightarrow{N_G} A$

$$H^1(G,A) = H^3(G,A) = \ldots = \ker(N_G\cdot)/\mathrm{im}((\sigma-1)\cdot) = \ker(N_G\cdot)/(\sigma-1)\cdot A$$

$$H^2(G,A) = H^4(G,A) = \ldots = \ker((\sigma-1)\cdot)/\mathrm{im}(N_G\cdot) = A^G/N_G\cdot A.$$

8.6. Examples

Ex Let $L|K$ be a Galois ext. with Galois group $G \cong \mathbb{Z}/n\mathbb{Z}$ gen. by σ.

a) $A = L^\times$

$\Rightarrow A^G = K^\times$

$\ker(N_G \cdot) = \{x \in L^\times : \mathrm{Nm}_{L|K}(x) = 1\}$

$\mathrm{im}((\sigma - 1)\cdot) = \{\frac{\sigma(y)}{y} \mid y \in L^\times\}$

$\Big\}$ Hilbert 90

$\mathrm{im}(N_G \cdot) = \mathrm{Nm}_{L|K}(L^\times)$.

$\Rightarrow H^0(G, L^\times) = K^\times$

$H^1(G, L^\times) = H^3(G, L^\times) = \ldots = 1$

$$H^2(G, L^\times) = H^4(G, L^\times) = \ldots = \underbrace{K^\times / \mathrm{Nm}_{L|K}(L^\times)}_{\text{We've encountered this in local CFT!}}.$$

b) $A = L$

$\Rightarrow A^G = K$

$\ker(N_G \cdot) = \{x \in L \mid \mathrm{Tr}_{L|K}(x) = 0\}$

$\mathrm{im}((\sigma - 1)\cdot) = \{\sigma(y) - y \mid y \in L\}$

$\Big\}$ Additive Hilbert 90

$\mathrm{im}(N_G \cdot) = \mathrm{Tr}_{L|K}(L) = K$

$\mathrm{Tr}_{L|K}(L) \neq 0$ by linear independence of the aut. of $L|K$

K-vector space contained in K

$\Rightarrow H^0(G, L) = K$

$H^1(G, L) = H^2(G, L) = \ldots = 0$

Thm ("Hilbert 90", Noether)

Let $L|K$ be any finite Galois ext. with Galois group G.

Then $H^1(G, L^\times) = 1$.

Pf Consider any 1-cocycle $(a_g)_{g\in G} \in Z^1(G, L^\times)$.

$\Rightarrow a_g \in L^\times \ \forall g \in G, \quad a_{gh} = a_g \cdot g(a_h) \ \forall g, h \in G.$

Let $t \in L$. Then, $b = \sum_{g\in G} a_g \, g(t) \in L$ satisfies

$$a_h h(b) = a_h \cdot \sum_g \underbrace{h(a_g g(t))}_{h(a_g)\cdot hg(t)} = \sum_g \underbrace{a_h h(a_g)}_{a_{hg}} \cdot hg(t)$$

$$= \sum_g a_{hg} \cdot hg(t) = \sum_g a_g \, g(t) = b \quad \forall h \in G.$$

Because the automorphisms $g \in G$ of $L|K$ are linearly independent, we can choose $t \in L$ so that $b \neq 0$, so $b \in L^\times$.

$$\Rightarrow a_g = \frac{g(b^{-1})}{b^{-1}} \quad \forall g \in G.$$

$\Rightarrow (a_g)_{g\in G}$ is a 1-coboundary $(\in B^1(G, L^\times))$.

$\Rightarrow Z^1(G, L^\times) = B^1(G, L^\times)$

$\Rightarrow H^1(G, L^\times) = 1.$ □

Normal basis theorem

Let $L|K$ be a fin. Gal. ext. with Galois group G.

Then, there is a normal basis of $L|K$: A basis of the form $(g(x))_{g\in G}$ for a fixed $x\in L$.

Cor $L \cong K[G]$ as left $K[G]$-modules.

(not as rings!!!)

~~$K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt[3]{2},\zeta_3)$ splitting field of X^3-1~~

Rmk If $(g(x))_{g\in G}$ is a basis, then $L=K(x)$.

Pf Since $g(x)\neq x$ for all $g\neq id$, the number x doesn't lie in any proper subfield of L (which would be fixed by all elements of a nontrivial subgroup of G). □

Cor L is a (co)induced G-module.

Cor of Cor $H^i(G,L)=0 \quad \forall i\geq 1$.

("Additive Hilbert 90")

Cor $L_G \xrightarrow[\mathrm{Tr}_{L|K}]{\sim} K$

Pf
$$L_G = L/\langle gx-x \mid g\in G, x\in L\rangle_{\mathbb{Z}}$$
$$\cong K[G]/\langle gx-x \mid g\in G, x\in K[G]\rangle_{\mathbb{Z}} \cong K$$
$$\sum_g a_g g \mapsto \sum a_g$$
□

Proof of the normal basis theorem assuming $|K|=\infty$.

Fix a basis $\omega_1,\dots,\omega_n$ of $L|K$. Let $G=\{g_1,\dots,g_n\}$.

Write $x=a_1\omega_1+\dots+a_n\omega_n$ with $a_1,\dots,a_n\in K$.

Let M be the $n\times n$-matrix sending the basis $(\omega_1,\dots,\omega_n)$ to $(g_1(x),\dots,g_n(x))$. $\left(g_j(x)=\sum_i a_i\, g_j(\omega_i).\right)$

Then, $(g(x))_{g\in G}$ is a basis of $L|K$ if and only if $f(a_1,\dots,a_n):=\det(M)\neq 0$.

Note that $f(X_1,\dots,X_n)$ is a polynomial (homogeneous of degree n).

Since $|K|=\infty$, if $f(a_1,\dots,a_n)=0$ $\forall a_1,\dots,a_n\in K$, then $f(X_1,\dots,X_n)=0$.

Since the automorphisms $g_1,\dots,g_n$ of $L|K$ are linearly independent, there exists $b_1,\dots,b_n\in L$ s.t. $\sum_{i=1}^n b_i\, g_j(\omega_i)=\omega_j$ $\forall j=1,\dots,n$.

$\Rightarrow f(b_1,\dots,b_n)=\det(I_n)=1\neq 0.$ □

8.7. Functoriality

"$H^n(G,A)$ is covariant in A and contravariant in G"

Def Let A be a G-module and A' be a G'-module. Homomorphisms $\mu : G' \longrightarrow G$ and $f : A \longrightarrow A'$ of groups are compatible (for cohomology) if

$$f(\mu(g')a) = g' f(a) \quad \forall g' \in G, a \in A.$$

We then obtain a homomorphism

$$\tilde{C}^n(G,A) \longrightarrow \tilde{C}^n(G',A')$$

$$\big(\underbrace{a_{g_0,\dots,g_n}}_{A}\big)_{g_0,\dots,g_n \in G} \longmapsto \big(\underbrace{f(a_{\mu(g'_0),\dots,\mu(g'_n)})}_{A'}\big)_{g'_0,\dots,g'_n \in G'}$$

which induces a homomorphism

$$H^n(G,A) \longrightarrow H^n(G',A').$$

Ex If $G = G'$, $\mu = id$, we get the usual hom.

$$H^n(G,A) \longrightarrow H^n(G,A').$$

Def For $H \subseteq G$ and any G-module A, the maps

$H \overset{\mu}{\hookrightarrow} G$, $A \xrightarrow{id} A$ induce the restriction hom.

$$\mathrm{Res} : H^n(G,A) \longrightarrow H^n(H,A).$$

Ex $(n=0)$: $\underset{H^0(G,A)}{\overset{\shortparallel}{A^G}} \hookrightarrow \underset{H^0(H,A)}{\overset{\shortparallel}{A^H}}$

Rmk A resolution $0 \leftarrow \mathbb{Z} \leftarrow P_0 \leftarrow P_1 \leftarrow \dots$ of $\mathbb{Z}$ by free G-mod. is a resolution by free H-mod. The inclusion $\mathrm{Hom}_G(P_n, A) \longrightarrow \mathrm{Hom}_H(P_n, A)$ induces the restriction hom. $H^n(G, A) \to H^n(H, A)$.

Def For $H \trianglelefteq G$ a normal subgroup and any G-module A, the maps $G \xrightarrow{\mu} G/H$, $\underset{\substack{\uparrow \\ G/H\text{-mod.}}}{A^H} \longrightarrow \underset{\substack{\uparrow \\ G\text{-mod.}}}{A}$

induce the inflation hom.

$$\mathrm{Inf} : H^n(G/H, A^H) \longrightarrow H^n(G, A).$$

Def For $H \leq G$ (of finite index) and any H-mod. A, then induced G-module is

$$\mathrm{Ind}_H^G A := \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A. \qquad (g(x \otimes a) = (gx) \otimes a)$$

(Note: $h(1 \otimes a) = h \otimes a = 1 \otimes ha$)

Rmk $\mathrm{Ind}_H^G A = \mathbb{Z}[G] \otimes_{\mathbb{Z}[H]} A \cong \{ \phi : G \to A \text{ map } \mid \phi(hg) = h\phi(g) \ \forall h \in H, g \in G \}$, (not nece. hom.)

$$\sum_{g \in H \backslash G} \underbrace{g^{-1} \otimes \phi(g)}_{= (hg)^{-1} \otimes \phi(hg) \ \forall h \in H}, \longleftarrow\!\mapsfrom \phi$$

Ex $\mathrm{Ind}_1^G A \cong \{ \phi : G \to A \text{ map} \}$ (not nec. hom.) (an induced G-module!)

Thm (Frobenius reciprocity)

For $H \leq G$ of finite index and any G-module A and H-module B,

$$\mathrm{Hom}_G(A, \mathrm{Ind}_H^G B) \cong \mathrm{Hom}_H(\underset{\uparrow}{A}, B).$$

only depends on action of H (not G) on A!

Pf $\quad a \mapsto (\underbrace{g \mapsto \phi(a)(g)}_{\phi(a)}) \longmapsto (a \mapsto \phi(a)(e))$

$\quad a \mapsto (g \mapsto f(ga)) \longleftarrow\!\!\shortmid f$

□

Rmk The functor $\mathrm{Ind}_H^G : \{H\text{-mod.}\} \longrightarrow \{G\text{-mod}\}$ is exact (sends short exact seq. of H-mod. to short exact seq. of G-mod.).

Thm (Shapiro's lemma)

Let $H \leq G$ of finite index and let A be an H-mod. Then, there is a (canonical) isomorphism

$$H^n(G, \mathrm{Ind}_H^G A) \cong H^n(H, A).$$

Pf Let $0 \leftarrow \mathbb{Z} \leftarrow P_0 \leftarrow P_1 \leftarrow \dots$ be a resolution by free G-modules. It's also a resolution by free H-modules (because $\mathbb{Z}[G] = \bigoplus_{g \in G/H} g\mathbb{Z}[H]$ is a free $\mathbb{Z}[H]$-module).

$$\mathrm{Hom}_G(P_i, \mathrm{Ind}_H^G A) \underset{\substack{\uparrow \\ \text{Frobenius reciprocity}}}{\cong} \mathrm{Hom}_H(P_i, A)$$

These $\underset{\substack{\uparrow \\ \text{(as constructed above)}}}{\text{isom.}}$ commute with the differential maps d^i.

□

Ex ($n = 0$) $\quad (\mathrm{Ind}_H^G A)^G \cong A^H.$

Def For $H \subseteq G$ of finite index and any G-module A,

the hom. $\mathrm{Ind}_H^G A \longrightarrow A$ of G-mod.
$$\underbrace{A}_{\text{depends only on } H\text{-action!}}$$
$$g \otimes a \longmapsto ga$$

induces a hom. $H^n(G, \mathrm{Ind}_H^G A) \longrightarrow H^n(G,A)$ of groups.

Then, the corestriction map is the composition

$$\mathrm{Cor}: H^n(H,A) \cong H^n(G, \mathrm{Ind}_H^G A) \longrightarrow H^n(G,A).$$

Ex Cor:
$$\begin{array}{ccc} H^0(H,A) & \longrightarrow & H^0(G,A) \\ \| & & \| \\ A^H & & A^G \\ a & \longmapsto & \displaystyle\sum_{g \in G/H} ga \end{array}$$

Thm $\mathrm{Cor} \circ \mathrm{Res}$ is the mult. by $[G:H]$ map.

$$H^n(G,A) \underset{\mathrm{Cor}}{\overset{\mathrm{Res}}{\rightleftarrows}} H^n(H,A).$$

Pf $\mathrm{Cor} \circ \mathrm{Res}$ is induced by

$$\mathrm{Hom}_G(P_i, A) \xrightarrow{\mathrm{Res}} \mathrm{Hom}_H(P_i, A) \cong \mathrm{Hom}_G(P_i, \mathrm{Ind}_H^G A) \longrightarrow \mathrm{Hom}_G(P_i, A)$$

$$f \mapsto f \mapsto \Big(p \mapsto \underbrace{\big(g \mapsto f(gp)\big)}_{= \sum_{g \in H\backslash G} g^{-1} \otimes f(gp)}\Big) \longmapsto \underbrace{\underbrace{\Big(p \mapsto \sum_{g \in H\backslash G} \underbrace{g^{-1} f(gp)}_{f(p) \text{ because } f \text{ is G-mod. hom.}}\Big)}_{[G:H] \cdot f(p)}}_{[G:H] \cdot f}$$

□

Rmk $$H^n(1, \underset{\substack{\uparrow \\ \text{any abelian group}}}{A}) = \begin{cases} A, & n=0 \\ 0, & n \geq 1 \end{cases}$$ (because A is a coinduced 1-module)

Cor If $|G| < \infty$, then $|G| \cdot H^n(G,A) = 0 \; \forall \, n \geq 1$.

Pf Apply the lemma with $H=1$:

$$\begin{tikzcd} H^n(G,A) \arrow[r, shift left, "\mathrm{Res}"] & H^n(1,A)=0 \arrow[l, shift left, "\mathrm{Cor}"] \end{tikzcd}$$ □

Cor If the mult. by $|G|$ map $A \to A$ is an isomorphism (e.g. $A = \mathbb{Q}$, or fin. ab. group of order coprime to $|G|$), then $H^n(G,A) = 0 \; \forall n \geq 1$.

Pf $A \xrightarrow{|G|\cdot} A$ isom.

$\Rightarrow H^n(G,A) \xrightarrow{|G|\cdot} H^n(G,A)$ isom. and zero (by prev. Cor.) □

Cor (If $|G|<\infty$, then) $H^n(G, \mathbb{Q}/\mathbb{Z}) \cong H^{n+1}(G, \mathbb{Z}) \quad \forall n \geq 1$.

Pf $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$

$$\cdots \to \overset{\overset{0}{\shortparallel}}{H^n(G,\mathbb{Q})} \to H^n(G,\mathbb{Q}/\mathbb{Z}) \to H^{n+1}(G,\mathbb{Z}) \to \underset{\underset{0}{\shortparallel}}{H^{n+1}(G,\mathbb{Q})} \to \cdots$$ □

Thm Let H be a normal subgroup of G and let A be a G-module. Let $n \geq 1$ such that $H^i(H,A) = 0$ for $i = 1, \dots, n-1$. Then, we obtain the <u>inflation-restriction exact sequence</u>

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

Pf Induction over n:

<u>$n=1$:</u>

$$\begin{tikzcd}[row sep=large]
0 \arrow[d] \\
H^1(G/H, A^H) = \left\{ \underset{\substack{\cap \\ A^H}}{(a_g)}_{g \in G/H} \;\middle|\; a_{g_1 g_2} = a_{g_1} + g_1 a_{g_2} \right\} \Big/ \left\{ (gb-b)_{g \in G/H} \;\middle|\; b \in A^H \right\} \arrow[d, "\mathrm{Inf}"] \\
H^1(G,A) = \left\{ \underset{\substack{\cap \\ A}}{(a_g)}_{g \in G} \;\middle|\; \dots \right\} \Big/ \left\{ (gb-b)_{g \in G} \;\middle|\; b \in A \right\} \arrow[d, "\mathrm{Res}"] \\
H^1(H,A) = \left\{ \underset{\substack{\cap \\ A}}{(a_g)}_{g \in H} \;\middle|\; \dots \right\} \Big/ \left\{ (gb-b)_{g \in H} \;\middle|\; b \in A \right\}
\end{tikzcd}$$

<u>Inf is injective:</u> Let $(a_g)_{g \in G/H} \in \ker(\mathrm{Inf})$.

$$\Rightarrow \exists\, b \in A : \forall g \in G : a_{gH} = gb - b$$

$$\Downarrow$$

$$\forall g \in H : \underset{\substack{\| \\ 0}}{a_H} = gb - b \Rightarrow b \in A^H$$

$$\Rightarrow (a_g) = 0 \text{ in } H^1(G/H, A^H).$$

...

<u>$n-1 \to n$</u>: Use construction 1 of cohom.

Let $A^* = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], A) = \{\text{maps } G \to A\}$
(coinduced),

$A \hookrightarrow A^*$ G-mod. hom. as before.

$a \mapsto (g \mapsto ga)$

$$0 \to A \to A^* \to A^*/A \to 0$$

$$\begin{tikzcd}
1 = H^k(G,A^*) \arrow[r] & H^k(G,A^*/A) \arrow[dll, out=0, in=180] & \\
H^{k+1}(G,A) \arrow[r] & H^{k+1}(G,A^*) = 1 &
\end{tikzcd}$$
$\forall k \geq 1$

$\Rightarrow H^k(G, A^*/A) \cong H^{k+1}(G,A) \quad \forall k \geq 1.$

(Same with G replaced by H ...)

$\Rightarrow H^i(H, A^*/A) = 0$ for $i = 1, \dots, n-2$ by assumption.

By induction,

$$\begin{tikzcd}
0 \arrow[r] & H^{n-1}(G/H, (A^*/A)^H) \arrow[r, "\mathrm{Inf}"] \arrow[d, phantom, sloped, "\cong"] & H^{n-1}(G, A^*/A) \arrow[r, "\mathrm{Res}"] \arrow[d, phantom, sloped, "\cong"] & H^{n-1}(H, A^*/A) \arrow[d, phantom, sloped, "\cong"] \\
0 \arrow[r] & H^n(G/H, A^H) \arrow[r, "\mathrm{Inf}"] & H^n(G, A) \arrow[r, "\mathrm{Res}"] & H^n(H, A)
\end{tikzcd}$$

$\Rightarrow$ bottom row exact. □

8.8. Cup products

Def Let M, N be G-modules and $r, s \geq 0$. Then,

$M \otimes_{\mathbb{Z}} N$ is also a G-module $(g(m \otimes n) = (gm \otimes gn))$.

Define the cup product

$$\cup: H^r(G, M) \times H^s(G, N) \longrightarrow H^{r+s}(G, M \otimes_{\mathbb{Z}} N)$$

by letting

$$(f_1 \cup f_2)(g_0, \dots, g_{r+s}) = \underbrace{f_1(g_0, \dots, g_r)}_{\in M} \otimes \underbrace{f_2(g_r, \dots, g_{r+s})}_{\in N}$$

for homogeneous cocycle $f_1 \in \tilde{C}^r(G, M)$, $f_2 \in \tilde{C}^s(G, N)$

$\left(\rightsquigarrow f_1 \cup f_2 \in \tilde{C}^{r+s}(G, M \otimes_{\mathbb{Z}} N) \right)$.

Ex $(r = s = 0)$

$$\cup: M^G \times N^G \longrightarrow (M \otimes_{\mathbb{Z}} N)^G$$

$$(m, n) \longmapsto m \otimes n$$

Rules $(x \cup y) \cup z = x \cup (y \cup z)$

$x \cup y = (-1)^{rs} \, y \cup x$ for $x \in H^r(G, M)$, $y \in H^s(G, N)$

(identifying $M \otimes N = N \otimes M$).

For $H \leq G$: $\mathrm{Res}_H(x \cup y) = \mathrm{Res}_H(x) \cup \mathrm{Res}_H(y)$

$\mathrm{Cor}(x \cup \mathrm{Res}(y)) = \mathrm{Cor}(x) \cup y$.

(Try this out with $M = \mathbb{Z}$, $r = 0$ ...)

8.9. Homology

Thm/Def There is a unique family of homology functors

$$H_i(G,\cdot) : \{G\text{-mod.}\} \longrightarrow \{\text{ab. grp.}\} \quad (i \geq 1)$$

satisfying the following axiom:

a) If $0 \to A \to B \to C \to 0$ is a short ex. seq. of G-modules, we obtain a long ex. seq.

$$\begin{tikzcd}
\cdots \arrow[r] & H_2(G,B) \arrow[r] & H_2(G,C) \arrow[dll, "\delta"] & \\
H_1(G,A) \arrow[r] & H_1(G,B) \arrow[r] & H_1(G,C) \arrow[dll, "\delta"] & \\
A_G \arrow[r] & B_G \arrow[r] & C_G \arrow[r] & 0
\end{tikzcd}$$

b) If A is an 'induced' G-module, then $H_i(G,A) = 1$ $\forall i \geq 1$.

c) A comm. diagram

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0
\end{tikzcd}$$

of short ex. seq. induces a comm. diagram

$$\begin{tikzcd}
\cdots \arrow[r] \arrow[d] & H_1(G,C) \arrow[r, "\delta"] \arrow[d] & A_G \arrow[r] \arrow[d] & B_G \arrow[r] \arrow[d] & C_G \arrow[r] \arrow[d] & 0 \\
\cdots \arrow[r] & H_1(G,C') \arrow[r, "\delta"'] & A'_G \arrow[r] & B'_G \arrow[r] & C'_G \arrow[r] & 0
\end{tikzcd}$$

By convention, we set $H_0(G,A) = A_G$.

Pf As for cohomology, but replace $\mathrm{Hom}_G(-,A)$ by $- \otimes_{\mathbb{Z}(G)} A$ and reverse some arrows. $\square$

__Rmk__ One can again define chains/cycles/boundaries using the standard resolution. H_i = cycles/boundaries.

__Def__ The kernel of the __augmentation map__

$$\varepsilon : \mathbb{Z}[G] \longrightarrow \mathbb{Z} \qquad \text{(a ring hom.)}$$
$$\sum_{g\in G} \underbrace{a_g}_{\in\mathbb{Z}} g \longmapsto \sum_{g\in G} a_g$$

is called the __augmentation ideal__ I_G.

__Rmk__ I_G has $\mathbb{Z}$-basis $(g-e)_{e\neq g\in G}$.

__Pf__ $\sum_{g\in G} a_g g = \sum_{g\in G} a_g (g-e)$. □

__Cor__ $A_G = A/\langle \underbrace{ga-a}_{(g-e)\cdot a} \mid g\in G, a\in A\rangle = A/I_G\cdot A$

__Lemma__ $H_1(G,\mathbb{Z}) \cong I_G/I_G\cdot I_G$

__Pf__ $0 \to I_G \longrightarrow \mathbb{Z}[G] \xrightarrow{\varepsilon} \mathbb{Z} \to 0$

$x \longmapsto x$

induced G-mod.

$$\begin{tikzcd}
 & 1 \arrow[d, equal] & \\
\cdots \arrow[r] & H_1(G,\mathbb{Z}[G]) \arrow[r] & H_1(G,\mathbb{Z}) \arrow[dll, "\delta"] \\
(I_G)_G \arrow[r] \arrow[d, equal] & \mathbb{Z}[G]_G \arrow[r] \arrow[d, equal] & \mathbb{Z}_G \arrow[d, equal] \\
H_0(G,I_G) \arrow[d, equal] & H_0(G,\mathbb{Z}[G]) \arrow[d, equal] & H_0(G,\mathbb{Z}) \arrow[d, equal] \\
I_G/I_G\cdot I_G \arrow[r, bend right] & \mathbb{Z}[G]/I_G\cdot\mathbb{Z}[G] \arrow[d, equal] & \mathbb{Z} \\
x \arrow[r, mapsto] & x_{=0}\ \mathbb{Z}[G]/I_G &
\end{tikzcd}$$

$\Rightarrow H_1(G,\mathbb{Z}) = \ker(I_G/I_G^2 \to \mathbb{Z}[G]/I_G)$ □

Lemma $I_G/I_G\cdot I_G \cong \mathbb{Z}(G)/\langle g_1g_2-g_1-g_2 \mid g_1,g_2\in G\rangle_{\mathbb{Z}\text{-mod}} \cong G^{ab}$

$[g-e] \longleftrightarrow [g] \qquad \uparrow$ additive $\qquad \longleftrightarrow [g]$ multiplicative

Pf $\underbrace{(g_1-e)(g_2-e)}_{\text{generate } I_G\cdot I_G} = (g_1g_2-e)-(g_1-e)-(g_2-e)$

$\mathbb{Z}(G)/\langle g_1g_2-g_1-g_2 \mid g_1,g_2\in G\rangle$ is the max. ab. quotient of G. □

8.10. Transfer map

Lemma C Let $H\le G$ be finite groups. Recall the transfer map $V: G^{ab}\longrightarrow H^{ab}$

$$t \longmapsto \prod_{i=1}^{n}[h_i]$$

, where $r_1,\dots,r_n\in G$ are repr. of the cosets in $H\backslash G$ and $r_i t = h_i r_{\pi(i)}$, $h_i\in H$, $\pi\in S_n$.

The following diagram commutes:

$$\begin{tikzcd}
G^{ab} \arrow[r, "V"] \arrow[dd, "\sim"'] & H^{ab} \arrow[d, "\sim"] \\
 & I_H/I_H\cdot I_H \arrow[d, hook, "\leftarrow \text{injective!}"] \\
I_G/I_G\cdot I_G \arrow[r] & I_G/I_H\cdot I_G \\
x \arrow[r, mapsto] & \sum_{i=1}^{n} r_i\cdot x
\end{tikzcd}$$

Pf $\quad t-e \longmapsto \sum_i r_i(t-e) = \sum(r_it-r_i) = \sum(h_ir_{\pi(i)}-r_i)$

$\equiv \sum(h_i+\cancel{r_{\pi(i)}}-\cancel{r_i}-e) = \sum(h_i-e)$

mod $I_H\cdot I_G$

□

Rmk

$$\begin{tikzcd} G^{ab} \arrow[r, "V"] \arrow[d, phantom, "\cong"] & H^{ab} \arrow[d, phantom, "\cong"] \\ H_1(G,\mathbb{Z}) \arrow[r, "Res"'] & H_1(H,\mathbb{Z}) \end{tikzcd}$$

$Res: H_i(G,A) \to H_1(H,A)$ is the composition

$$H_i(G,A) \longrightarrow H_i(G, \mathrm{coind}^G_H A) \xrightarrow{\sim} H_i(H,A)$$

arising from $A \to \mathrm{coind}^G_H A$ co-Shapiro

For the principal ideal theorem, we used:

Thm Let G be a finite group and $H = [G,G]$ its commutator subgroup. Then $V: G^{ab} \to H^{ab}$ is the "zero map": $V([g]) = [e]$ $\forall [g] \in G^{ab}$.

Reference: Witt, Verlagerung von Gruppen und Hauptidealsatz.

Pf $G/H = G^{ab} = I_G / I_G \cdot I_G$.

Recall: $I_G = \bigoplus_{e \neq g \in G} \mathbb{Z} \cdot (g-e) \cong \mathbb{Z}^{|G|-1}$.

$\Rightarrow I_G \cdot I_G \subseteq I_G$ is a subgroup of index $[G:H]$.

$\Rightarrow I_G \cdot I_G \cong \mathbb{Z}^{|G|-1}$ as groups.

Let $\Big(\underbrace{\sum_{e \neq g \in G} \underbrace{m_{g'g}}_{\in \mathbb{Z}} (g-e)}_{I_G}\Big)_{e \neq g' \in G}$ be a $\mathbb{Z}$-basis of $I_G \cdot I_G$.

$$\Rightarrow \det (m_{g'g})_{e\neq g', g\in G} = \underset{\boxed{\text{w.l.o.g.} +}}{\underset{\uparrow}{\pm}} [G:H].$$

since $\sum_g m_{g'g} \underbrace{(g-e)}_{\text{basis of } I_G} \in I_G \cdot I_G$, we can

find $\mu_{g'g} \in \mathbb{Z}[G]$ s.t. $\mu_{g'g} \equiv m_{g'g} \mod I_G$ (1)

and $\sum_g \mu_{g'g}(g-e) = 0 \ \forall\, e \neq g' \in G$. (2)

Idea: solve the system of lin. eq. (2) for $g-e$.

Problem: $\mathbb{Z}[G]$ isn't commutative!

But $\mathbb{Z}[G/H] \cong \mathbb{Z}[G^{ab}]$ is commutative.

Claim We have a ring isomorphism

$$\mathbb{Z}[G] \big/ \underbrace{I_H \cdot G}_{\text{two-sided } \mathbb{Z}[G]\text{-ideal generated by } I_H} \xrightarrow[\varphi]{\sim} \mathbb{Z}[G/H]$$

because H is a normal subgroup of G

Pf $$\Big[\sum_g a_g g\Big] \longmapsto \sum_g a_g \overbrace{(Hg)}^{\in G/H}$$

$$\sum a_g (Hg) = 0 \text{ in } \mathbb{Z}[G/H]$$

$$\shortparallel$$

$$\sum_i \sum_h a_{hr_i}(Hr_i)$$

$$\Leftrightarrow \sum_h a_{hr_i} = 0 \ \forall i \Rightarrow \sum a_g g = \sum a_{hr_i} h r_i$$

$$= \sum_i \underbrace{\underbrace{\Big(\sum_h a_{hr_i} h\Big)}_{\in I_H} \underbrace{r_i}_{\in G}}_{\in I_H \cdot G}.$$

$\square$

...

~> We can interpret $(\mu_{g'g})_{g',g}$ as a matrise with entries in $\mathbb{Z}[G/H]$ and construct its adjoint matrise $(\lambda_{g'g})_{g',g}$ with entries in $\mathbb{Z}[G/H]$. Lift them to entries in $\mathbb{Z}[G]$ using ρ. The product of the matrices over $\mathbb{Z}[G/H]$ is $\det(\mu_{g'g})_{g'g}$ times the identity matrise.

$$\Rightarrow \sum_{g'} \lambda_{g''g'}\mu_{g'g} \equiv \begin{cases} \det(\mu_{g'g})_{g',g}, & g''=g \\ 0, & g''\neq g \end{cases} \mod I_H\cdot G.$$

$$\Rightarrow \sum_{g',g} \lambda_{g''g'}\mu_{g'g}\underbrace{(g-e)}_{\in I_G} \overset{(2)}{=\!=} 0$$

$$|||$$

$$\underbrace{\det(\mu_{g'g})_{g',g}}\cdot\underbrace{(g''-e)}_{\in I_G} \mod I_H\cdot G\cdot I_G$$

$$\boxed{I_G \subseteq I_H\cdot G}$$

$$\overset{}{\underset{(1)}{\equiv}} \det(m_{g'g})_{g',g} \mod I_H\cdot G$$

$$\equiv [G:H] \qquad \mod I_H\cdot G$$

$$\equiv \sum_{i=1}^{n} r_i \qquad \mod I_G \subseteq I_H\cdot G$$

$$\Rightarrow \sum_i r_i(g''-e) \in I_H\cdot G\cdot I_G = I_H\cdot I_G.$$

$$\Rightarrow \quad V([g'']) = 0 = (e)$$

□

Lemma C