Notes on Class Field Theory

Thomas Krämer (HU Berlin, Winter 23/24)

Intro to CFT

ANT = Arithmetic of Galois extensions of number fields

∪

CFT = Arithmetic of abelian extensions of number fields

0. What does "arithmetic" mean?

$K/\mathbb{Q}$ number field

$\mathcal{O}_K :=$ int. closure of $\mathbb{Z}$ in K

$= \{ a \in K \mid \exists P \in \mathbb{Z}[x] \text{ monic w/ } P(a)=0 \}$

$\Rightarrow \mathcal{O}_K$ is Dedekind

$\Rightarrow$ every nonzero ideal $I \trianglelefteq \mathcal{O}_K$ decomposes uniquely (up to permutation of the factors) as

$I = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$ w/ $\mathfrak{p}_i \in \mathrm{Spm}(\mathcal{O}_K)$, $e_i \in \mathbb{N}$.

(pairwise distinct)

K/k extension of number fields

$\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_k)$

$\Rightarrow \mathfrak{p}\cdot\mathcal{O}_K = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ w/ $\mathfrak{P}_i \in \mathrm{Spm}(\mathcal{O}_K)$, $e_i \in \mathbb{N}$.

(pairwise distinct)

We have an extension of finite fields

$$\mathbb{F}_{\mathfrak{p}} := \mathcal{O}/\mathfrak{p} \hookrightarrow \mathbb{F}_{\mathfrak{P}_i} := \mathcal{O}_K/\mathfrak{P}_i$$

Def e_i is called the ramification index,

$f_i := [\mathbb{F}_{\mathfrak{P}_i} : \mathbb{F}_{\mathfrak{p}}]$ the inertia degree of $\mathfrak{P}_i/\mathfrak{p}$.

Basic formula: $[K:k] = \sum_{i=1}^{g} e_i f_i$.

Rem If K/k is Galois, then $e_1 = \cdots = e_g =: e$

$f_1 = \cdots = f_g =: f$

& $[K:k] = efg$.

How to control these decompositions?

Recall:

$\mathfrak{p}$ ramifies in K/k $:\iff$ $e_i > 0$ for some i

$\iff$ $\mathfrak{p} \mid \partial_{K/k}$:= discriminant ideal of K/k

only finitely many such $\mathfrak{p}$, don't give much information about K/k.

At the opposite side we have:

Def $\mathfrak{p}$ splits (completely) in K/k if $e_i = f_i = 1$ for all i.

$\mathfrak{p}$ is inert in K/k if $g = e = 1$, ie $f = [K:k]$.

Q Which primes split in a given extension K/k?

↳ much more information: For K/k Galois, the set of split primes determines K!

Ex $K = \mathbb{Q}(\sqrt{d}) \,/\, k = \mathbb{Q}$ w/ $d \in \mathbb{Z}$ squarefree

$$\mathcal{O}_K = \mathbb{Z}[\alpha] \text{ w/ } \alpha := \begin{cases} \sqrt{d} & \text{if } d \not\equiv 1 \ (4) \\ \frac{1+\sqrt{d}}{2} & \text{else} \end{cases}$$

$$\partial_{K/k} = (\Delta) \text{ w/ } \Delta = \begin{cases} 4d & \text{if } d \not\equiv 1 \ (4) \\ d & \text{else} \end{cases}$$

a) $\mathfrak{p}$ ramifies in $K \iff \mathfrak{p}\mathcal{O}_K = \mathfrak{P}^2$ for some $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_K)$

$\iff \mathfrak{p} \mid \Delta$

b) $\mathfrak{p}$ splits in $K \iff \mathfrak{p}\mathcal{O}_K = \mathfrak{P}\mathfrak{Q}$ w/ $\mathfrak{P} \neq \mathfrak{Q} \in \mathrm{Spm}(\mathcal{O}_K)$

$\iff \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \simeq \mathbb{F}_\mathfrak{p} \times \mathbb{F}_\mathfrak{p}$

$\mathbb{F}_\mathfrak{p}[t]/(t^2 - d)$

$\iff d$ is a square mod $\mathfrak{p}$, ie $\left(\frac{d}{\mathfrak{p}}\right) = 1$.

c) $\mathfrak{p}$ inert in $K \iff \mathfrak{p}\mathcal{O}_K = \mathfrak{P}$ prime

$\iff \mathcal{O}_K/\mathfrak{p}\mathcal{O}_K \simeq \mathbb{F}_{\mathfrak{p}^2} \iff \left(\frac{d}{\mathfrak{p}}\right) = -1$.

Note: By quadratic reciprocity, $\left(\frac{d}{\mathfrak{p}}\right)$ only depends on $\mathfrak{p}$ mod d!

Ex Cyclotomic fields:

$K = \mathbb{Q}(\zeta_m) \,/\, k = \mathbb{Q}$ w/ $\zeta_m = e^{2\pi i/m}$

Galois with $(\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\sim} Gal(K/k)$

$[a] \longmapsto (\zeta_m \mapsto \zeta_m^a)$

$\mathcal{O}_K = \mathbb{Z}[\zeta_m]$

a) p ramifies in $K \iff p \mid m$

(ramificat^{n} index $e = \varphi(p^i) = p^{i-1}(p-1)$ for $p^i \| m$,
thus wild ramification $\iff p^2 \mid m$)

b) If $p \nmid m$, then $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$

w/ inertia degree

$f = [\mathbb{F}_{\mathfrak{p}_i} : \mathbb{F}_p] =$ order of p in $(\mathbb{Z}/m\mathbb{Z})^*$

↑ look at Frobenius...

Thus:

p splits completely in $K \iff p \equiv 1 \ (m)$.

1. Frobenii & quadratic reciprocity, revisited

K/k Galois extension of # fields

$\mathfrak{P} \in Spm(\mathcal{O}_K)$, $\mathfrak{p} := \mathfrak{P} \cap \mathcal{O}_k \in Spm(\mathcal{O}_k)$

$G := Gal(K/k)$

$\cup$

$D_{\mathfrak{P}|\mathfrak{p}} := \{ g \in G \mid g\mathfrak{P} = \mathfrak{P} \}$ "decomposition gp"

acts on $\mathbb{F}_{\mathfrak{P}} = \mathcal{O}_K/\mathfrak{P}$

$\Rightarrow$ epi $\varphi : D_{\mathfrak{P}|\mathfrak{p}} \longrightarrow Gal(\mathbb{F}_{\mathfrak{P}} / \mathbb{F}_{\mathfrak{p}})$

Put $I_{\mathfrak{P}|\mathfrak{p}} := \ker(\varphi)$ "inertia group"

Rem • For $\mathfrak{Q} = g(\mathfrak{P})$ have $D_{\mathfrak{Q}|\mathfrak{p}} = g D_{\mathfrak{P}|\mathfrak{p}} g^{-1}$

$I_{\mathfrak{Q}|\mathfrak{p}} = g I_{\mathfrak{P}|\mathfrak{p}} g^{-1}$

• For G abelian we write $D_{\mathfrak{p}} := D_{\mathfrak{P}|\mathfrak{p}}$

$I_{\mathfrak{p}} := I_{\mathfrak{P}|\mathfrak{p}}$.

Fact $\mathfrak{p}$ unramified in $K \iff I_{\mathfrak{p}} = (1)$

In that case φ is an iso

$$\begin{array}{ccc} D_{\mathfrak{p}} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}} | \mathbb{F}_p) \\ \cup & & \cup \\ \exists!\, \sigma_{\mathfrak{p}} & \longmapsto & (x \mapsto x^q), \quad q = \#\mathbb{F}_{\mathfrak{p}}. \end{array}$$

Def $\sigma_{K/k,\mathfrak{p}} := \sigma_{\mathfrak{p}} \in \mathrm{Gal}(K/k)$ "Frobenius at $\mathfrak{p}$"

Rem The inertia degree is given by

$f =$ order of $\sigma_{\mathfrak{p}}$ in $\mathrm{Gal}(K/k)$.

In particular we have:

$\mathfrak{p}$ splits completely $\iff \sigma_{\mathfrak{p}} = 1$.

Ex $K = \mathbb{Q}(\zeta_m)$

For $p \nmid m$, have $\sigma_p \in \mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^*$

given by $\zeta_m \mapsto \zeta_m^p$.

Cor (Quadratic reciprocity) Let p, q be odd primes, then

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) \quad \text{for} \quad p^* := (-1)^{\frac{p-1}{2}} \cdot p.$$

Pf. Let $L = \mathbb{Q}(\zeta_p)$

$$\begin{array}{ccc} \mathrm{Gal}(L|\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^* & & L \\ \cup \qquad\qquad \cup & & | \\ H := \{\text{squares}\} & & K := L^H \\ & & | \wr \text{ quadratic extension} \\ & & \mathbb{Q} \end{array}$$

Consider $x := \sum_{n=0}^{p-1} \zeta_p^{n^2} \in L^H = K$

$\Rightarrow x^2 = p^*$ by direct computation

$\Rightarrow K = \mathbb{Q}(\sqrt{p^*})$ for degree reasons

Thus:

$\left(\frac{q}{p}\right) = 1 \iff \sigma_{L|\mathbb{Q},q} \in H$ (by def^n of $(\frac{\cdot}{p})$ and H)

$\iff 1 = \sigma_{L|\mathbb{Q},q}|_K \; (= \sigma_{K/\mathbb{Q},q})$

$\iff q$ splits completely in $K = \mathbb{Q}(\sqrt{p^*})$

$\iff \left(\frac{p^*}{q}\right) = 1$

□

2. CFT over $k = \mathbb{Q}$

Upshot of the proof:

For odd primes p & $p^* := (-1)^{\frac{p-1}{2}} \cdot p$ we have

looked at $L = \mathbb{Q}(\zeta_p) \supset K = \mathbb{Q}(\sqrt{p^*})$:

$$\begin{array}{ccc} (\mathbb{Z}/p\mathbb{Z})^* & \xrightarrow[q \mapsto \sigma_q]{\sim} & \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \\ & \searrow^{(\frac{p^*}{\cdot})} & \downarrow (-)|_K \\ & & \mathrm{Gal}(K/\mathbb{Q}) = \{\pm 1\} \end{array}$$

$\Rightarrow (\frac{p^*}{\cdot}) : (\mathbb{Z}/p\mathbb{Z})^* \twoheadrightarrow \{\pm 1\}$ epi

cyclic, hence has a unique subgp of index 2

$\Rightarrow (\frac{p^*}{\cdot}) = (\frac{\cdot}{p})$

Such a strategy works for ANY abelian $K/\mathbb{Q}$:

Thm (Kronecker–Weber = CFT over $\mathbb{Q}$)

For any abelian Galois extension $K/\mathbb{Q}$,

$\exists\, m \in \mathbb{N}$ w/ $K \subset L_m := \mathbb{Q}(\zeta_m)$.

We get:

$$\begin{array}{ccc} (\mathbb{Z}/m\mathbb{Z})^* & \xrightarrow{\sim} & \mathrm{Gal}(L_m/\mathbb{Q}) \\ & \searrow & \downarrow \\ & & \mathrm{Gal}(K/\mathbb{Q}) \end{array}$$

"Artin map"

The smallest such m is called the conductor of K.

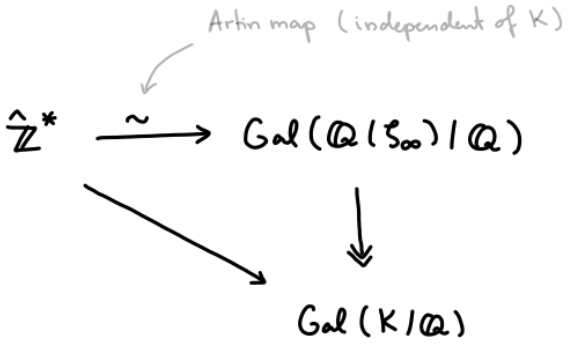
Intrinsic reformulation If you don't want to choose an m for each given $K/\mathbb{Q}$ separately, consider instead

$$\hat{\mathbb{Z}}^* := \varprojlim_m (\mathbb{Z}/m\mathbb{Z})^* \overset{\text{CRT}}{\simeq} \prod_p \mathbb{Z}_p^*$$

Let $\mathbb{Q}(\zeta_\infty) := \bigcup_m \mathbb{Q}(\zeta_m)$,

then we get for every finite abelian extension $K/\mathbb{Q}$

a surjection as shown below ("idelic CFT over $\mathbb{Q}$"):



Upshot: $\exists$ bijection

$$\left\{ \begin{array}{c} \text{open subgps} \\ \text{of } \hat{\mathbb{Z}}^* \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{finite abelian Galois} \\ \text{extensions } K/\mathbb{Q} \end{array} \right\}$$

$$H \longmapsto K = (\mathbb{Q}(\zeta_\infty))^H$$

s.th.

q splits in $K \iff q \equiv 1 \bmod H$

Punchline: $\hat{\mathbb{Z}}^*$ only uses arithmetic of $\mathbb{Q}$, not of $\mathbb{Q}(\zeta_\infty)$!

3. Ray class gps: Towards base fields $k \neq \mathbb{Q}$

Motivation: For $K/\mathbb{Q}$ abelian Galois (& finite),

$\exists m$: $K \subset \mathbb{Q}(\zeta_m)$ (Kronecker-Weber)

$\Rightarrow$ For prime numbers $p \nmid m$,

$\sigma_p :=$ (Frobenius at p) $\in \mathrm{Gal}(K/\mathbb{Q})$

only depends on $p \bmod m$!

(hence ditto for split primes etc...)

Q Analog for abelian Galois extensions K/k

of number fields with $k \neq \mathbb{Q}$?

→ main thm of CFT (see below)!

Need to replace

"prime number p ⇝ prime ideal $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_k)$"

$p \bmod m$ ⇝ ??

Note For $a \in \mathbb{Q}$ put $(a) := a\mathbb{Z} \subset \mathbb{Q}$.

Write $a \equiv 1 \bmod m$ if $v_p(a-1) \geq v_p(m)$ for all $p \mid m$.

Then for $p, q \in \mathbb{N}$ we have:

- $p \equiv \pm q \bmod m$

  $\iff (p) = (a)\cdot(q)$

  for some $a \in \mathbb{Q}^*$ w/ $a \equiv 1 \bmod m$

- $p \equiv q \bmod m$

  $\iff (p) = (a)\cdot(q)$

  for some positive $a \in \mathbb{Q}^*$ w/ $a \equiv 1 \bmod m$

Thus

$$(\mathbb{Z}/m\mathbb{Z})^* = \frac{\{(a) : a \in \mathbb{Q}^* \text{ coprime to } m\}}{\{(a) : a \equiv 1 \bmod m \text{ and } a > 0\}}$$

RHS is purely in terms of (fractional) ideals!

Def Let k be a number field.

A cycle (or modulus) for k is a formal product $m = m_f \cdot m_\infty$ with

- $m_f \trianglelefteq \mathcal{O}_k$ a nonzero ideal,
- m_∞ a set of real places $\sigma : K \hookrightarrow \mathbb{R}$.

Inside the group of fractional ideals

$$I_k := \{ \underbrace{a\mathcal{O}_k}_{\| (a)} \subseteq k^* \mid a \in k^* \} \simeq \bigoplus_{\mathfrak{p} \in \operatorname{Spm} \mathcal{O}_k} \mathbb{Z}\cdot\mathfrak{p}$$

consider the subgroups

$$I(m) := I(m_0) := \langle \mathfrak{p} \mid \mathfrak{p} \nmid m \rangle$$

$$\cup$$

$$R(m) := \{(a) \mid a \equiv 1 \bmod^* m\}$$

w/ $a \equiv 1 \bmod^* m :\iff \begin{cases} v_\mathfrak{p}(a-1) \geq v_\mathfrak{p}(m_f) \ \forall \mathfrak{p} \mid m_f, \\ \sigma(a) > 0 \ \forall \sigma \in m_\infty \end{cases}$

We call $R(\mathfrak{m})$ a "ray"

and $Cl(\mathfrak{m}) := I(\mathfrak{m})/R(\mathfrak{m})$

the "ray class group with modulus $\mathfrak{m}$".

Ex For $k = \mathbb{Q}$, there are two types of cycles:

a) $\mathfrak{m} = \mathfrak{m}_f = (m)$ w/ $m \in \mathbb{N}$

$\Rightarrow Cl(\mathfrak{m}) = (\mathbb{Z}/m\mathbb{Z})^*/\{\pm 1\}$

b) $\mathfrak{m} = (m)\cdot\infty$ w/ $m \in \mathbb{N}$

$\Rightarrow Cl(\mathfrak{m}) = (\mathbb{Z}/m\mathbb{Z})^*$

Ex For $\mathfrak{m} = (1)$ the "empty cycle" we recover the class group $Cl((1)) = I_k/k^* =: Cl_k$.

Rem We say that a cycle $\mathfrak{m}$ divides a cycle $\mathfrak{n}$ and write $\mathfrak{m} \mid \mathfrak{n}$ if $\mathfrak{m}_f \mid \mathfrak{n}_f$ and $\mathfrak{m}_\infty \subset \mathfrak{n}_\infty$.

Then $R(\mathfrak{n}) \subset R(\mathfrak{m})$,

$Cl(\mathfrak{n}) \twoheadrightarrow Cl(\mathfrak{m})$.

4. The main thm of global CFT

K/k abelian Galois extension of # fields

For any cycle $\mathfrak{m}$ divisible by all primes ramified in K/k,

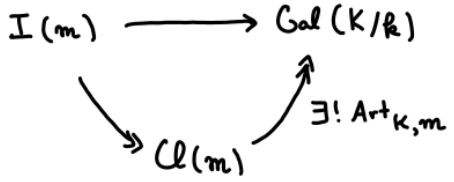
we have the "Artin map"

$$\begin{array}{ccc} I(\mathfrak{m}) & \longrightarrow & Gal(K/k) \\ \cup & & \cup \\ [\mathfrak{p}] & \longmapsto & \sigma_{\mathfrak{p}} \quad \text{for } \mathfrak{p} \text{ prime} \end{array}$$

Main thm a) Artin reciprocity: For every abelian K/k,

$\exists$ cycle $\mathfrak{m}$ divisible by all ramified primes

s.th. the Artin map factors as



Moreover, $\exists!$ minimal such $\mathfrak{m}$, the conductor of K/k,

divisible by precisely the places that ramify

(including possibly real places, see below).

b) Existence: For any cycle $\mathfrak{m}$, $\exists!$ subfield $k_{\mathfrak{m}} \subseteq k^{ab}$ w/ conductor dividing $\mathfrak{m}$ sth the Artin map

$$\mathrm{Art}_{\mathfrak{m}} : Cl(\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(k_{\mathfrak{m}}) \quad \text{is an iso.}$$

$\uparrow (:= \mathrm{Art}_{k_{\mathfrak{m}},\mathfrak{m}})$

We call $k_{\mathfrak{m}}$ the <u>ray class field</u> w/ modulus $\mathfrak{m}$.

c) Completeness: For K/k abelian w/ conductor $\mathfrak{f}$,

$$K \subset k_{\mathfrak{m}} \iff \mathfrak{f} \mid \mathfrak{m}.$$

<u>Upshot</u> Every finite abelian extension K/k embeds in some $k_{\mathfrak{m}}/k$, and $\exists$ inclusion-reversing bijection

$$\{\text{subgroups of } Cl(\mathfrak{m})\} \xleftrightarrow{1:1} \{\text{subfields of } k_{\mathfrak{m}}\}$$

$$H = \ker(\mathrm{Art}_{K,\mathfrak{m}}) \longmapsto (K \subset k_{\mathfrak{m}})$$

<u>Note</u> $\mathrm{Art}_{K,\mathfrak{m}} : Cl(\mathfrak{m})/H \xrightarrow{\sim} \mathrm{Gal}(K/k)$,

so the inertia degree of any prime $\mathfrak{p} \nmid \mathfrak{m}$ is

$$f_{\mathfrak{p}} = \text{order of } [\mathfrak{p}] \text{ in } Cl(\mathfrak{m})/H$$

<u>Rem</u> A more precise version of Artin reciprocity describes $H := \ker(\mathrm{Art}_{K,\mathfrak{m}})$ via the norm

$$N_{K/k} : I_K \to I_k : \quad (\mathfrak{P} \mapsto \mathfrak{p}^f \text{ for } \mathfrak{P} \mid \mathfrak{p} \text{ prime w/ inertia degree } f)$$

Define a cycle $\mathfrak{M}$ for K by $\mathfrak{M}_{\mathfrak{f}} := \mathfrak{m}_{\mathfrak{f}} \cdot \mathcal{O}_K$,

$\mathfrak{M}_{\infty} := \{\text{real places of } K \text{ above a place in } \mathfrak{m}_{\infty}\}$.

Then we have

$$\begin{array}{ccc} I_K & \xrightarrow{N_{K/k}} & I_k \\ \cup & & \cup \\ I(\mathfrak{M}) & \longrightarrow & I(\mathfrak{m}) \\ \cup & & \cup \\ R(\mathfrak{M}) & \longrightarrow & R(\mathfrak{m}) \end{array}$$

$$\Rightarrow N_{K/k} : Cl(\mathfrak{M}) \to Cl(\mathfrak{m})$$

The explicit form of Artin reciprocity then says that $H = N_{K/k}(Cl(\mathfrak{M}))$.

$$\Rightarrow \quad I(\mathfrak{m}) \Big/ R(\mathfrak{m}) \cdot N_{K/k}(I(\mathfrak{M})) \xrightarrow{\sim} \mathrm{Gal}(K/k)$$

Ex Ray class fields over $k = \mathbb{Q}$:

a) For cycles $\mathfrak{m} = (m) \cdot \infty$ we have

$$Cl(\mathfrak{m}) \simeq (\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\sim} Gal(\mathbb{Q}(\zeta_m)/\mathbb{Q}),$$

hence the ray class field of $\mathfrak{m}$ is $\mathbb{Q}(\zeta_m)$.

Any cycle for $\mathbb{Q}$ divides a cycle of this form, so part c) in the main thm recovers Kronecker-Weber: $\mathbb{Q}^{ab} = \bigcup_m \mathbb{Q}(\zeta_m)$.

b) For cycles $\mathfrak{m} = (m)$ one similarly sees that the ray class field of $\mathfrak{m}$ is the maximal real subfield $\mathbb{Q}(\zeta_m + \overline{\zeta}_m) \subset \mathbb{Q}(\zeta_m)$.

Caution Kronecker-Weber only holds over $\mathbb{Q}$:

For every # field $k \neq \mathbb{Q}$, $\exists$ quadratic extension K/k which is not cyclotomic, ie. $K \not\subset k(\zeta_m)$ for any m (see exercises).

Ex Conductor of quadratic # fields over $k = \mathbb{Q}$:

Let $K = \mathbb{Q}(\sqrt{d})$ w/ $d \in \mathbb{Z}$ squarefree

In the exercises we'll see

$$K \subset \mathbb{Q}(\zeta_m) \text{ for } m = \begin{cases} |d| & \text{if } d \equiv 1 \ (4) \\ 4|d| & \text{else,} \end{cases}$$

and that this m is minimal w/ that property.

Moreover $K \subset \mathbb{Q}(\zeta_m + \overline{\zeta}_m)$ if and only if $d > 0$.

$\Rightarrow$ The conductor of $K/\mathbb{Q}$ is

$$\mathfrak{f} = \begin{cases} (m) & \text{if } d > 0 \\ (m)\infty & \text{if } d < 0 \end{cases}$$

If we want the statement about ramified places in the main thm to be true, we must define the place ∞ of $\mathbb{Q}$ to be ramified in $K/\mathbb{Q}$ iff $d < 0$, ie iff it extends to a cplex place of K...

A brief reminder about places:

Def A place v of a # field k is one of the following:

a) A prime $\mathfrak{p} \in \mathrm{Spm}(\mathcal{O}_k)$ (finite places)

b) An embedding $\sigma : k \hookrightarrow \mathbb{R}$ (real places)

c) A pair of two distinct complex conjugate embeddings $\sigma, \overline{\sigma} : k \hookrightarrow \mathbb{C}$ (cplex places)

Each place gives rise to an absolute value

$$|\cdot|_v : k^* \longrightarrow \mathbb{R}_{>0}$$

$$|x|_v := \begin{cases} |\mathbb{F}_{\mathfrak{p}}|^{-\nu_{\mathfrak{p}}(x)} & \text{in case a)} \\ |\sigma(x)| & \text{in case b), c).} \end{cases}$$

The places in b), c) are called archimedean.

Def An archimedean place v of k ramifies in an extension K/k if it is real but extends to a cplex place w of K

Def By the Hilbert class field of k we mean the ray class field $H := HCF(k) := k_{(1)}$ for the empty modulus $m = (1)$.

By the properties in the main thm,

- H is the largest abelian extension of k that is unramified at all places.
- $Cl_k = Cl((1)) \xrightarrow{\sim} Gal(H/k)$.

Rem Another marvellous property of $H = HCF(k)$ is that for any ideal $\mathfrak{a} \trianglelefteq \mathcal{O}_k$, the ideal $\mathfrak{a} \cdot \mathcal{O}_H$ becomes principal (but that's not immediate from the main thm).

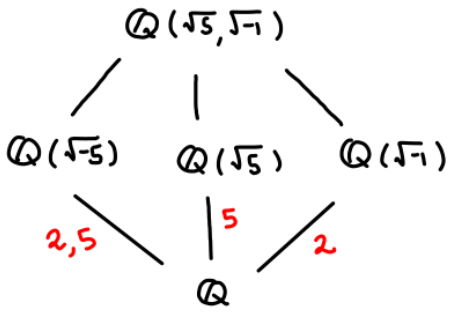
Caution: We can still have $Cl_H \neq 1$!

Ex $\mathcal{O}_k$ is a UFD iff $H := HCF(k) = k$

($\mathcal{O}_k$ UFD $\Leftrightarrow Cl_k = \{1\} \Leftrightarrow Gal(H/k) = \{1\}$)

Ex $k = \mathbb{Q}(\sqrt{-5})$ has $HCF(k) = \mathbb{Q}(\sqrt{5}, \sqrt{-1})$:

Looking at discriminants, one sees that $p = 2, 5$ are the only primes ramified in $\mathbb{Q}(\sqrt{5}, \sqrt{-1})$.



only the written primes ramify in the respective extensions ...

$\Rightarrow$ $H := \mathbb{Q}(\sqrt{5}\sqrt{-1})$ unramified over $k = \mathbb{Q}(\sqrt{-5})$

(note: k has no real places, so no ramificat^n at ∞)

But $Cl(k) \simeq \mathbb{Z}/2 \Rightarrow H = HCF(k)$

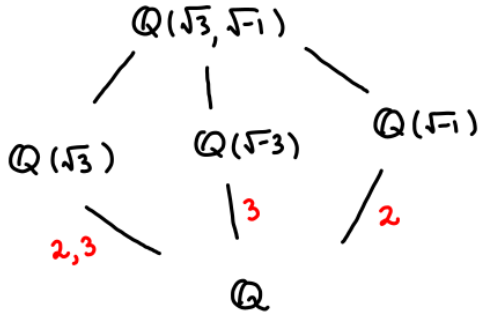
e.g. use Minkowski bound: Cl_k is generated by prime ideals of norm $\leq \sqrt{|\Delta|} \cdot \left(\frac{4}{\pi}\right)^s \cdot \frac{n!}{n^n} < 3$ for $|\Delta| = 20$, $s = 1$, $n = 2$

Ex Why ramification at ∞ matters:

$k = \mathbb{Q}(\sqrt{3})$ has $HCF(k) = k$,

since $Cl_k = \{1\}$ (eg by Minkowski bound).

Consider now $K = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$:



$\Rightarrow$ $K = \mathbb{Q}(\sqrt{3}, \sqrt{-1})$ over $k = \mathbb{Q}(\sqrt{3})$ unramified at all finite places of k!

But: Both real places of k ramify in K/k, so there's no contradiction to CFT.

5. Idelic version of the main thm

The main thm of CFT says every finite abelian extension of k is contained in a ray class field $k_{\mathfrak{m}}$ for some cycle $\mathfrak{m}$. To avoid the choice of $\mathfrak{m}$, consider

$$k^{ab} = \bigcup_{\mathfrak{m}} k_{\mathfrak{m}} \quad \text{(inside a fixed alg closure } \bar{k}/k\text{)}$$

$$\circlearrowleft$$

$$\mathrm{Gal}(k^{ab}/k) = \varprojlim_{\mathfrak{m}} \mathrm{Gal}(k_{\mathfrak{m}}/k)$$

For $\mathfrak{m} \mid \mathfrak{n}$ we have $k_{\mathfrak{m}} \subset k_{\mathfrak{n}}$ and a natural commutative diagram

$$\begin{array}{ccc} Cl(\mathfrak{n}) & \xrightarrow[\mathrm{Art}_{\mathfrak{n}}]{\sim} & \mathrm{Gal}(k_{\mathfrak{n}}/k) \\ \downarrow & & \downarrow \\ Cl(\mathfrak{m}) & \xrightarrow[\mathrm{Art}_{\mathfrak{m}}]{\sim} & \mathrm{Gal}(k_{\mathfrak{m}}/k) \end{array}$$

$\Rightarrow$ The Artin maps fit together to give an iso

$$\mathrm{Art}: \varprojlim_{\mathfrak{m}} Cl(\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(k^{ab}/k).$$

Ex For $k = \mathbb{Q}$ we get

$$\hat{\mathbb{Z}}^* := \varprojlim_{\mathfrak{m}} (\mathbb{Z}/m\mathbb{Z})^* \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$$

$$\| $$

$$\prod_p \mathbb{Z}_p^*$$

To realize a similar description via local data at each prime also for $k \neq \mathbb{Q}$, we use idèles...

Def For a place v of k we put

$k_v :=$ completion of k wrt the abs. value $|\cdot|_v$

Ex For $k = \mathbb{Q}$ we get

$$k_v = \begin{cases} \mathbb{R} & \text{if } v = \infty \\ \mathbb{Q}_p & \text{if } v = p \text{ for a prime } p \end{cases}$$

In general, for any # field k we have:

- If v is a real place, then $k_v \simeq \mathbb{R}$
- If v is a cplex place, then $k_v \simeq \mathbb{C}$
- If v is a finite place, say above a prime number p, then k_v is a finite ext^n of $\mathbb{Q}_p$.

For finite places $v = \wp$, we have $|x|_\wp = N^{-v_\wp(x)}$
w/ $N = \#\mathbb{F}_\wp$ & the discrete valuation $v_\wp : k^* \to \mathbb{Z}$,
so in particular

$$\mathcal{O}_\wp := \{x \in k_\wp \mid |x|_\wp \leq 1\} \quad \text{is a DVR}$$
$$\cup$$
$$\mathfrak{m}_\wp := \wp \cdot \mathcal{O}_\wp = \{x \in k_\wp \mid |x|_\wp < 1\} \quad \text{max. ideal}$$

$$\mathcal{O}_\wp^* = \{x \in k_\wp \mid |x|_\wp = 1\}$$

Def The group of idèles of k is

$$\mathbb{I}_k := \prod_v{}' k_v^* \quad \leftarrow \text{"restricted product"}$$

$$:= \left\{ (x_v) \in \prod_v k_v^* \;\middle|\; x_v \in \mathcal{O}_v^* \text{ for almost all } v \right\}$$

(for archimedean places v we put $\mathcal{O}_v := k_v$,
but for the restricted product this is really
irrelevant as $\exists$ only finitely many such places)

Each k_v^* comes w/ a natural topology,
and we make $\mathbb{I}_k$ a loc. cpact top gp
by declaring the open subsets to be those
of the form

$$U := \prod_{v \notin S} \mathcal{O}_v^* \times \prod_{v \in S} U_v$$

w/ S a finite set of places
& $U_v \subseteq k_v^*$ open subsets.

Note This is NOT the topology induced from the product topology via the inclusion $\mathbb{I}_k \hookrightarrow \prod_v k_v^*$. The latter would NOT make $\mathbb{I}_k$ locally cpact...

Rem We used the "restricted product" in the def of idèles since this gives a natural epi

$$\begin{array}{ccc} \mathbb{I}_k & \twoheadrightarrow & I_k := \text{gp of fractional ideals of } k \\ \wr\downarrow & & \wr\downarrow \\ (x_\mathfrak{p}) & \longmapsto & \mathfrak{a} := \{a \in k^* \mid v_\mathfrak{p}(a) \geq v_\mathfrak{p}(x_\mathfrak{p}) \ \forall \mathfrak{p} \nmid \infty\}. \end{array}$$

Its kernel is the open subgp $U(1) := \prod_v \mathcal{O}_v^*$

$$\Rightarrow \quad \mathbb{I}_k / U(1) \xrightarrow{\sim} I_k$$

Dividing out the diagonally embedded $k^* \hookrightarrow \mathbb{I}_k$ we get:

$$\mathbb{I}_k / k^* \cdot U(1) \xrightarrow{\sim} \mathcal{C}l_k$$

More generally:

To any modulus $\mathfrak{m} = \prod_v v^{n_v}$ w/ $n_v \in \mathbb{N}_0$ for v finite, $n_v \in \{0,1\}$ for v real, $n_v = 0$ for v cplex

we attach the open subgp

$$U(\mathfrak{m}) := \prod_v U_v^{(n_v)} \subset \mathbb{I}_k$$

where

- for $v = \mathfrak{p}$ finite we put

$$U_v^{(n)} := 1 + \mathfrak{p}^n \mathcal{O}_\mathfrak{p}^\times \subset \mathcal{O}_\mathfrak{p}^\times \quad \text{for } n \in \mathbb{N}_0.$$

- for $v \mid \infty$ we put

$$U_v^{(n)} := \begin{cases} \mathbb{R}_{>0} & \text{for } v \text{ real } \& \ n = 1 \\ \mathbb{R}^* & \text{for } v \text{ real } \& \ n = 0 \\ \mathbb{C}^* & \text{for } v \text{ cplex} \end{cases}$$

Note: Every open subgp of $\mathbb{I}_k$ contains one of this form for some $\mathfrak{m}$.

Lemma $\mathbb{I}_k / k^\times \cdot U(\mathfrak{m}) \xrightarrow{\sim} \mathcal{C}\ell(\mathfrak{m})$ (:= ray class gp of modulus $\mathfrak{m}$)

Pf. Put

$$\mathbb{I}(\mathfrak{m}) := \{ (x_v) \in \mathbb{I}_k \mid x_v \in U(\mathfrak{m})_v \ \forall\, v \mid \mathfrak{m} \}$$

$$\Rightarrow \quad \mathbb{I}(\mathfrak{m}) / U(\mathfrak{m}) \xrightarrow{\sim} I(\mathfrak{m}) \quad (:= \text{fractional ideals coprime to } \mathfrak{m}_f)$$

We have

$$k^\times(\mathfrak{m}) := k^\times \cap \mathbb{I}(\mathfrak{m})$$
$$= \{ x \in k^* \mid x \equiv 1 \bmod^\times \mathfrak{m} \}$$

$$\Rightarrow \quad \mathbb{I}(\mathfrak{m}) / k^\times(\mathfrak{m}) \cdot U(\mathfrak{m}) \xrightarrow{\sim} \mathcal{C}\ell(\mathfrak{m}) := I(\mathfrak{m}) / R(\mathfrak{m})$$

Now use that $\mathbb{I} = \mathbb{I}(\mathfrak{m}) \cdot k^\times$

so that $\mathbb{I}(\mathfrak{m}) / k^\times(\mathfrak{m}) \simeq \mathbb{I} / k^\times$

Dividing by $U(\mathfrak{m})$ gives the result. □

Rem

- $k^\times \hookrightarrow \mathbb{I}_k$ is a discrete subgp (exercise, using the approximation thm)
- The idèle class gp $C_k := \mathbb{I}_k / k^\times$ inherits from $\mathbb{I}_k$ a natural loc cpact topology. The open subgps of C_k are precisely the subgps $k^\times \cdot U(\mathfrak{m}) / k^* \subset C_k$ for arbitrary moduli $\mathfrak{m}$. We get:

Main thm (version for idèles) $\exists$ natural epi

$$\mathrm{Art}_k : C_k \twoheadrightarrow \mathrm{Gal}(k^{ab}/k) \text{ inducing}$$

for any finite abelian K/k an iso

$$\mathrm{Art}_{K/k} : C_k / U \xrightarrow{\sim} \mathrm{Gal}(K/k)$$

ψ $\qquad$ Ψ

$\pi_\varphi := (x_v) \longmapsto \sigma_\varphi$ for φ unramified in K/k

w/ $x_v = \begin{cases} 1, & v \neq \varphi \\ \text{local uniformizer}, & v = \varphi \end{cases}$

for the open subgp $U = N_{K/k}(C_K) \subset C_k$.

Thus we get a 1:1 correspondence

$$\{\text{open subgps of } C_k\} \overset{1:1}{\longleftrightarrow} \{\text{finite abelian ext}^s \text{ of } k\}$$

$$U = N_{K/k}(C_K) \longleftrightarrow K/k$$

Note: We no longer need to fix a modulus!

6. Local CFT

Let k still be a # field.

For a finite place $v = \wp$ consider the inclusion

$$k_\wp \hookrightarrow \mathbb{I}_k, \quad a \mapsto (x_v) \text{ w/ } x_v := \begin{cases} a & \text{for } v = \wp \\ 1 & \text{for } v \neq \wp \end{cases}$$

For K/k finite abelian we get

$$\begin{array}{ccc} k_\wp & & \\ \downarrow & \searrow & \\ \mathbb{I}_k & \xrightarrow[\text{Art}]{} & \mathrm{Gal}(K/k) \end{array}$$

Fact: This map has image in the decomposition gp $D_\wp \subset \mathrm{Gal}(K/k)$!

(For $\wp$ unramified in K/k, this is clear since $\mathrm{Art}(\pi_\wp) = \sigma_\wp \in D_\wp$ by def^n of the Frobenius. But it holds also for $\wp$ ramified in K/k.)

Fixing $\mathfrak{P} \in \mathrm{Spm}(\mathcal{O}_K)$ above $\wp$, we have

$$D_\wp = \{\sigma \in \mathrm{Gal}(K/k) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\} = \mathrm{Gal}(K_\mathfrak{P}/k_\wp).$$

Thus we get a diagram

$$\begin{array}{ccc} k_v^\times & \overset{\exists!}{\longrightarrow} & \mathrm{Gal}(K_\mathfrak{P}/k_\wp) \\ \downarrow & & \downarrow \\ \mathbb{I}_k & \xrightarrow{\mathrm{Art}_{K/k}} & \mathrm{Gal}(K/k) \end{array}$$

Now forget about our number field:

$k_\wp \rightsquigarrow$ a local field E

$K_\mathfrak{P} \rightsquigarrow$ a finite abelian extension F/E

Main thm of local CFT Let ϵ be a local field.

Then for any finite abelian extension F/ϵ

$\exists$ natural epi

$$\mathrm{Art}_{F/\epsilon} : \epsilon^\times = \langle \pi \rangle \times \mathcal{O}_\epsilon^\times \twoheadrightarrow \mathrm{Gal}(F/\epsilon)$$

which induces an iso

$$\mathrm{Art}_{F/\epsilon} : \epsilon^\times / N_{F/\epsilon}(F^\times) \xrightarrow{\sim} \mathrm{Gal}(F/\epsilon).$$

Rem In the limit we get an injection w/ dense image

$$\mathrm{Art}_\epsilon : \epsilon^\times \hookrightarrow \mathrm{Gal}(\epsilon^{ab}/\epsilon)$$

Note that Art_ϵ is NOT surjective:

$\langle \pi \rangle \simeq \mathbb{Z}$ but $\mathrm{Gal}(\epsilon^{ab,nr}/\epsilon) \simeq \hat{\mathbb{Z}}$ ...

Ex Quadratic extensions $F/\epsilon = \mathbb{Q}_p$ $(p \neq 2)$

$\updownarrow$ local CFT

Index 2 subgps $H = N_{F/\epsilon}(F^\times) \subset \epsilon^\times = \mathbb{Q}_p^\times$

Now:

- $\mathbb{Q}_p^\times \simeq \langle p \rangle \times \mathbb{Z}_p^\times \simeq \langle p \rangle \times U_1 \times \mathbb{F}_p^\times$

  w/ $U_1 = \{1 + p\alpha \mid \alpha \in \mathbb{Z}_p\} = \ker(\mathbb{Z}_p^\times \to \mathbb{F}_p^\times)$

  (note: the extension $1 \to U_1 \to \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \to 1$ splits since $\mathbb{F}_p^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \simeq \{\alpha \in \mathbb{Z}_p \mid \alpha^{p-1} = 1\}$)

  Hensel's lemma: All $(p-1)$st roots of unity lie in $\mathbb{Z}_p^\times$

- $U_1 = \{x^2 \mid x \in U_1\}$ by Hensel's lemma for $X^2 - (1+p\alpha)$ or binomial expansion of $(1+p\alpha)^{1/2}$

$$\Rightarrow \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \simeq \langle p \rangle / \langle p^2 \rangle \times \mathbb{F}_p^\times / \mathbb{F}_p^{\times 2}$$

$$\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$\Rightarrow$ $\exists$ precisely three subgps of index 2 in $\mathbb{Q}_p^\times$

& —— # —— quadratic extensions $F/\mathbb{Q}_p$:

a) $H = \langle p \rangle \cdot \mathbb{Q}_p^{\times 2} \longleftrightarrow F = \mathbb{Q}_p(\sqrt{p})$

b) $H = \langle a \rangle \cdot \mathbb{Q}_p^{\times 2} \longleftrightarrow F = \mathbb{Q}_p(\sqrt{a})$

w/ $a \in \mathbb{Z}_p$

$\bar{a} \in \mathbb{F}_p \setminus \mathbb{F}_p^2$

c) $H = \langle ap \rangle \times \mathbb{Q}_p^{\times 2} \longleftrightarrow F = \mathbb{Q}_p(\sqrt{ap})$

Group Cohomology

1. Abstract definition of gp cohomology

Let G be a gp.

Def A (left) **G-module** is an abelian gp A together w/ an action $\varrho : G \to \mathrm{Aut}(A)$.

We write

$g \cdot a := (\varrho(g))(a)$ for $g \in G$, $a \in A$.

A **morphism** between G-modules A, B is a group homom $f : A \to B$ sth

$f(g.a) = g \cdot f(a)$ for all $g \in G$, $a \in A$.

$\rightsquigarrow$ abelian category $\mathrm{Mod}(G)$ of G-modules, w/ morphisms

$\mathrm{Hom}_G(A,B) := \{ f : A \to B \text{ morph of } G\text{-mod} \}$.

We can view G-modules as modules over a ring:

Def The **group algebra** $\mathbb{Z}G$ is the ring given by

- the additive gp $(\mathbb{Z}G, +) := \bigoplus_{g \in G} \mathbb{Z}$,

  whose elements we write as formal sums

  $\sum_{g \in G} n_g \cdot g$ w/ $n_g \in \mathbb{Z}$ almost all zero.

- the multiplication

  $$\Big(\sum_{g \in G} n'_g \cdot g\Big)\Big(\sum_{h \in G} n''_h \cdot h\Big) := \sum_{a \in G} n_a \cdot a$$

  $$\text{w/ } n_a := \sum_{gh = a} n'_g n''_h$$

Then we have a natural equivalence

$$\mathrm{Mod}(G) \simeq \mathrm{Mod}(\mathbb{Z}[G])$$

$\rightsquigarrow$ can apply homological algebra over (non-commutative) rings!

Def For $A \in \mathrm{Mod}(G)$ consider the invariants

$$A^G := \{ a \in A \mid \forall g \in G : ga = a \} \subset A,$$

the maximal submodule w/ trivial G-action.

$\Rightarrow$ functor $(-)^G : \mathrm{Mod}(G) \to \mathrm{AbGps}$

which is left exact: For any short exact sequence $0 \to A \to B \to C \to 0$ in $\mathrm{Mod}(G)$, also

$$0 \to A^G \to B^G \to C^G \quad \text{is exact.}$$

Ex $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$

$$1 \to \{\pm 1\} \to \mathbb{C}^\times \xrightarrow{z \mapsto z^2} \mathbb{C}^\times \to 1 \qquad \text{exact in } \mathrm{Mod}(G)$$

Take G-invariants:

$$1 \to \{\pm 1\} \to \mathbb{R}^\times \to \mathbb{R}^\times$$

↑ no longer surjective!

Salvage exactness via derived functors:

- Recall a G-module I is injective if $\mathrm{Hom}_G(-, I)$ is exact, ie. if $\forall$ embedding $A \hookrightarrow B$ in $\mathrm{Mod}(G)$ the map $\mathrm{Hom}_G(B) \twoheadrightarrow \mathrm{Hom}_G(A)$ is surjective.

- Exercise: $\mathrm{Mod}(G)$ has enough injectives, ie. every G-module A embeds in an injective one.

  $\Rightarrow \exists$ injective resolution $A \to I_\bullet$, ie an exact sequence $1 \to A \xrightarrow{i} I_0 \to I_1 \to I_2 \to \cdots$ w/ $I_k \in \mathrm{Mod}(G)$ injective for all k.

- Take invariants:

  $$I_0^G \xrightarrow{d_0} I_1^G \xrightarrow{d_1} I_2^G \to \cdots \quad \text{(no longer exact!)}$$

- Define

  $$H^i(G, A) := \frac{\ker(d_i)}{\mathrm{im}(d_{i-1})}$$

Given another G-module B w/ an injres $B \to J_\bullet$,

any $f \in \mathrm{Hom}_G(A, B)$ extends to a morphism of

resolutions:

$$\begin{array}{ccccccccc} 0 & \to & A & \to & I_0 & \to & I_1 & \to & I_2 & \to & \cdots \\ & & f \downarrow & & \exists f_0 \downarrow & & \exists f_1 \downarrow & & \exists f_2 \downarrow & & \\ 0 & \to & B & \to & J_0 & \to & J_1 & \to & J_2 & \to & \cdots \end{array}$$

Lemma The induced maps $f_*: H^i(G, A) \to H^i(G, B)$

only depend on f (not on $f_0, f_1, \ldots$).

Pf. Enough to show $f = 0$ implies $f_* = 0$.

For this show that for $f = 0$ $\exists$ "chain homotopy" $h_\bullet$

w/ $f_i = h_i \circ d_i + d_{i-1} \circ h_{i-1}$:

$$\begin{array}{ccccccccc} 0 & \to & A & \to & I_0 & \to & I_1 & \to & I_2 & \to & \cdots \\ & & f=0 \downarrow & & f_0 \downarrow & \swarrow h_0 & f_1 \downarrow & \swarrow h_1 & f_2 \downarrow & \swarrow h_2 & \\ 0 & \to & B & \to & J_0 & \to & J_1 & \to & J_2 & \to & \cdots \end{array}$$

$\Rightarrow f_*: H^i(G, A) \to H^i(G, B)$ the zero map. □

$\Rightarrow H^i(G, A)$ independent of chosen resolution

& we get functors $H^i(G, -): \mathrm{Mod}(G) \to \mathrm{AbGps}$

sth for $i = 0$, we have $H^0(G, -) = (-)^G$.

This salvages the failure of right exactness:

Lemma For any short exact seq $0 \to A \to B \to C \to 0$

in $\mathrm{Mod}(G)$, we get a long exact sequence

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

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

$$\to H^2(G, A) \to \cdots$$

Pf. Exercise, using the snake lemma. □

2. Description via cocycles

We have $(-)^G = \mathrm{Hom}_{\mathbb{Z}G}(\mathbb{Z}, -)$ (with trivial G-action)

hence

$$H^i(G, -) = \mathrm{Ext}^i_{\mathbb{Z}G}(\mathbb{Z}, -)$$

$\Rightarrow$ can compute $H^i(G, A) = \mathrm{Ext}^i_{\mathbb{Z}G}(\mathbb{Z}, A)$

not only via an injective resolution $A \to I_\bullet$,

but also via a projective (e.g. free) resolution $P_\bullet \to \mathbb{Z}$:

Given an exact sequence $\cdots \to P_2 \to P_1 \to P_0 \to \mathbb{Z} \to 0$

w/ $P_i \simeq (\mathbb{Z}G)^{n_i}$ free $\mathbb{Z}G$-module, we have

$$H^i(G, A) \simeq H^i(C^\bullet) \quad \text{w/} \quad C^\bullet := \mathrm{Hom}_{\mathbb{Z}G}(P_\bullet, A).$$

This can be taken as a quick (cheating) definition of gp cohomology. It makes functoriality obvious and is computable since $\exists$ nice resolut^n $P_\bullet \to \mathbb{Z}$!

Def The bar resolution $\cdots \to X_2 \xrightarrow{d_2} X_1 \xrightarrow{d_1} X_0 \xrightarrow{\varepsilon} \mathbb{Z}$

is given by the free $\mathbb{Z}G$-modules

$$X_0 := \mathbb{Z}G$$

$$X_k := \bigoplus_{(g_1,\dots,g_k) \in G^k} \mathbb{Z}G \cdot \underbrace{(g_1, \dots, g_k)}_{\text{formal basis vector}} \quad \text{for } k > 0$$

& the morphisms

$$\varepsilon = d_0 : \quad X_0 = \mathbb{Z}G \longrightarrow \mathbb{Z} \qquad \text{"augmentation"}$$
$$\sum_g n_g \cdot g \longmapsto \sum_g n_g$$

$$d_1 : X_1 = \bigoplus_{g \in G} \mathbb{Z}G \cdot (g) \longrightarrow X_0 = \mathbb{Z}G$$
$$(g) \longmapsto g^{-1}$$

$$d_k : X_k \longrightarrow X_{k-1}$$
$$(g_1, \dots, g_k) \longmapsto g_1 \cdot (g_2, \dots, g_k)$$
$$+ \sum_{i=1}^{k-1} (-1)^i \cdot (g_1, \dots, g_{i-1}, g_i g_{i+1}, g_{i+2}, \dots, g_k)$$
$$+ (-1)^k \cdot (g_1, \dots, g_{k-1}).$$

Lemma $X_\bullet \to \mathbb{Z}$ is a resolution in $\mathrm{Mod}(G)$.

Pf. The maps ε and d_k are G-linear,

and clearly $X_\bullet \to \mathbb{Z}$ is a cplex, ie $d_k \circ d_{k+1} = 0 \ \forall k$.

To see exactness we show the cplex has no cohomology.

Define a homotopy $h_\bullet$ by the $\mathbb{Z}$-homomorphisms

$h_{-1} : \mathbb{Z} \to X_0, \quad 1 \mapsto 1$

$h_0 : X_0 \to X_1, \quad g \mapsto (g)$

$h_k : X_k \to X_{k+1}, \quad g\cdot(g_1,\dots,g_k) \mapsto (g, g_1, \dots, g_k)$

$\Rightarrow \quad h_{k-1} \circ d_k + d_{k+1} \circ h_k = id \quad \forall k$

$\Rightarrow \quad 0 = id \text{ on } H^k(X_\bullet \to \mathbb{Z})$

$\Rightarrow \quad H^k(X_\bullet \to \mathbb{Z}) = 0$ □

Thus

$$H^k(G, A) = H^k(\mathrm{Hom}_{\mathbb{Z}G}(X_\bullet, A)).$$

Concretely:

X_q free $\mathbb{Z}G$-module on the set G^q

$$\mathrm{Hom}_G(X_q, A) \simeq \mathrm{Maps}(G^q, A) =: A_q$$

Elements $f \in A_q$ are maps $f : G^q \to A$, and

$\mathrm{Hom}_{\mathbb{Z}G}(X_\bullet, A) \simeq$

$$\left[\cdots \to A_{q-1} \xrightarrow{\partial_q} A_q \xrightarrow{\partial_{q+1}} A_{q+1} \xrightarrow{\partial_{q+2}} \cdots \right]$$

has differentials

$\partial_1 : A_0 := A \to A_1 = \mathrm{Maps}(G, A)$

$$(\partial_1 a)(g) := g\cdot a - a$$

$\partial_q : A_{q-1} \to A_q = \mathrm{Maps}(G^q, A)$

$$(\partial_q f)(g_1,\dots,g_q) := g_1 \cdot f(g_2,\dots,g_q) + \sum_{i=1}^{q-1} (-1)^i f(g_1,\dots,g_i g_{i+1},\dots,g_q) + (-1)^q \cdot f(g_1,\dots,g_{q-1}).$$

Def $Z_q := Z_q(G,A) := \ker(\partial_{q+1})$ "q-cocycles"
$\cup$
$B_q := B_q(G,A) := \operatorname{im}(\partial_q)$ "q-coboundaries"

$\Rightarrow H^q(G,A) = Z_q / B_q$.

3. Examples in low degree

Clearly $H^0(G,A) = Z^0(G,A)$ (by def" $B^0 := 0$)
$= \ker(\partial_1 : A \to A_1,\ a \mapsto (g \mapsto ga - a)) = A^G$

3a) $H^1(G,A)$ & torsors

$(\partial_1 f)(g,h) = g \cdot f(h) - f(gh) + f(g)$

$\Rightarrow Z^1(G,A) = \{ f : G \to A$ sth
$f(gh) = gf(h) + f(g) \quad \forall g,h \in G \}$
↑
"crossed homomorphisms"

$B^1(G,A) = \{ f : G \to A \mid \exists a \in A\ \forall g \in G : f(g) = ga - g \}$

(note that $B^1 \subset Z^1$: $gha - a = g(ha-a) + (ga-a)$)

Special case: If G acts trivially on A,
then $H^1(G,A) = \operatorname{Hom}(G,A)$.

For the general case we need:

Def Let $A \in \operatorname{Mod}(G)$.

A torsor over A is a set $P \neq \emptyset$ w/

- a simply transitive action $+ : A \times P \to P$
  ↳ ie. $\forall p \in P$ get a bijection" $A \xrightarrow{\sim} P$, $a \mapsto a+p$
- a compatible action $\cdot : G \times P \to P$
  ↳ i.e. $g(a+p) = ga + gp \quad \forall g \in G, a \in A, p \in P$.

An isomorphism $P \simeq Q$ between such torsors is a bijection equivariant for the actions of A and G.

Ex
- A is a torsor over itself, the "trivial torsor"
- $P \simeq A \iff P^G \neq \emptyset$, ie $\exists \sigma \in P\ \forall g \in G : g\sigma = \sigma$

(given $\varphi : A \xrightarrow{\sim} P$ put $\sigma := \varphi(0)$ w/ the zero $0 \in A$;
given $\sigma \in P^G$ define $\varphi : A \xrightarrow{\sim} P$ by $a \mapsto a + \sigma$)

Ex E elliptic curve over k

By an E-torsor we mean a smooth proj curve C w/ an algebraic gp action $E \times C \to C$ over k that is simply transitive on points over $\bar{k}$.

Put

$G := \mathrm{Gal}(\bar{k}/k)$

$A := E(\bar{k}) \in \mathrm{Mod}(G)$

$\Rightarrow P := C(\bar{k})$ is a torsor over A.

We have:

P trivial torsor $\iff P^G \neq \emptyset$

$\iff C(k) \neq \emptyset$

$\iff \exists$ iso $E \xrightarrow{\sim} C$ over k

(use action $E \times C \to C$ & restrict to $E \times \mathrm{Spec}\, k \to C$ for a pt $\mathrm{Spec}\, k \to C$)

Slogan An E-torsor is a "form" of E/k w/ E-action. It is trivial iff it has a k-rational point.

Back to the general case:

Lemma For any $A \in \mathrm{Mod}(G)$, we have

$$H^1(G, A) \xrightarrow{\sim} \{\text{torsors over } A\}/\simeq$$

Pf. "$\leftarrow$":

Given a torsor P over A, pick any $p \in P$.

For $g \in G$ $\exists!\, a \in A$: $gp = a + p$ (since A acts simply trans on P)

We write $a = gp - p$.

Define $f_p : G \to A$, $g \mapsto gp - p$

- $f_p \in Z^1(G, A)$:

  $f_p(gh) = ghp - p = \cdots = g f_p(h) + f_p(g)$.

- For any other pt $q \in P$, say $q = a + p$ w/ $a \in A$,

  $(f_p - f_q)(g) = ga - a \underset{a \in A}{\Rightarrow} f_p - f_q \in B^1(G, A)$

$\Rightarrow [f_p] \in H^1(G, A)$ only depends on P, not on p.

"$\to$":

Given $f \in Z^1(G,A)$, define

- $P := A$ as a set
- $+ : A \times P \to P$ addition in the ab gp A
- $\cdot : G \times P \to P$,

$$g \cdot (a + p_0) := g \cdot a + f(g)$$ for any chosen reference point $p_0 \in P$

Check that this gives a torsor over A,
modifying f by a coboundary gives an isomorphic torsor,
& this gives mutually inverse bijections

$$H^1(G,A) \rightleftarrows \{\text{torsors over } A\}/\simeq \qquad \square$$

Ex E elliptic curve / number field k
then (see e.g. Silverman, Chapter X):

$$H^1(\mathrm{Gal}(\bar{k}/k), E(\bar{k})) \simeq \{E\text{-torsors}\}/\simeq$$

↑
We're cheating: $G := \mathrm{Gal}(\bar{k}/k)$ is a top gp w/ the profinite topology & its action is continuous wrt the discrete topology on $A := E(\bar{k})$. Here $H^1(G,A)$ is to be defined using only continuous 1-cocycles $f : G \to A$, not all 1-cocycles!

36) $H^2(G,A)$ & extensions

Def An extension of G by A is a short exact sequence

$$1 \to A \xrightarrow{i} E \xrightarrow{p} G \to 1$$

of groups (where E may be nonabelian)
sth the conjugation action $E \to \mathrm{Aut}(A)$
$e \mapsto (e(-)e^{-1})$
induces the given action of G on $M \in \mathrm{Mod}(G)$.

We say two such extensions (E_ν, i_ν, p_ν) are isomorphic if $\exists\, \varphi : E_1 \to E_2$ making the diagram below commutative:

$$\begin{array}{ccccccccc} 1 & \to & A & \xrightarrow{i_1} & E_1 & \xrightarrow{p_1} & G & \to & 1 \\ & & \| & & \downarrow \varphi & & \| & & \\ 1 & \to & A & \xrightarrow{i_2} & E_2 & \xrightarrow{p_2} & G & \to & 1 \end{array}$$

Ex For any $A \in \mathrm{Mod}(G)$, consider the semidirect product $\in = A \rtimes G$:

As a set $\in = A \times G$, but the gp structure is defined by

$$(a_1, g_1) \cdot (a_2, g_2) := (a_1 + g_1 a_2,\ g_1 g_2).$$

[e.g. affine transformations of the real line are given by $(\mathbb{R}, +) \rtimes \mathbb{R}^* \ni (a, c) \widehat{=} (x \mapsto a + cx)$ since $a_1 + c_1(a_2 + c_2 x) = (a_1 + c_1 a_2) + c_1 c_2 x$.]

We have the "split extension"

$$1 \longrightarrow A \xrightarrow{i} A \rtimes G \xrightarrow{p} G \longrightarrow 1$$

w/ $i(a) := (a, 1)$ & $p(a, g) := g$.

Q How to describe non-split extensions?

Lemma $\exists$ natural bijection

$$H^2(G, A) \simeq \{\text{extensions of } G \text{ by } A\}/\simeq$$

Pf. "$\longleftarrow$"

Given an extension $1 \to A \xrightarrow{i} \in \xrightarrow{p} G \to 1$,

pick a map of sets $s: G \to \in$ with $p \circ s = \mathrm{id}$.

$$\Rightarrow \in = \bigsqcup_{g \in G} A \cdot s(g) \quad \text{coset decomposition}$$

$$= A \times G \quad \text{as a set.}$$

We know p is a homom.

$$\Rightarrow s(g)s(h) \in p^{-1}(gh) \quad \forall\, g, h \in G$$

$$\Rightarrow \exists\, c(g,h) \in A : \quad s(g)s(h) = c(g,h)\, s(gh).$$

$\Rightarrow$ $c: G^2 \to A$ sth gp law on $\in = A \times G$ is given by

$$(a, g) \cdot (b, h) = (a + gb + c(g,h),\ gh). \qquad (*)$$

(more precisely:

$a \cdot s(g) \cdot b \cdot s(h)$

$= a \cdot \underbrace{s(g)\, b\, s(g)^{-1}}_{\text{conjugation in } \in} \cdot s(g)s(h) = \underbrace{a \cdot gb \cdot c(g,h)}_{\text{the factors are in } A \subset \in,\ \text{so pass to additive notation}} \cdot s(gh)$)

$\widehat{=}$ action $b \mapsto gb$ of the G-module A

Associativity of the gp law $(*)$ amounts to:

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

ie we get a 2-cocycle $c \in Z^2(G, A)$.

One can check its class $[c] \in H^2(G,A)$ is independent of the chosen section $s: G \to \in$.

"$\to$" : Exercise – check that for $c \in Z^2(G,A)$, formula $(*)$ defines a gp structure on $A \times G$ etc. $\square$

4. Homology & Tate cohomology

Recall For $A \in \mathrm{Mod}(G)$ we have:

a) Invariants:

$$A^G := \{a \in A \mid \forall g \in G : ga = a\} \subset A,$$

maximal submodule w/ trivial G-action.

b) Dually have coinvariants:

$$A_G := A / \langle g \cdot a - a \mid g \in G,\ a \in A \rangle,$$

maximal quotient w/ trivial G-action.

Get:

a) $(-)^G = \mathrm{Hom}_G(\mathbb{Z}, -) : \mathrm{Mod}(G) \to \mathrm{AbGps}$ left exact

$\rightsquigarrow H^i(G,-) := \mathrm{Ext}^i_{\mathbb{Z}G}(\mathbb{Z}, -) = H^i(\mathrm{Hom}_G(X_\bullet, -))$ for a $\mathbb{Z}G$-proj (e.g. free) res $\cdots \to X_1 \to X_0 \to \mathbb{Z} \to 0$

b) $(-)_G = \mathbb{Z} \otimes_{\mathbb{Z}G} (-) : \mathrm{Mod}(G) \to \mathrm{AbGps}$ right exact (trivial RIGHT $\mathbb{Z}G$-module)

$\rightsquigarrow H_i(G,-) := \mathrm{Tor}_i^{\mathbb{Z}G}(\mathbb{Z}, -) = H^{-i}(Y_\bullet \otimes_{\mathbb{Z}G} (-))$ for a $(\mathbb{Z}G)^{op}$-flat (e.g. free) res $\cdots \to Y_1 \to Y_0 \to \mathbb{Z} \to 0$.

↳ ie resolut^n by RIGHT $\mathbb{Z}G$-modules Y_i

Ex a) By construction $H_0(G,A) = A_G = A/I_G A$ for the augmentation ideal

$$I_G := \ker\left(\mathbb{Z}G \to \mathbb{Z},\ \sum_g n_g \cdot g \mapsto \sum_g n_g\right) \trianglelefteq \mathbb{Z}G.$$

b) Free modules $A \simeq (\mathbb{Z}G)^{\oplus n}$ have $H_i(G,A) = 0\ \forall i > 0$

c) $H_1(G,\mathbb{Z}) \simeq G^{ab}$ ("Hurewicz thm")

Pf of c) $0 \to I_G \to \mathbb{Z}G \to \mathbb{Z} \to 0$ exact

$$\Rightarrow \underbrace{H_1(G,\mathbb{Z}G)}_{=0} \to H_1(G,\mathbb{Z}) \to \underbrace{H_0(G,I_G)}_{= I_G/I_G^2} \to \underbrace{H_0(G,\mathbb{Z}G)}_{= \mathbb{Z}G/I_G}$$

$$\Rightarrow H_1(G,\mathbb{Z}) \simeq I_G/I_G^2$$

Now consider $G \to I_G/I_G^2$, $g \mapsto g-1 \bmod I_G^2$. Since

$gh \mapsto gh-1 = (g-1)+(h-1)+(g-1)(h-1) \equiv (g-1)+(h-1) \bmod I_G^2$

we get a hom. $G^{ab} \to I_G/I_G^2$. Using $I_G = \bigoplus_{g \in G} \mathbb{Z}\cdot(g-1)$ as an abelian gp, one checks that we can define an inverse by $I_G/I_G^2 \to G^{ab}$, $g-1 \mapsto g$. □

From now on assume G is finite.

Apply duality to resolutions:

For any left $\mathbb{Z}G$-module M,
view $M^\vee := \mathrm{Hom}_{\mathbb{Z}}(M,\mathbb{Z})$ as a right $\mathbb{Z}G$-module
via $(\varphi \cdot g)(m) := \varphi(g \cdot m)$ for $m \in M$, $g \in G$, $\varphi \in M^\vee$.

$\rightsquigarrow$ $\mathrm{Mod}(\mathbb{Z}G) \to \mathrm{Mod}((\mathbb{Z}G)^{op})$, $M \mapsto M^\vee$ contravariant,
exact on modules that are free of finite rk over $\mathbb{Z}$.

Given a resolut^n by free left-$\mathbb{Z}G$-modules of finite rk

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

(we start labelling w/ X_{-1} since X_0 was already used...),
we get a resolut^n by free right-$\mathbb{Z}G$-modules

$$0 \leftarrow \mathbb{Z} \leftarrow Y_0 \leftarrow Y_{-1} \leftarrow \cdots \quad \text{w/} \quad Y_i := X_{i-1}^\vee$$

$$\Rightarrow H_i(G,A) = H^{-i}(Y_\bullet \otimes_{\mathbb{Z}G} A) = H^{-i-1}(\mathrm{Hom}_G(X_\bullet, A))$$

For any free $\mathbb{Z}G$-module X of finite rk,
we have $X^\vee \otimes_{\mathbb{Z}G} A \xrightarrow{\sim} \mathrm{Hom}_G(X,A)$ (exercise...)

Upshot This looks exactly like group cohomology,

except that $\cdots \to X_1 \to X_0 \to \mathbb{Z}$

is replaced by $\mathbb{Z} \to X_{-1} \to X_{-2} \to \cdots$

Can unite both:

Def By a complete resolution of the G-module $\mathbb{Z}$ we mean a commutative diagram in $\mathrm{Mod}(G)$

$$\cdots \leftarrow X_{-2} \leftarrow X_{-1} \longleftarrow X_0 \leftarrow X_1 \leftarrow X_2 \leftarrow$$
$$\nwarrow \quad \swarrow$$
$$\mathbb{Z}$$

that combines two exact sequences

a) $\cdots \to X_1 \to X_0 \to \mathbb{Z} \to 0$

b) $0 \to \mathbb{Z} \to X_{-1} \to X_{-2} \to \cdots$

We'll see complete resolutions exist & put

$X_\bullet := [\cdots \to X_1 \to X_0 \to X_{-1} \to \cdots]$

$H_T^i(G, A) := H^i(\mathrm{Hom}_G(X_\bullet, A))$

"Tate cohomology" – independent of chosen complete resolution (e.g. by formulas below, or by using more homological algebra)

Rem An explicit complete resolution can be obtained by taking the bar resolution $\cdots \to X_1 \to X_0 \to \mathbb{Z}$ and defining $\mathbb{Z} \to X_{-1} \to X_{-2} \to \cdots$ by applying $\mathrm{Hom}_{\mathbb{Z}}(-, \mathbb{Z}) : \mathrm{Mod}(G) \to \mathrm{Mod}(G)$, i.e.

$$X_{-i-1} := \mathrm{Hom}_{\mathbb{Z}}(X_i, \mathbb{Z}) \quad \forall i \geq 0$$

(w/ G-action $(g \cdot f)(x) := f(\bar{g}^{-1} x)$)

(exactness is preserved since all X_i are free $\mathbb{Z}$-modules)

$$\Rightarrow H_T^i(G, A) \simeq H^i(A_\bullet) \text{ for the cplex}$$

$$A_\bullet := [\cdots \to A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \xrightarrow{\partial_2} \cdots]$$

where

$$A_{-k-1} = A_k = \mathrm{Maps}(G^k, A) \quad \text{for } k \geq 0$$

identify free $\mathbb{Z}$-module of finite rk w/ its dual using the given basis

(we assume $|G| < \infty$ hence $\mathrm{rk}\, \mathbb{Z}G < \infty$)

(for $k = 0$ we let $A_{-1} = A_0 = \mathrm{Maps}(\mathrm{pt}, A) = A$)

$\Rightarrow$ By construction

$$H_T^i(G,A) = \begin{cases} H^i(G,A), & i > 0 \\ H_{-i-1}(G,A), & i < -1 \end{cases}$$

For the only "new cases" $i = -1, 0$ we have

$$\cdots \to A_{-2} \xrightarrow{\partial_{-1}} A_{-1} \xrightarrow{\partial_0} A_0 \xrightarrow{\partial_1} A_1 \to \cdots$$

$$\begin{array}{ccccccc} \| & & \| & & \| & & \| \\ \mathrm{Maps}(G,A) & \longrightarrow & A & \xrightarrow{N_G} & A & \longrightarrow & \mathrm{Maps}(G,A) \end{array}$$

w/ • $(\partial_1 a)(g) = ga - a$

• $\partial_0 a = N_G(a) := \sum_{g \in G} ga$

• $\partial_{-1} f = \sum_{g \in G} (g^{-1} \cdot f(g) - f(g))$ (*) (see next page)

$\Rightarrow$ $H_T^0(G,A) = A^G / N_G A$ "norm index gp"

$H_T^{-1}(G,A) = \ker(N_G) / I_G A$

Ex F/E finite Galois extension of fields, $G = \mathrm{Gal}(F/E)$

$\Rightarrow H_T^0(G, F^*) = E^* / N_{F/E}(F^*)$ ...that enters in local CFT!

Pf of (*): We have

$$X_1 = \bigoplus_{g \in G} \mathbb{Z}G \cdot e_g \qquad h \cdot e_g$$

$$d_1 \downarrow$$

$$X_0 = \mathbb{Z} \cdot e \ni h(g-1) \cdot e = (hg - h) \cdot e$$

w/ e_g, e : formal basis vectors

Dualize:

$$X_{-2} = \mathrm{Hom}_{\mathbb{Z}}(X_1, \mathbb{Z}) = \bigoplus_{g \in G} \mathbb{Z}G \cdot e_g^\vee$$

$$d_{-1} \uparrow$$

$$X_{-1} = \mathrm{Hom}_{\mathbb{Z}}(X_0, \mathbb{Z}) = \mathbb{Z}G \cdot e^\vee$$

w/ $e^\vee(h \cdot e) := \begin{cases} 1 & \text{if } h = 1 \\ 0 & \text{else} \end{cases}$

$e_g^\vee(h \cdot e_f) := \begin{cases} 1 & \text{if } h = 1,\ f = g \\ 0 & \text{else} \end{cases}$

Rem By def^n of the G-action on $\mathrm{Hom}_{\mathbb{Z}}(X_1, \mathbb{Z})$,

$(g^{-1} \cdot e_g^\vee)(h \cdot e_f) = e_g^\vee(gh \cdot e_f)$.

Thus

$$(\bar{g}^{-1}\cdot e^\vee_g - e^\vee_g)(h\cdot e_f) = \begin{cases} e^\vee(hg) - e^\vee(h), & f = g \\ 0, & f \neq g \end{cases}$$

$$= \begin{cases} e^\vee(d_1(h\cdot e_f)), & f = g \\ 0, & f \neq g. \end{cases}$$

$$\Rightarrow \quad d_{-1}(e^\vee) := e^\vee \circ d_1 = \sum_{g\in G} (\bar{g}^{-1}\cdot e_g - e_g)$$

Pass to $\mathrm{Hom}_G(X_\bullet, A) = A_\bullet$:

$$\begin{array}{ccc} A_{-2} = \mathrm{Hom}_G(X_{-2}, A) & \xrightarrow{\simeq} & \mathrm{Maps}(G, A) \\ \downarrow & & \\ A_{-1} = \mathrm{Hom}_G(X_{-1}, A) & \xrightarrow{\simeq} & A \end{array}$$

$$\begin{array}{ccc} \varphi & \longmapsto & f = (g \mapsto \varphi(e^\vee_g)) \\ \downarrow & & \downarrow \\ \varphi \circ d_{-1} & \longmapsto & \sum_{g\in G} (\bar{g}^{-1} f(g) - f(g)) \end{array}$$

(evaluate on $e^\vee$)

□

Lemma For any short exact sequence of G-modules $0 \to A \to B \to C \to 0$ we get a long exact sequence of Tate cohom.

$$\cdots \to H^i_T(G, A) \to H^i_T(G, B) \to H^i_T(G, C) \to H^{i+1}_T(G, A) \to H^{i+1}_T(G, B) \to \cdots$$

(infinite in both directions $i \to \pm\infty$)

Pf. Take a complete resolution $X_\bullet$.

All $X_i = (\mathbb{Z}G)^{n_i}$ are free $\mathbb{Z}G$-modules

$$\Rightarrow \quad 0 \to \mathrm{Hom}_G(X_\bullet, A) \to \mathrm{Hom}_G(X_\bullet, B) \to \mathrm{Hom}_G(X_\bullet, C) \to 0$$

still an exact sequence of complexes

(in degree i it is just $0 \to A^{n_i} \to B^{n_i} \to C^{n_i} \to 0$)

$\Rightarrow$ get long exact sequence after taking cohomology

(see eg Weibel p 13/14 : The argument works the same for cplexes infinite in both directions)

□

Alternative pf. The norm $N_A : A \to A^G$, $a \mapsto \sum_{g \in G} ga$ factors over a hom.

$$N_A : \quad A_G = H_0(G,A) \to A^G = H^0(G,A).$$

Long exact sequences in homology / cohomology give

$$\begin{array}{ccccccccccc}
\cdots \to & H_1(G,C) & \to & H_0(G,A) & \to & H_0(G,B) & \to & H_0(G,C) & \to 0 & \to \cdots \\
 & \downarrow & & \downarrow N & & \downarrow N & & \downarrow N & \downarrow & \\
\cdots \to & 0 & \to & H^0(G,A) & \to & H^0(G,B) & \to & H^0(G,C) & \to H^1(G,A) & \to \cdots
\end{array}$$

from which one gets the sequence in Tate cohomology. □

5. Example: Cyclic gps & the Herbrand quotient

The Tate coh. of finite cyclic gps is 2-periodic:

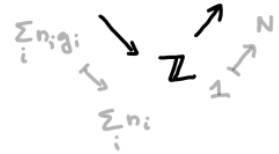
Prop Let G be a finite cyclic gp & $A \in \mathrm{Mod}(G)$, then

$$H_T^i(G,A) \simeq \begin{cases} H_T^0(G,A) = A^G/N_G(A) & \text{for } 2 \mid i \\ H_T^{-1}(G,A) = \ker(N_G)/I_G A & \text{for } 2 \nmid i. \end{cases}$$

Pf. Say $G = \langle g \rangle$ w/ $n \cdot g = 1$

Put $N := \sum_{g \in G} g \in \mathbb{Z}G$, then we have the complete resolution

$$X_\bullet = \Big[\cdots \xrightarrow{N} \mathbb{Z}G \xrightarrow{g-1} \mathbb{Z}G \xrightarrow{N} \mathbb{Z}G \xrightarrow{g-1} \mathbb{Z}G \xrightarrow{N} \cdots \Big]$$

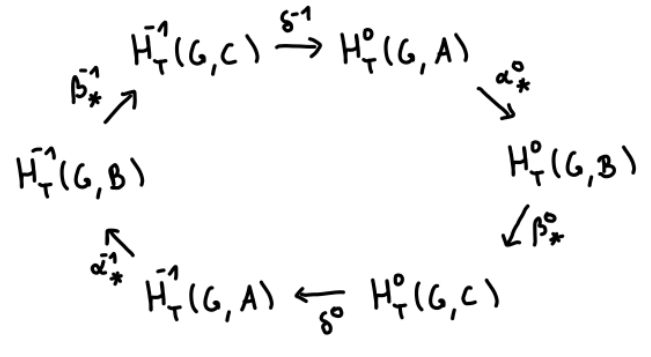


which is 2-periodic

$\Rightarrow H_T^i(G,A) = H^i(\mathrm{Hom}_{\mathbb{Z}}(X_\bullet, A))$ is 2-periodic. □

Rem
- Conversely, if G is any finite group sth $H_T^i(G,\mathbb{Z}) \simeq H_T^{i+2}(G,\mathbb{Z})$ for all i, then G must be cyclic since $G_{ab} \simeq H_T^{-2}(G,\mathbb{Z}) \simeq H_T^0(G,\mathbb{Z}) \simeq \mathbb{Z}/|G|$.
- $\exists$ finite nonabelian gps G w/ $H_T^\bullet(G,\mathbb{Z})$ periodic of period $d \neq 2$. But for G abelian this doesn't happen (see exercises).

Rem Let G be finite cyclic. Then for any exact sequence $0 \to A \xrightarrow{\alpha} B \xrightarrow{\beta} C \to 0$ of G-modules the long exact sequence gives an exact hexagon



The terms may still be hard to control, but there is a very useful invariant that's much easier to compute:

Def Let G be finite cyclic and $A \in \mathrm{Mod}(G)$. If $h^i(A) := \#\, H_T^i(G,A)$ is finite for $i = 0, -1$ (hence for all $i \in \mathbb{Z}$), we define the Herbrand quotient

$$h(A) := \frac{h^0(A)}{h^{-1}(A)} \left(= \frac{h^{2n}(A)}{h^{2n-1}(A)} \text{ for any } n \right) \in \mathbb{Q}$$

Morally, the Herbrand quotient can be seen as a kind of "Euler characteristic" even though there are infinitely many nonzero cohomology groups:

Cor Let G be finite cyclic & consider an exact sequence $0 \to A \to B \to C \to 0$ in $\mathrm{Mod}(G)$. If any two of $h(A), h(B), h(C)$ are defined, then so is the third and in that case

$$h(B) = h(A)h(C).$$

Pf. Use the exact hexagon

$$h^0(A) = |\ker \alpha_*^0| \cdot |\mathrm{im}\, \alpha_*^0| = |\ker \alpha_*^0| \cdot |\ker \beta_*^0| \text{ etc}$$

$$\Rightarrow h^0(A)h^0(C)h^{-1}(B) = \prod_{i=0,-1} |\ker \alpha_*^i| |\ker \beta_*^i| |\ker \delta^i|$$

$$= h^{-1}(A)h^{-1}(C)h^0(B)$$

If any two of $h(A), h(B), h(C)$ are defined, then four of the gps of the hexagon are finite & the other two are not adjacent, hence also finite. $\square$

Cor Let G be a finite cyclic gp & $A \in \mathrm{Mod}(G)$.

a) If $|A| < \infty$, then $h(A) = 1$.

b) More generally, for A finitely generated as an abelian gp we have

$$h(A) = h(A/A_{tors})$$

(A_{tors}: torsion subgp of A)

whenever either of the two is defined.

c) Trivial G-modules $A \simeq \mathbb{Z}^r \oplus \text{torsion}$ have $h(A) = |G|^r$.

d) Let $f : A \to B$ be a G-module hom w/ $\ker(f)$ & $\mathrm{cok}(f)$ finite. If one of $h(A), h(B)$ is defined, then so is the other and $h(A) = h(B)$.

Pf. a) Let $G = \langle g \rangle$.

Use $0 \to A^G \to A \xrightarrow{g-1} A \to A_G \to 0$

$$\Rightarrow |A^G| = |\ker(g-1)| = |\mathrm{cok}(g-1)| = |A_G|$$

$$\Rightarrow h^0(A) = |\ker(N_G)| / |\mathrm{im}(g-1)| \quad \text{w/ } N_G : A \to A$$

$$= |A| / |\mathrm{im}(N_G)| \cdot |\mathrm{im}(g-1)|$$

$$= |\ker(g-1)| / |\mathrm{im}(N_G)| = h^1(A)$$

$$\Rightarrow h(A) = 1$$

b) Use $0 \to A_{tors} \to A \to A/A_{tors} \to 0$ w/ $h(A_{tors}) = 1$ by a)

c) Use b) and $H^0_T(G, \mathbb{Z}) = \mathbb{Z}/|G|$, $H^{-1}_T(G, \mathbb{Z}) = \{0\}$ $\Rightarrow h(\mathbb{Z}) = |G|$

d) Use b) and $0 \to \ker f \to A \to \mathrm{im} f \to 0$, $0 \to \mathrm{im} f \to B \to \mathrm{cok} f \to 0$ □

6. Induced modules

For a subgp $H \subset G$ consider

$\mathrm{Res}^G_H := (-)|_H : \mathrm{Mod}\, G \to \mathrm{Mod}\, H$ restriction to $H \subset G$

Q: Left / right adjoint?

Def $\mathrm{Ind}^G_H := \mathbb{Z}G \otimes_{\mathbb{Z}H} (-) : \mathrm{Mod}\, H \to \mathrm{Mod}\, G$

$\mathrm{Coind}^G_H := \mathrm{Hom}_H(\mathbb{Z}G, -) : \mathrm{Mod}\, H \to \mathrm{Mod}\, G$

Explicitly, for $N \in \mathrm{Mod}\, H$:

- G acts on $\mathrm{Ind}_H^G N = \mathbb{Z}G \otimes_{\mathbb{Z}H} N$ via $g \cdot (g' \otimes n) = (gg') \otimes n$,

  so

  $$\mathrm{Ind}_H^G N = \bigoplus_{i \in I} g_i \otimes N \quad \text{for } G = \coprod_{i \in I} g_i \cdot H$$

  w/ $g \cdot (g_i \otimes n) := g_j \otimes (hn)$ for $gg_i = g_j h$.

- G acts on $\mathrm{Coind}_H^G(N) = \mathrm{Hom}_H(\mathbb{Z}G, N)$ via

  $(g \cdot f)(x) := f(xg)$ for $g \in G$, $f \in \mathrm{Hom}_H(\mathbb{Z}G, N)$,

  so

  $$\mathrm{Coind}_H^G N = \mathrm{Hom}_H\Big(\bigoplus_{i \in I} \mathbb{Z}H \cdot g_i^{-1}, N\Big) \simeq \prod_{i \in I} g_i \otimes N$$

  $$\sum_{i \in I} (g_i^{-1} \mapsto n_i) \longleftarrow\!\shortmid (g_i \otimes n_i)_{i \in I}$$

  where

  $$(g_i^{-1} \mapsto n_i)(x) := \begin{cases} h \cdot n_i & \text{if } x = h \cdot g_i^{-1} \quad (h \in H) \\ 0 & \text{if } x \notin H \cdot g_i^{-1} \end{cases}$$

Rem The iso $\varphi : \mathrm{Coind}_H^G(N) \xrightarrow{\sim} \prod_{i \in I} g_i \otimes N$ is $\mathbb{Z}G$-linear for the G-action on the target given by

$$g \cdot (g_i \otimes n_i) := (g_j \otimes h_i n_i) \text{ for } gg_i = g_j h_i \quad (j = j(i)).$$

(in i-th component; in j-th component)

Pf.

$$\begin{aligned}
(g \cdot (g_i^{-1} \mapsto n_i))(x) &= (g_i^{-1} \mapsto n_i)(xg) \\
&= \begin{cases} hn_i & \text{if } xg = h \cdot g_i^{-1} \\ 0 & \text{if } xg \notin H \cdot g_i^{-1} \end{cases} \\
&= \begin{cases} hn_i & \text{if } x = h \cdot (gg_i)^{-1} = hh_i^{-1} \cdot g_j^{-1} \\ 0 & \text{if } x \notin H \cdot g_j^{-1} \end{cases} \\
&= \begin{cases} hh_i^{-1} \cdot h_i n_i & \text{if } x = hh_i^{-1} \cdot g_j^{-1} \\ 0 & \text{if } x \notin H \cdot g_j^{-1} \end{cases} \\
&= (g_j^{-1} \mapsto h_i n_i)(x) \\
&= \varphi^{-1}(g \cdot (g_i \otimes n_i))
\end{aligned}$$

($g \cdot$: action on $\mathrm{Coind}_H^G(N)$; action on $\prod_i g_i \otimes N$)

□

Cor $\exists$ embedding of G-modules

$$\mathrm{Ind}_H^G(N) \hookrightarrow \mathrm{Coind}_H^G(N)$$

which is an iso iff $[G:H] < \infty$.

Pf. This is just $\bigoplus_{i\in I} g_i \otimes N \hookrightarrow \prod_{i\in I} g_i \otimes N$. $\square$

Prop ("Frobenius reciprocity") $\exists$ natural iso

a) $\mathrm{Hom}_G(\mathrm{Ind}_H^G N, M) \simeq \mathrm{Hom}_H(N, M|_H)$,

b) $\mathrm{Hom}_G(M, \mathrm{Coind}_H^G N) \simeq \mathrm{Hom}_H(M|_H, N)$.

Pf. For any ring hom. $R \to S$ & $M \in \mathrm{Mod}\, S$, $N \in \mathrm{Mod}\, R$ we have

$$\mathrm{Hom}_S(S \otimes_R N, M) \simeq \mathrm{Hom}_R(N, M|_R)$$

$$\mathrm{Hom}_S(M, \mathrm{Hom}_R(S, N)) \simeq \mathrm{Hom}_R(M|_R, N).$$ $\square$

Here $\mathrm{id} \in \mathrm{Hom}_H(M|_H, M|_H)$ corresponds to the adjunction maps

- $\alpha_M : \mathrm{Ind}_H^G(M|_H) = \mathbb{Z}G \otimes_{\mathbb{Z}H} M|_H \longrightarrow M$

  $g \otimes m \longmapsto g \cdot m$.

- $\beta_M : M \longrightarrow \mathrm{Coind}_H^G(M|_H) \simeq \prod_{i\in I} g_i \otimes M|_H$

  $m \longmapsto (g_i \otimes (g_i^{-1} \cdot m))_{i\in I}$

Since we'll be interested in Tate cohomology, let's from now on assume G is finite.

$\Rightarrow \mathrm{Ind}_H^G(-) \simeq \mathrm{Coind}_H^G(-)$

both left and right adjoint to $(-)|_H$

Cor (Shapiro's lemma) $\exists$ natural iso

- $H^i(G, \mathrm{Ind}_H^G N) \xrightarrow{\sim} H^i(H, N) \quad \forall i \geq 0$
- $H_T^i(G, \mathrm{Ind}_H^G N) \xrightarrow{\sim} H_T^i(H, N) \quad \forall i \in \mathbb{Z}$

Pf. Use $\mathrm{Hom}_G(X_\bullet, \mathrm{Ind}_H^G N) \simeq \mathrm{Hom}_H(X_\bullet|_H, N)$. □

(complete) $\mathbb{Z}G$-free resolut^n — still exact w/ $\mathbb{Z}H$-free terms of rk $< \infty$

Let's apply this for $H = \{1\}$:

Def $M \in \mathrm{Mod}(G)$ is called an *induced module*
if $\exists$ ab gp N sth $M \simeq \mathbb{Z}G \otimes_{\mathbb{Z}} N = \mathrm{Ind}_1^G N$.

Cor Any induced module M satisfies

a) $H^i(G, M) = 0 \quad \forall i > 0$, ← in general not for $i = 0$. that's why Tate cohom. is nicer (like reduced cohom. in topology)!

b) $H_T^i(G, M) = 0 \quad \forall i \in \mathbb{Z}$.

Pf. Shapiro's lemma w/ $H^i(\{1\}, -) = 0 \ \forall i > 0$,
$H_T^i(\{1\}, -) = 0 \ \forall i \in \mathbb{Z}$. □

Ex a) Free $\mathbb{Z}G$-modules are induced

b) If $M \in \mathrm{Mod}(G)$ is induced, then

i) $M \otimes_{\mathbb{Z}} A \in \mathrm{Mod}(G)$ is induced $\forall A \in \mathrm{Mod}(G)$.

ii) $M|_H \in \mathrm{Mod}(H)$ is induced $\forall$ subgp $H \subset G$.

Pf of b) i) $M = \mathrm{Ind}_1^G N = \bigoplus_{g \in G} gN$

$$\Rightarrow M \otimes A = \bigoplus_g (gN) \otimes A$$
$$\simeq \bigoplus_g gN \otimes gA$$
$$= \bigoplus_g g(N \otimes A) = \mathrm{Ind}_1^G (N \otimes A).$$

ii) $M = \bigoplus_{g \in G} gN, \qquad G = \bigsqcup_{i \in I} Hg_i$

$$\Rightarrow M|_H = \bigoplus_{h \in H} \bigoplus_{i \in I} hg_i N = \bigoplus_{h \in H} h \cdot \left(\bigoplus_{i \in I} g_i N\right)$$
$$= \mathrm{Ind}_1^H \left(\bigoplus_{i \in I} g_i N\right).$$ □

Ex ("dimension shifting")

Have exact sequences

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

$$0 \to \mathbb{Z} \xrightarrow{N} \mathbb{Z}G \to \mathfrak{J}_G \to 0 \quad \text{for } G \text{ finite}$$

w/ $I_G = \langle g-1 \mid g \in G \rangle$ & $\mathfrak{J}_G = \mathbb{Z}G/\mathbb{Z}G \cdot N$

$(N := \sum_{g \in G} g)$

Since $\mathbb{Z}G \otimes_{\mathbb{Z}} A$ is induced for any $A \in \mathrm{Mod}(G)$,

we get for all $i \in \mathbb{Z}$:

$$\delta : H_T^{i-1}(G, A) \xrightarrow{\sim} H_T^i(G, I_G \otimes A)$$

$$\delta : H_T^i(G, \mathfrak{J}_G \otimes A) \xrightarrow{\sim} H_T^{i+1}(G, A)$$

Iterating this we get for all $m \in \mathbb{Z}$:

$$\delta^m : H_T^i(G, A[m]) \xrightarrow{\sim} H_T^{i+m}(G, A)$$

where

$$A[m] := \begin{cases} \mathfrak{J}_G^{\otimes m} \otimes A, & m \geq 0 \\ I_G^{\otimes |m|} \otimes A, & m < 0 \end{cases}$$

Ex Let $n = |G|$

Then for any $A \in \mathrm{Mod}(G)$,

we have $\quad n \cdot H_T^i(G, A) = 0 \quad \forall\, i \in \mathbb{Z}$.

Pf. Dimension shifting: $H_T^0(G, A[i]) \simeq H_T^i(G, A)$

$\Rightarrow$ Replacing A by $A[i]$, only need to discuss $H_T^0(G, -)$.

But $H_T^0(G, A) = A^G/N_G(A)$ is killed by n,

since $n \cdot a = N_G(a)$ for $a \in A^G$. □

Ex If $A \in \mathrm{Mod}(G)$ is uniquely divisible,

ie $\forall n \in \mathbb{N}$: $A \xrightarrow{\sim} A$, $a \mapsto n.a$ is an iso,

then $\quad H_T^i(H, A|_H) = 0$

for all i & all subgroups $H \subset G$.

Pf. Take $n = |H|$ in the previous example. □

7. Restriction & Inflation

$H \subset G$ a subgp of a gp G

$A \in \mathrm{Mod}(G)$

$\Rightarrow$ embedding $A^G \hookrightarrow A^H$

$\| \qquad\qquad \|$

$H^0(G,A) \qquad H^0(H,A)$

This gives a morphism of functors

$$(-)^G \to (-)^H : \mathrm{Mod}(G) \to \mathrm{AbGps}.$$

Def The induced morphism on derived functors is called the restriction

$$\mathrm{res}^i : H^i(G,-) \longrightarrow H^i(H,-).$$

Explicitly it is given by restriction of cochains:

$$\begin{array}{ccc} H^i(G,A) = H^i(A_0 \to A_1 \to \cdots) & \text{w/ } A_i := \mathrm{Maps}(G^i, A) \\ \mathrm{res}^i \downarrow & \downarrow (-)|_{H^i} \\ H^i(H,A) = H^i(A|_{H,0} \to A|_{H,1} \to \cdots) & \text{w/ } A|_{H,i} := \mathrm{Maps}(H^i, A) \end{array}$$

If $H \trianglelefteq G$ is normal, we can also pass to $Q := G/H$:

Then $B := A^H \in \mathrm{Mod}(G/H)$ and we have a map between the bar resolutions

$$\begin{array}{ccc} B_\bullet = [B_0 \to B_1 \to \cdots] \\ \downarrow \\ A_\bullet = [A_0 \to A_1 \to \cdots] \end{array}$$

given by

$$\begin{array}{ccc} B_i := \mathrm{Maps}(Q^i, B) & \ni & f \\ \downarrow & & \downarrow \\ A_i := \mathrm{Maps}(G^i, A) & \ni & \iota \circ f \circ p \end{array}$$

$$\iota \circ f \circ p : G^i \xrightarrow{p} Q^i \xrightarrow{f} B \xrightarrow{\iota} A.$$

Def The induced map on cohomology is called the inflation

$$H^i(G/H, A^H) = H^i(B_\bullet) \to H^i(A_\bullet) = H^i(G,A).$$

Lemma ("inflation-restriction sequence")

For $H \trianglelefteq G$ normal & $A \in \mathrm{Mod}(G)$, the following sequence is exact:

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

Pf 1 (by hand):

- inf injective: Let $f \in Z^1(G/H, A^H)$

$$\begin{aligned} \inf(f) = 0 &\Rightarrow \exists\, a \in A\ \forall g \in G: f(gH) = ga - a \\ &\Rightarrow gha - a = ga - a \text{ for all } g \in G, h \in H \\ &\Rightarrow ha - a = 0 \text{ for all } h \in H \ (\text{take } g = 1) \\ &\Rightarrow a \in A^H \text{ \& hence } f \in B^1(G/H, A^H) \end{aligned}$$

- $\mathrm{im}(\inf) \subset \ker(\mathrm{res})$ clear as $H \hookrightarrow G \twoheadrightarrow G/H$ (trivial)
- $\ker(\mathrm{res}) \subset \mathrm{im}(\inf)$:

Let $f \in Z^1(G,A)$ w/ $\mathrm{res}(f) = 0$

$\Rightarrow \exists\, a \in A\ \forall h \in H: f(h) = h \cdot a - a$

Subtract $\delta(a) \in B^1(G,A)$ from f $\Rightarrow$ wlog $f(h) = 0$ $\forall h \in H$

$\Rightarrow$ f factors over a map $\bar{f}: G/H \to A$

(use that $f(gh) = f(g) + g f(h)$)

Moreover $\bar{f}(gH) \in A^H$ as $f(hg) = f(h) + hf(g)$, with $f(hg) = f(g)$ and $f(h) = 0$ □

In fact we have:

Prop (Hochschild-Serre) $\exists$ spectral sequence

$$E_2^{p,q}: \quad H^p(G/H, H^q(H,A)) \Rightarrow H^{p+q}(G,A)$$

Pf.

$$\begin{array}{ccc} \mathrm{Mod}(G) & \xrightarrow{F := (-)^G} & \mathrm{AbGps} \\ & F_1 := (-)^H \searrow \quad \nearrow F_2 := (-)^{G/H} & \\ & \mathrm{Mod}(G/H) & \end{array}$$

F_1 sends injectives to injectives:

$$\begin{aligned} \mathrm{Hom}_{G/H}(-, F_1(I)) &= \mathrm{Hom}_{G/H}(-, I^H) \\ &= \mathrm{Hom}_G(p^*(-), I) \end{aligned}$$

is exact for I injective since $p^*: \mathrm{Mod}\, G/I \to \mathrm{Mod}\, G$ is exact.

$\Rightarrow$ Grothendieck spectral sequence:

$$\underbrace{R^pF_2}_{H^p(G/H,-)} \circ \underbrace{R^qF_1}_{H^q(H,-)} \Rightarrow \underbrace{R^{p+q}F}_{H^{p+q}(G,-)}$$

□

Reminder A spectral sequence in an abelian cat is a sequence $(E_r, d_r)_{r \geq r_0}$ w/

$E_r = \bigoplus_{p,q \geq 0} E_r^{p,q}$ bigraded object

$d_r : E_r \to E_r$ of bidegree $(r, 1-r)$

(ie $d_r^{p,q} : E_r^{p,q} \longrightarrow E_r^{p+r, q-r+1}$)

sth $d_r \circ d_r = 0$ & $E_{r+1} = H^\bullet(E_r, d_r)$.

For $r > p+1$ we have $d_r^{p,q} = 0$,

so $E_r^{pq} \simeq E_{r+1}^{pq} \simeq \cdots =: E_\infty^{pq}$.

For a graded object $E^\bullet = \bigoplus_{n \geq 0} E^n$ we write $E_r^{p,q} \Rightarrow E^{p+q}$ if each E has a filtrat^n

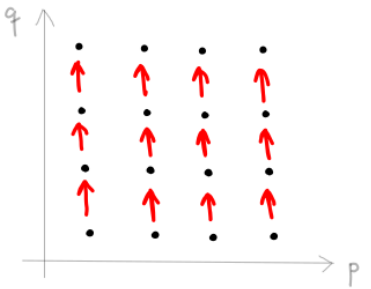
$0 = F^{n+1} E^n \subset F^n E^n \subset \cdots \subset F^0 E^n = E^n$

sth

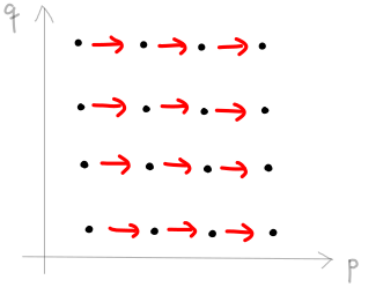
$$E_\infty^{pq} \simeq \mathrm{gr}_F^p E^{p+q} \quad \text{for all } p,q.$$

The differentials d look as follows:

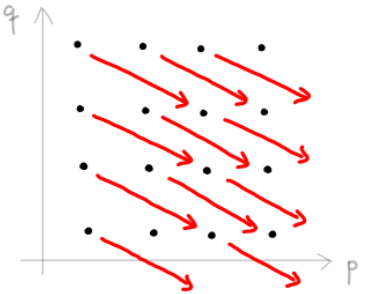
$E_0^{p,q}$:



$E_1^{p,q}$:

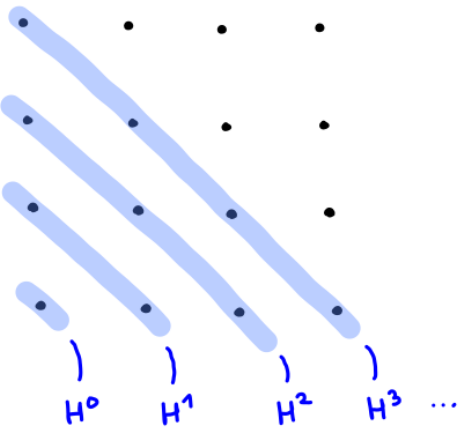


$E_2^{p,q}$:



Low degree terms on E_2 page:

E_2^{pq} :



$$gr^1 E^1 = F^1 E^1 \hookrightarrow F^0 E^1 \twoheadrightarrow gr_F^0 E^1$$
$$\| \qquad\qquad \| \qquad\qquad \|$$
$$E_2^{1,0} \qquad E^1 \qquad \ker(E_2^{0,1} \xrightarrow{d_2} E_2^{2,0})$$

$$gr^2 E^2 = F^2 H^2 \hookrightarrow E^2$$
$$\|$$
$$E_2^{2,0} / d_2(E_2^{0,1})$$

$\Rightarrow$ exact sequence of low degree terms:

$$0 \to E_2^{1,0} \to E^1 \to E_2^{0,1} \to E_2^{2,0} \to E_2$$

Back to Hochschild-Serre we get from

$$E_2^{pq} = H^p(G/H, H^q(H,A)) \Rightarrow H^{p+q}(G,A)$$

the exact sequence

$$0 \to H^1(G/H, A^H) \xrightarrow{\inf} H^1(G,A) \xrightarrow{\text{res}} H^1(H,A)^{G/H}$$
$$\to H^2(G/H, A^H) \xrightarrow{\inf} H^2(G,A)$$

(part of which we had checked by hand before).

We defined the restriction

$\mathrm{res}^i : H^i(G,-) \to H^i(H,-)$

as the morphism induced on derived functors by the inclusion $(-)^G \hookrightarrow (-)^G$ of invariants.

Dually we define the corestriction

$\mathrm{cores}_i : H_i(H,-) \to H_i(G,-)$

as the morphism induced on derived functors by the projection $(-)_H \twoheadrightarrow (-)_G$ on coinvariants.

Rem For G finite we have:

$$\begin{array}{ccc} H^0(G,A) = A^G & \twoheadrightarrow & H^0_T(G,A) = A^G/N_G(A) \\ \downarrow \mathrm{res}^0 & & \downarrow \exists!\, \mathrm{res}^0 \\ H^0(H,A) = A^H & \twoheadrightarrow & H^0_T(H,A) = A^H/N_H(A) \end{array} \qquad N_G(A)$$

$$\begin{array}{ccc} H_0(H,A) = A_H & \hookleftarrow & H^{-1}_T(H,A) = \ker(N_H)/I_H A \\ \downarrow \mathrm{cores}_0 & & \downarrow \exists!\, \mathrm{cores}^{-1} \\ H_0(G,A) = A_G & \hookleftarrow & H^{-1}_T(G,A) = \ker(N_G)/I_G A \end{array} \qquad I_G A$$

In fact we can extend to Tate coh in all degrees:

Prop If G is finite, $\exists!$ collection of natural trafos

$$H^i_T(G,-) \underset{\mathrm{cores}^i}{\overset{\mathrm{res}^i}{\rightleftarrows}} H^i_T(H,-) \quad \forall i \in \mathbb{Z}$$

that extend the above res^0 & cores^{-1} and are compatible w/ boundary operators:

For $0 \to A \to B \to C \to 0$ exact in $\mathrm{Mod}(G)$ the diagram

$$\begin{array}{ccc} H^i_T(G,C) & \xrightarrow{\delta} & H^{i+1}_T(G,A) \\ \downarrow \mathrm{res}^i & & \downarrow \mathrm{res}^{i+1} \\ H^i_T(H,C) & \xrightarrow{\delta} & H^{i+1}_T(H,A) \end{array}$$

commutes, & dually for cores^i.

Pf. We discuss res (cores is similar)

- Uniqueness: Use dimension shifting. By assumption

$$\begin{array}{ccc} H^0_T(G, A\langle m\rangle) & \xrightarrow[\delta^{-m}]{\sim} & H^m(G, A) \\ \downarrow{\scriptstyle \mathrm{res}^0} & & \downarrow{\scriptstyle \mathrm{res}^m} \\ H^0_T(H, A\langle m\rangle) & \xrightarrow[\delta^{-m}]{\sim} & H^m(H, A) \end{array}$$

commutes & res^0 is given already.

- Existence: From $\mathbb{Z}H \hookrightarrow \mathbb{Z}G$ we get a $\mathbb{Z}H$-linear map of bar resolutions

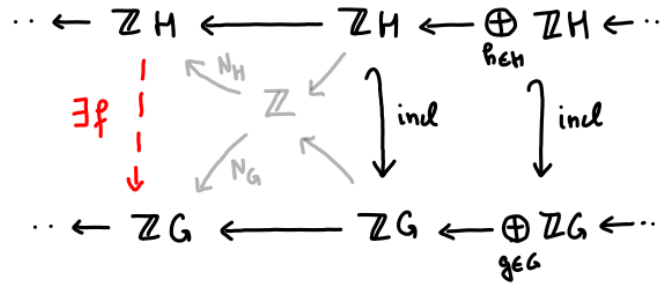
$$\begin{array}{ccc} Y_{\cdot\geq 0} = [\cdots \to Y_1 \to Y_0] & \text{w/} & Y_i = \bigoplus_{\gamma \in H^i} \mathbb{Z}H \cdot \gamma \\ \downarrow & & \\ X_{\cdot\geq 0} = [\cdots \to X_1 \to X_0] & & X_i = \bigoplus_{\gamma \in G^i} \mathbb{Z}G \cdot \gamma \end{array}$$

Extend it to a map of complete resolutions $Y_\cdot \xrightarrow{f} X_\cdot$ using extension properties of such resolutions, and take the map on cohom. induced by

$$\mathrm{Hom}_G(X_\cdot, A) \to \mathrm{Hom}_H(X_\cdot, A) \xrightarrow[f^*]{} \mathrm{Hom}_H(Y_\cdot, A). \qquad \square$$

Caution While $\mathrm{res}^i: H^i_T(G, A) \to H^i_T(H, A)$ for $i \geq 0$ is given by restriction of cocycles to $H^i \subset G^i$ the situation is more complicated for $i < 0$.

For instance, in a diagram of complete resolutions



we cannot take f to be the inclusion, since $N_H \neq N_G$ for $H \neq G$!

In general formulas for res^i for $i < 0$ are more cumbersome to get.

Ex For $i=-2$ we get a homom.

$$\mathrm{Ver} := \mathrm{res}^{-2}: \quad \underset{\| \; H_T^{-2}(G,\mathbb{Z})}{G^{ab}} \longrightarrow \underset{\| \; H_T^{-2}(H,\mathbb{Z})}{H^{ab}}.$$

called the Verlagerung. Exercise: Find an explicit formula for this homom!

Restriction & corestriction are related by:

Lemma For G finite & all $i \in \mathbb{Z}$ we have

$$H_T^i(G,A) \xrightarrow{\mathrm{res}} H_T^i(H,A) \xrightarrow{\mathrm{cores}} H_T^i(G,A)$$

$$[G:H]\cdot \mathrm{id}$$

Pf. For $i=0$:

$$A^G/_{N_G(A)} \longrightarrow A^H/_{N_H(A)} \longrightarrow A^G/_{N_G(A)}$$
$$[a] \longmapsto [a] \longmapsto [N_{G/H}(a)]$$

General case by dim shifting:

$$\begin{array}{ccc} H^0(G,A[i]) & \xrightarrow[\sim]{\delta^i} & H^i(G,A) \\ \downarrow{\scriptstyle \varphi_0} & & \downarrow{\scriptstyle \varphi_i} \\ H^0(H,A[i]) & \xrightarrow[\sim]{\delta^i} & H^i(H,A) \end{array}$$

$(\varphi_i := \mathrm{cores}^i \circ \mathrm{res}^i)$ ∎

Ex Write $H^i(G,A) = \bigoplus_{p \text{ prime}} \underbrace{H^i(G,A)_p}_{p\text{-torsion}}$

(possible since $H^i(G,A)$ is a torsion gp).

Then for any p-Sylow subgp $H \subset G$,

$\mathrm{res}: H^i(G,A)_p \hookrightarrow H^i(H,A)$ is inj.

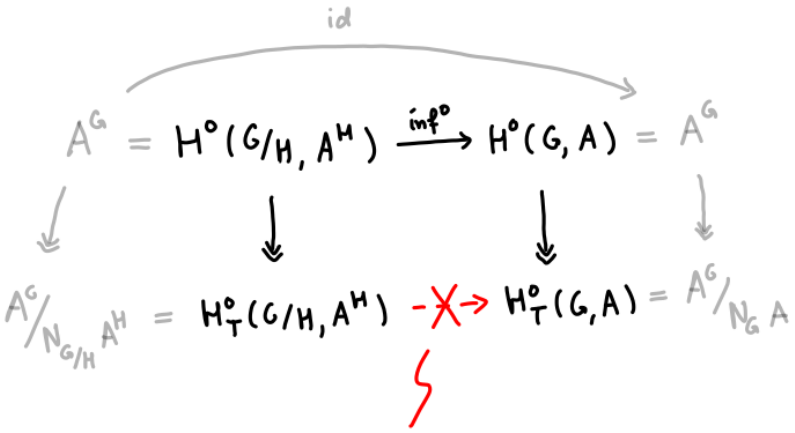
$\mathrm{cores}: H^i(H,A) \twoheadrightarrow H^i(G,A)_p$ is surj.

(since $\mathrm{cores} \circ \mathrm{res} = [G:H]\cdot \mathrm{id}$ invertible on $H^i(G,A)_p$)

Cor If $\forall p \; \exists p$-Sylow $H \subset G$ w/ $H^i(H,A)=0$, then already $H^i(G,A)=0$.

Pf. By the above $H^i(G,A)_p = 0 \; \forall p$. ∎

Rem Unlike (co-)restriction, the inflation does not extend to Tate cohomology, even in degree zero:



8. The cup product

$A, B \in \mathrm{Mod}(G)$

$\rightsquigarrow A \otimes_{\mathbb{Z}} B \in \mathrm{Mod}(G)$

via $g \cdot (a \otimes b) := ga \otimes gb$

We have a natural inclusion

$$\begin{array}{ccc} A^G \otimes B^G & \hookrightarrow & (A \otimes B)^G \\ \| & & \| \\ H^0(G,A) \otimes H^0(G,B) & & H^0(G, A \otimes B) \end{array}$$

To extend this map to pairings on higher cohom, it is convenient to use "homogenous cochains":

$$\mathrm{Maps}_G(G^{q+1}, A)$$

$$:= \{ a : G^{q+1} \to A \mid a(gg_0, \dots, gg_q) = g \cdot a(g_0, \dots, g_q) \text{ for all } g, g_0, \dots, g_q \in G \}$$

Rem We have isomorphisms

$$\varphi: A_q^{hom} := Maps_G(G^{q+1}, A)$$

$$\xrightarrow{\sim} A_q := Maps(G^q, A),$$

$$(\varphi(a))(g_1, .., g_q) := a(1, g_1, g_1g_2, \cdots, g_1 \cdots g_q)$$

via which the differential $d: A_{q-1} \to A_q$ of the bar resolution translates to

$$d: A_{q-1}^{hom} \longrightarrow A_q^{hom}$$

$$(da)(x_0, \cdots, x_q) = \sum_{i=0}^{q} (-1)^i a(x_0, \cdots, \hat{x}_i, \cdots, x_q).$$

($\hat{x}_i$: omitted)

Upshot Homogenous cochains include redundant information but make the formula for the differentials easier!

Def The cup product of homogenous cochains of degree $p, q \geq 0$ is

$$\cup: A_p^{hom} \times B_q^{hom} \longrightarrow (A \otimes B)_{p+q}^{hom},$$

$$(a \cup b)(g_0, \cdots, g_{p+q}) := a(g_0, \cdots, g_p) \otimes b(g_p, \cdots, g_{p+q}).$$

Lemma For $a \in A_p^{hom}$ and $b \in B_q^{hom}$ we have

$$d(a \cup b) = (da) \cup b + (-1)^p a \cup (db).$$

Pf.

$$d(a \cup b)(g_0, .., g_{p+q+1})$$

$$= \sum_{i=0}^{p} (-1)^i a(g_0, .., \hat{g}_i, .., g_{p+1}) \otimes b(g_{p+1}, .., g_{p+q+1})$$

$$+ \sum_{j=p+1}^{p+q+1} (-1)^j a(g_0, .., g_p) \otimes b(g_p, .., \hat{g}_j, .., g_{p+q+1})$$

$$= ((da) \cup b + (-1)^p a \cup (db))(g_0, \cdots, g_{p+q+1})$$

(terms with $i = p+1$ and $j = p$ cancel out)

□

Cor The cup product induces for all $p,q \geq 0$ a natural bilinear pairing

$$\cup : H^p(G,A) \times H^q(G,A) \longrightarrow H^{p+q}(G,A).$$

Pf. For $a \in Z_p^{hom}(A) := \ker(d : A_p^{hom} \to A_{p+1}^{hom})$ and $b \in Z_q^{hom}(B)$ the lemma shows:

- $a \cup b \in Z_{p+q}^{hom}(A \otimes B)$
- $a \cup b = 0$ if $a \in \mathrm{im}(d)$ or $b \in \mathrm{im}(d)$ □

Now assume G is finite. We will extend "$\cup$" to Tate cohom in all degrees. The starting case:

$$\begin{array}{ccc} H_T^0(G,A) \otimes H_T^0(G,B) & \xrightarrow{\cup} & H_T^0(G, A\otimes B) \\ \| & & \| \\ A^G/_{N_G(A)} \otimes B^G/_{N_G(B)} & \longrightarrow & (A\otimes B)^G/_{N_G(A\otimes B)} \\ [a]\otimes[b] & \longmapsto & [a\otimes b] \end{array}$$

(well defined as $N_G(A) \otimes B^G \subset N_G(A\otimes B)$ etc)

Thm $\exists!$ family of pairings

$$\cup : H_T^p(G,A) \times H_T^q(G,B) \longrightarrow H_T^{p+q}(G, A\otimes B)$$

for all $p,q \in \mathbb{Z}$, natural in $A, B \in \mathrm{Mod}(G)$, sth:

a) For $p = q = 0$ it is the pairing given above.

b) For $0 \to A' \to A \to A'' \to 0$ exact in $\mathrm{Mod}(G)$ w/ $0 \to A'\otimes B \to A\otimes B \to A''\otimes B \to 0$ exact:

$$\begin{array}{ccc} H_T^p(G,A'') \times H_T^q(G,B) & \xrightarrow{\cup} & H_T^{p+q}(G, A''\otimes B) \\ \downarrow \delta\times 1 & \circlearrowright & \downarrow \delta \\ H_T^{p+1}(G,A') \times H_T^q(G,B) & \xrightarrow{\cup} & H_T^{p+q+1}(G, A'\otimes B) \end{array}$$

c) For $0 \to B' \to B \to B'' \to 0$ exact in $\mathrm{Mod}(G)$ w/ $0 \to A\otimes B' \to A\otimes B \to A\otimes B'' \to 0$ exact:

$$\begin{array}{ccc} H_T^p(G,A) \times H_T^q(G,B'') & \xrightarrow{\cup} & H_T^{p+q}(G, A\otimes B'') \\ \downarrow 1\times\delta & \circlearrowright & \downarrow (-1)^p\cdot\delta \\ H_T^p(G,A) \times H_T^{q+1}(G,B') & \xrightarrow{\cup} & H_T^{p+q+1}(G, A\otimes B') \end{array}$$

think of homogeneous cocycles for $p,q > 0$!

Pf. Uniqueness is clear by dimension shifting

(for simplicity we put $H^i(-) := H^i_T(G,-)$):

$$\begin{array}{ccc}
H^0(A\lceil p\rceil)\times H^0(B\lceil q\rceil) & \xrightarrow{\cup} & H^0((A\otimes B\lceil q\rceil)\lceil p\rceil) \\
\downarrow{\scriptstyle \delta^p\times 1} & & \downarrow{\scriptstyle \delta^p} \\
H^p(A)\times H^0(B\lceil q\rceil) & \xrightarrow{\exists!} & H^p(A\otimes B\lceil q\rceil) \\
\downarrow{\scriptstyle 1\times\delta^q} & & \downarrow{\scriptstyle (-1)^{pq}\cdot\delta^q} \\
H^p(A)\times H^q(B) & \xrightarrow{\exists!} & H^{p+q}(A\otimes B)
\end{array}$$

apply c) q times

Existence:

Define $\cup : H^p(A)\times H^q(B) \to H^{p+q}(A\otimes B)$

by the above diagram.

Naturality in $A, B \in \mathrm{Mod}(G)$ is clear

& property a) holds by construction.

We need to check b) & c) holds.

Let's check c) for instance:

We first note that for $p=0$, our definition implies that

$$\cup : \quad H^0(A)\times H^q(B) \longrightarrow H^q(A\otimes B)$$

is given on cocycles by $[a]\cup\lceil b\rceil = [\underbrace{a\otimes b}_{\text{again a cocycle since } a\in A^G}]$!

for $a \in \ker(A_0 \to A_1) = A^G$

$b \in \ker(B_q \to B_{q+1}) \subset B_q = \mathrm{Maps}(G^k, B)$,

$$k = \begin{cases} q & \text{if } q\geq 0 \\ -q-1 & \text{if } q<0 \end{cases}$$

(because the maps $([a],\lceil b\rceil)\mapsto \lceil a\otimes b\rceil$ make the diagram on the previous page for $p=0$ commute, hence agree w/ $([a],[b])\mapsto [a]\cup\lceil b\rceil$ by def^n).

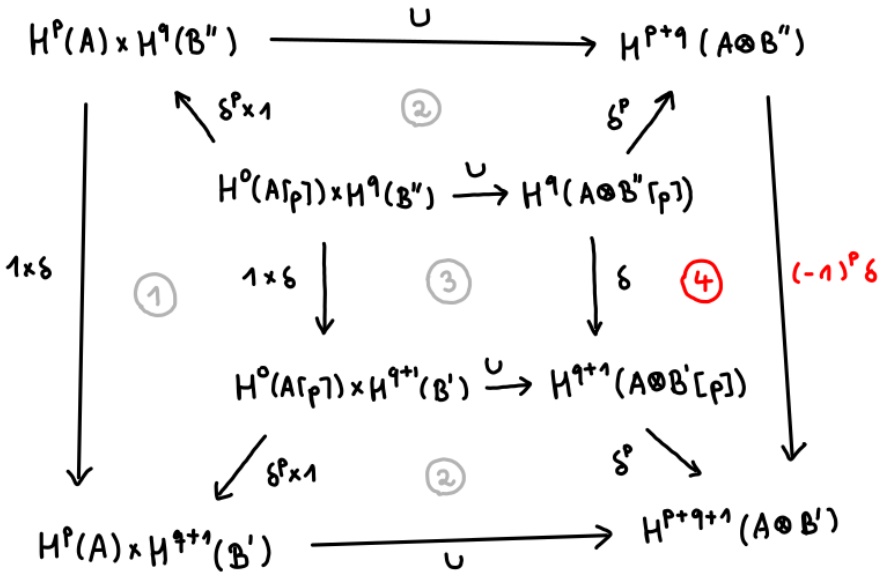
$\Rightarrow$ property c) holds for $p=0$

by direct inspection

For arbitrary $p \in \mathbb{Z}$ reduce to $p = 0$ by dim shifting:

Say $0 \to B' \to B \to B'' \to 0$

& $0 \to A \otimes B' \to A \otimes B \to A \otimes B'' \to 0$ both exact.



① commutes trivially.

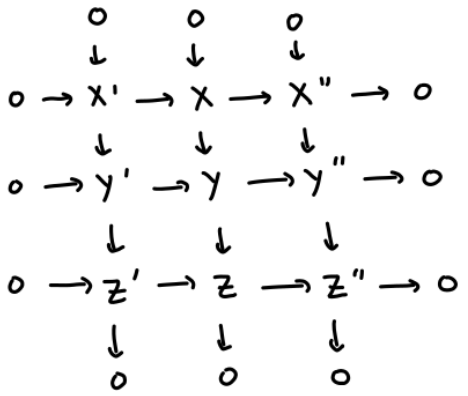
② commutes by our definition of "$\cup$"

③ commutes by the case $p = 0$ from above

④ commutes by the lemma below.

□

Lemma Given a diagram



of complexes X, Y, Z etc. in an abelian category w/ exact rows and columns, the boundary maps fit in the comm. diagram

$$\begin{array}{ccc} H^{q-1}(Z'') & \xrightarrow{\delta} & H^q(Z') \\ {\scriptstyle \delta}\downarrow & & \downarrow{\scriptstyle -\delta} \\ H^q(X'') & \xrightarrow{\delta} & H^{q+1}(X') \end{array}$$

(note the sign!)

Pf. Exercise. □

Prop The cup product has the following properties:

a) Associativity: $a \cup (b \cup c) = (a \cup b) \cup c$

b) Graded commutativity: $a \cup b = (-1)^{pq}\, b \cup a$

for $a \in H_T^p(G, A)$, $b \in H_T^q(G, B)$ via the natural iso $H_T^{p+q}(G, A \otimes B) \simeq H_T^{q+p}(G, B \otimes A)$

c) Restriction: For subgps $H \subset G$,

$$\operatorname{res}_H^G(a \cup b) = \operatorname{res}_H^G(a) \cup \operatorname{res}_H^G(b)$$

d) "Projection formula":

$$\operatorname{cores}_H^G(\operatorname{res}_H^G(a) \cup b) = a \cup \operatorname{cores}_H^G(b).$$

Pf. Use dim shifting. The sign in b) comes from

$$\begin{array}{ccc} H^0((A \otimes B\lceil q \rceil)\lceil p \rceil) & \xrightarrow{\sim} & H^0((B \otimes A\lceil p \rceil)\lceil q \rceil) \\ \downarrow \delta^p & & \downarrow \delta^p \\ H^p(A \otimes B\lceil q \rceil) & & H^q(B \otimes A\lceil p \rceil) \\ \downarrow \delta^q & & \downarrow (-1)^{pq} \cdot \delta^q \quad \text{(by the lemma above)} \\ H^{p+q}(A \otimes B) & \xrightarrow{\sim} & H^{p+q}(B \otimes A) \end{array}$$

For d) dim shifting reduces to degree zero. Then have

$$\begin{array}{ccc} H_T^0(G, A) & \underset{\text{cores}}{\overset{\text{res}}{\rightleftarrows}} & H_T^0(H, A) \\ \| & & \| \\ A^G/N_G(A) & \underset{\text{"}N_{G/H}\text{"}}{\overset{[a]_G \mapsto [a]_H}{\rightleftarrows}} & A^H/N_H(A) \end{array}$$

w/ $\lceil a \rceil_G := (a + N_G(A))$

$\lceil a \rceil_H := (a + N_H(A))$

For $\alpha = \lceil a \rceil_G$, $\beta \in \lceil b \rceil_H$ w/ $a \in A^G$, $b \in B^H$:

$$\operatorname{cor}(\operatorname{res}(\alpha) \cup \beta) = N_{G/H}([a \otimes b]_H)$$

$$= \sum_{i \in I} \lceil g_i \cdot (a \otimes b) \rceil_G \quad \text{w/ } G = \dot{\bigcup}_{i \in I} g_i H$$

$$= \sum_{i \in I} [a \otimes g_i b]_G \quad \text{since } a \in A^G$$

$$= \Big[a \otimes \sum_{i \in I} g_i b\Big]_G = \alpha \cup \operatorname{cores}(\beta).$$

□

Explicit formulas in low degree:

a) $(p,q) = (1,-1)$:

For $a \in Z^1(G,A) \subset A_0 = \mathrm{Maps}(G,A)$

and $b \in Z^{-1}(G,B) \subset B_{-1} = \ker(N_G) \subset B$,

$$a \cup b = \sum_{g \in G} a(g) \otimes g \cdot b \quad \text{in } H^0_T(G, A \otimes B)$$

b) $(p,q) = (1,-2)$ & $B = \mathbb{Z}$:

For $a \in Z^1(G,A)$ and $b \in H^{-2}_T(G,\mathbb{Z}) \simeq G^{ab}$ ($b \mapsto [g]$)

we have

$$a \cup b = a(g) \text{ in } H^{-1}_T(G,A).$$

c) $(p,q) = (2,-2)$ & $B = \mathbb{Z}$:

For $a \in Z^2(G,A)$ and $b = [g] \in H^{-2}_T(G,\mathbb{Z}) \simeq G^{ab}$

we have

$$a \cup b = \sum_{h \in G} a(h,g) \in H^0_T(G,A).$$

Pf. a) Consider $0 \to A \to \underbrace{\mathbb{Z}G \otimes A}_{=:\tilde{A}} \xrightarrow{pr} \underbrace{A\lceil 1 \rceil}_{=\mathbb{Z}_G \otimes A} \to 0$

We have

$$H^0_T(G, A\lceil 1\rceil) \xrightarrow[\delta]{\sim} H^1_T(G,A) \longrightarrow H^1_T(G,\tilde{A}) = 0$$

$$\exists\, [c] \longmapsto [a] \longmapsto [0]$$

explicitly:

$c = pr(\tilde{c}) \in A\lceil 1 \rceil$

$$\Rightarrow \exists\, \tilde{c} \in \tilde{A} \ \ \forall g \in G: \quad a(g) = g \cdot \tilde{c} - \tilde{c} \qquad (*)$$

Thus

$$\begin{aligned}
a \cup b &= \delta(c) \cup b \\
&= \delta(c \cup b) && \text{(now } \delta \text{ for } 0 \to A \otimes B \to \tilde{A} \otimes B \to A\lceil 1 \rceil \otimes B \to 0) \\
&= d(\tilde{c} \otimes b) && \text{(w/ } d \text{ differential in the bar resolution, by definition of the boundary map } \delta) \\
&= N_G(\tilde{c} \otimes b) \\
&= \sum_{g \in G} g\tilde{c} \otimes gb \\
&= \sum_{g \in G} (a(g) + \tilde{c}) \otimes gb \quad \text{by } (*) \\
&= \sum_{g \in G} a(g) \otimes gb + \tilde{c} \otimes \underbrace{N_G(b)}_{=0 \text{ since } b \in Z^{-1}(G,B)}
\end{aligned}$$

b) Consider $0 \to \underbrace{A[-1]}_{= A \otimes I_G} \to \underbrace{A \otimes \mathbb{Z}G}_{=: \tilde{A}} \to A \to 0$.

We have

$$H_T^{-1}(G, A) \xrightarrow[\delta]{\sim} H_T^0(G, A[-1])$$

$\Rightarrow$ enough to show $\delta(a \cup b) = \delta(a(g))$

for $a \in Z^1(G, A)$, $b = [g] \in H_T^{-2}(G, \mathbb{Z}) \simeq G^{ab}$.

From the def^n of δ we get

$$\delta(a(g)) = \sum_{\tau \in G} \underbrace{(\tau \cdot a(g))}_{\in A} \otimes \underbrace{\tau}_{\in \mathbb{Z}G} =: x \quad \text{in } H_T^0(G, A[-1])$$

On the other hand

$$\begin{array}{ccc} H_T^{-2}(G, \mathbb{Z}) & \xrightarrow[\delta]{\sim} & H_T^{-1}(G, I_G) \\ \psi & & \psi \\ b = [g] & \longmapsto & [g-1] \end{array}$$

so that $\delta(a \cup b) = -(a \cup \delta(b)) = -a \cup (g-1) =: y$.

Applying part a) to the cocycle y we get

$$\begin{aligned} y &= -a \cup (g-1) \\ &= -\sum_{\tau \in G} a(\tau) \otimes (\tau \cdot (g-1)) \\ &= \sum_{\tau \in G} a(\tau) \otimes \tau - \sum_{\tau \in G} a(\tau) \otimes \tau g \\ &= \sum_{\tau \in G} \underbrace{a(\tau g)}_{= a(\tau) + \tau a(g)} \otimes \tau g - \sum_{\tau \in G} a(\tau) \otimes \tau g \\ &= \sum_{\tau \in G} \tau a(g) \otimes \tau g \end{aligned}$$

$$\Rightarrow \quad y - x = \sum_{\tau \in G} \tau a(g) \otimes \tau(g-1)$$

$$= N_G\left(\underbrace{a(g) \otimes (g-1)}_{\in A \otimes I_G = A[-1]}\right)$$

$\Rightarrow y = x$ in $H_T^0(G, A[-1])$ as desired.

c) Consider again $0 \to A \to \underbrace{\mathbb{Z}G \otimes A}_{=:\tilde{A}} \to \underbrace{A^{[1]}}_{=J_G \otimes A} \to 0$.

$a \in Z^2(G,A)$ & $H^2_T(G,\tilde{A}) = 0$

$\Rightarrow \exists \tilde{a} \in Z^1(G,\tilde{A})$: $a = d(\tilde{a})$, i.e.

(*) $a(\tau,\sigma) = \tau\tilde{a}(\sigma) - \tilde{a}(\tau\sigma) + \tilde{a}(\tau) \quad \forall \tau,\sigma \in G$

Let $c := \text{image}(\tilde{a}) \in Z^1(G, A^{[1]})$,

then $a = \delta(c)$.

$\Rightarrow$ For $b = [g] \in H^{-2}_T(G,A) \simeq G^{ab}$ we get

$$\begin{aligned} a \cup b &= \delta(c) \cup [g] \\ &= \delta(c \cup [g]) \\ &= \delta(c(g)) \text{ by part b)} \\ &= d(\tilde{a}(g)) \text{ by construction of } \delta \\ &= \sum_{\tau \in G} \tau \cdot \tilde{a}(g) \\ &\overset{\text{by (*)}}{=} \sum_{\tau \in G} a(\tau,\sigma) + \underbrace{\sum_{\tau \in G} \tilde{a}(\tau\sigma) - \sum_{\tau \in G} \tilde{a}(\tau)}_{=0} \end{aligned}$$

□

Rem Part c) is what we want for CFT:

Given a class $a \in H^2_T(G,A)$, we get a homom.

$$a \cup (-) : \underbrace{H^{-2}_T(G,\mathbb{Z})}_{\| \; G^{ab}} \longrightarrow \underbrace{H^0_T(G,A)}_{\| \; A^G/N_G(A)}$$

This will give us the local Artin map!

II. Abstract CFT

Motivation: L/K finite abelian extension of local fields w/ $G = \mathrm{Gal}(L/K)$

Local CFT predicts iso

$$\mathrm{Art}_{L/K}: \underbrace{G^{ab}}_{\| H_T^{-2}(G,\mathbb{Z})} \xrightarrow{\sim} \underbrace{K^*/N_{L/K}(K^*)}_{\| H_T^0(G,L^*)}$$

$$x \longmapsto u_{L/K} \cup x$$

for a "fundamental class" $u_{L/K} \in H^2(G,\mathbb{Z})$

& these should be compatible in towers $K \subset L \subset M \cdots$

We'll give an abstract criterion for existence of such an iso ("Tate's thm") & capture compatibility in an axiomatic framework.

1. Tate's thm

Let G be a finite gp.

Def $A \in \mathrm{Mod}(G)$ is cohomologically trivial if for every subgroup $H \subset G$, we have

$$H_T^i(H,A) = 0 \quad \text{for all } i \in \mathbb{Z}.$$

Ex Induced modules are coh. trivial.

In general we have:

Thm ("criterion for coh. triviality")

Let $A \in \mathrm{Mod}(G)$. If $\exists\, i_0 \in \mathbb{Z}$ sth $\forall$ subgp $H \subset G$:

$$H_T^{i_0}(H,A) = H_T^{i_0+1}(H,A) = 0,$$

then A is cohom. trivial.

Pf. It suffices to show:

If $H_T^{i_0}(H,A) = H_T^{i+1}(H,A) = 0 \quad \forall H \subset G$,

then $H_T^{i_0-1}(H,A) = H_T^{i_0+2}(H,A) = 0 \quad \forall H \subset G$.

Dimension shifting $\Rightarrow$ wlog $i_0 = 1$.

So assume

$$H_T^1(H,A) = H_T^2(H,A) = 0 \quad \forall H \subset G.$$

We need to show for all $H \subset G$:

$$(*_H): \quad H_T^0(H,A) = H_T^3(H,A) = 0$$

Use induction on $|G|$:

For $|G| = 1$ the claim is trivial.

Assume now by induction that we already know $(*_H)$ for all proper subgps $H \subsetneq G$.

We must show that $(*_G)$ holds.

If G is not a p-group for any p, then every Sylow subgp is a proper subgp of G.

$\Rightarrow H_T^0(H,A) = H_T^3(H,A) = 0$

for all Sylow subgroups $H \subset G$

$\Rightarrow H_T^0(G,A) = H_T^3(G,A) = 0$

(see corollary to cores $\circ$ res $= [G:H]$)

So we may assume G is a p-group.

$\Rightarrow \exists$ normal subgp $H \trianglelefteq G$ w/ G/H cyclic

(finite p-groups are nilpotent, ie. the subgps $G_i \subset G$ defined by $G_0 = G$, $G_{i+1} = [G_i, G]$ satisfy $G_n = \{1\}$ for some n. In particular $G_1 = [G,G] \subsetneq G$, so $G^{ab} \neq \{1\}$ and hence $\exists$ epi $p: G^{ab} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$. Put $H := \ker(p)$.)

By assumption $H_T^j(H,A) = 0$ for $j = 0,1,2,3$.

$\Rightarrow H^j(H,A) = 0$ for $j = 1,2,3$

$\Rightarrow$ The Hochschild-Serre spectral sequence has

$E_2^{ij} = H^i(G/H, H^j(H,A)) = 0$ for $j = 1,2,3$:

$H^3(G/H, A^H)$	0	0	...
$H^2(G/H, A^H)$	0	0	...
$H^1(G/H, A^H)$	0	0	...
$H^0(G/H, A^H)$	0	0	...

$\Rightarrow H_T^i(G/H, A^H) \xrightarrow{\simeq} H_T^i(G,A)$ for $i = \cancel{0},1,2,3$. (*)

- $H_T^3(G,A) \simeq H_T^3(G/H, A^H)$ by (*)
  $\simeq H_T^1(G/H, A^H)$ since G/H cyclic
  $\simeq H_T^1(G,A)$ by (*)
  $= 0$ by assumption

- $H_T^0(G/H, A^H) \simeq H_T^2(G/H, A^H)$ since G/H cyclic
  $\simeq H_T^2(G,A)$ by (*)
  $= 0$ by assumption

$\Rightarrow A^G = N_{G/H}(A^H) = N_G(A) \Rightarrow H_T^0(G,A) = 0$

($N_{G/H}(A^H) = N_G(A)$ since $H_T^0(H,A) = 0$)

□

Thm ("almost Tate's thm") Let $M \in \mathrm{Mod}(G)$

Assume that for all subgps $H \subset G$,

a) $H_T^{-1}(H,A) \simeq 0$, and

b) $H_T^0(H,A)$ is cyclic of order $|H|$.

Pick a generator a of $H_T^0(H,A)$. Then for all $i \in \mathbb{Z}$ we get an iso

$$a \cup (-) : H_T^i(G,\mathbb{Z}) \xrightarrow{\simeq} H_T^i(G,A)$$

no degree shift yet!
here cup product is just given by $a \otimes (-)$ on cochains.

Pf. Pick $a_0 \in A$ w/ $a = (a_0 + N_G(A)) \in H_T^0(G,A)$.

If $z_{a_0} : \mathbb{Z} \to A$, $n \mapsto n \cdot a_0$ is not injective,

consider instead

$\tilde{\imath} := z_{\tilde{a}_0} : \mathbb{Z} \hookrightarrow \tilde{A} := A \oplus \mathbb{Z}G$

w/ $\tilde{a}_0 := (a_0, N_G) \in \tilde{A}$

We have $$\begin{array}{ccc} H_T^\bullet(G,\mathbb{Z}) & \xrightarrow{z_{a_0}*} & H_T^\bullet(G,A) \\ \| & & \downarrow z \\ H_T^\bullet(G,\mathbb{Z}) & \xrightarrow{z_{\tilde{a}_0}*} & H_T^\bullet(G,\tilde{A}) \end{array}$$

$\Rightarrow$ Replacing A by $\tilde{A}$ & a_0 by $\tilde{a}_0$,

may assume $z := z_{a_0} : \mathbb{Z} \hookrightarrow A$ injective.

$\Rightarrow$ exact sequence $0 \to \mathbb{Z} \to A \to \underbrace{Q}_{\cong \operatorname{cok}(z_{a_0})} \to 0$

For any subgp $H \subset G$,

$H_T^{-1}(H,A) = 0$ by assumpt^n & $H_T^1(H,\mathbb{Z}) = \operatorname{Hom}(H,\mathbb{Z}) = 0$

so we get

$$0 \to H_T^{-1}(H,Q) \to H_T^0(H,\mathbb{Z}) \xrightarrow{z_*} H_T^0(H,A) \to H_T^0(H,Q) \to 0$$

$$H_T^0(H,\mathbb{Z}) \cong \mathbb{Z}/_{|H|\mathbb{Z}} \quad (a_0 \otimes (-)), \qquad H_T^0(H,A) \cong \mathbb{Z}/_{|H|\cdot\mathbb{Z}} \text{ by assumption}$$

Claim z_* is an iso,

i.e. $a|_H = [a_0]$ generates $H_T^0(H,A)$.

For $H = G$ this holds by our choice of a.

In general we have

$$H_T^0(G,A) \xrightarrow{\text{res}^0} H_T^0(H,A) \xrightarrow{\text{cores}^0} H_T^0(G,A), \qquad \text{cores}^0 \circ \text{res}^0 = [G:H]\cdot \mathrm{id}$$

$$\mathbb{Z}/_{|G|\mathbb{Z}} \longrightarrow \mathbb{Z}/_{|H|\mathbb{Z}} \qquad \mathbb{Z}/_{|G|\mathbb{Z}}$$

hence $\ker(\text{res}^0) = [G:H]\cdot \mathbb{Z}/_{|G|\mathbb{Z}}$

$\Rightarrow$ res^0 surjective & $a|_H$ generates $H_T^0(H,A)$

$\Rightarrow$ In the (not so) long exact sequence from the previous page z_* is an iso

$\Rightarrow$ $H_T^{-1}(H,Q) = H_T^0(H,Q) = 0$

$\Rightarrow$ By the criterion for cohom. triviality

$H_T^i(H,Q) = 0 \quad \forall i \in \mathbb{Z}, \ \forall H \subset G$

$\Rightarrow$ $z_* : H_T^i(H,\mathbb{Z}) \xrightarrow{\sim} H_T^i(H,A)$ iso $\forall i \in \mathbb{Z}$. $\square$

Cor ("Tate's thm") Let $A \in \mathrm{Mod}(G)$.

Assume that for all subgps $H \subset G$,

a) $H_T^1(H, A) = 0$

b) $H_T^2(H, A)$ is cyclic of order $|H|$.

Let a be a generator of $H_T^2(G, A)$, then for all $i \in \mathbb{Z}$ we get an iso

$$a \cup (-) : H_T^i(G, \mathbb{Z}) \xrightarrow{\sim} H_T^{i+2}(G, A).$$

(for $i = -2$ that's what we want in CFT)

Moreover for any subgp $H \subset G$, $a|_H$ still generates $H_T^2(H, G)$ and we thus get

$$a|_H \cup (-) : H_T^i(H, \mathbb{Z}) \xrightarrow{\sim} H_T^{i+2}(H, A).$$

Pf. Consider $\delta^2 : H_T^i(H, \underbrace{A[2]}_{=: B}) \xrightarrow{\sim} H_T^{i+2}(H, A)$.

By assumption

$$H_T^{-1}(H, B) = 0 \quad \& \quad H_T^0(H, B) \simeq \mathbb{Z}/_{|H|\mathbb{Z}}.$$

The previous thm for B and $b := \delta^{-2}(a)$ gives

$$\begin{array}{ccc} H^i(G, \mathbb{Z}) & \xrightarrow[b \cup (-)]{\sim} & H^i(G, B) \\ \| & & \downarrow \delta^2 \\ H^i(G, \mathbb{Z}) & \xrightarrow{a \cup (-)} & H^{i+2}(G, A) \end{array}$$

hence an iso!

The same then also follows for any subgp $H \subset G$ using $\mathrm{cores} \circ \mathrm{res} = [G : H] \cdot \mathrm{id}$ as above. □

2. A reminder about profinite gps

Recall A profinite gp is a group of the form

$$G \simeq \varprojlim_{i \in I} G_i$$
$$= \{ (g_i)_{i \in I} \mid g_i \in G_i,\ \pi_{ji}(g_j) = g_i \ \forall j \geq i \}$$

w/ a directed set $(I, \geq)$,
a system of finite gps G_i $(i \in I)$ and
group hom. $\pi_{ji} : G_j \to G_i$ for $j \geq i$
s.th $\pi_{kj} \circ \pi_{ji} = \pi_{ki}$ $(k \geq j \geq i)$ & $f_{ii} = id$.

We endow G with the subspace topology for the inclusion $G \hookrightarrow \prod_{i \in I} G_i$

w/ product topology, where each G_i is given the discrete topology

i.e. G has a nbhood basis of cosets $g \cdot N_i$ for the open normal subgps $N_i := \ker(G \xrightarrow{pr_i} G_i) \trianglelefteq G$

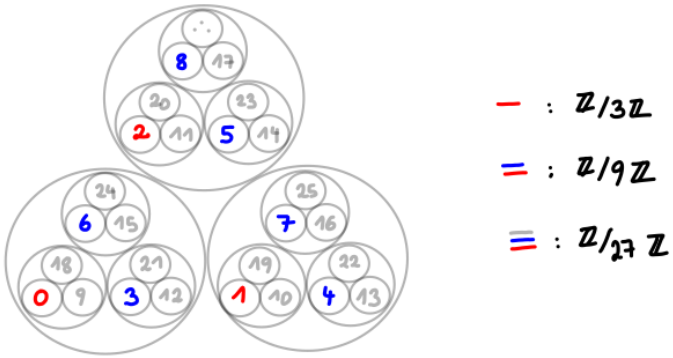
(and $G = \varprojlim_i G_i$ in the category of top gps ...)

Ex a) Any finite gp G w/ the discrete top. is profinite.

b) For any prime p, $\mathbb{Z}_p := \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is profinite

(w/ $\pi_{m,n} : \mathbb{Z}/p^m\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ $(x \bmod p^m) \mapsto (x \bmod p^n)$, $m \geq n$)

Cartoon of $\mathbb{Z}_3$ $\cdots \twoheadrightarrow \mathbb{Z}/27 \twoheadrightarrow \mathbb{Z}/9 \twoheadrightarrow \mathbb{Z}/3$:



— : $\mathbb{Z}/3\mathbb{Z}$

= : $\mathbb{Z}/9\mathbb{Z}$

≡ : $\mathbb{Z}/27\mathbb{Z}$

Note : The profinite topology on $\mathbb{Z}_p$ is induced by the p-adic metric $d(x,y) = |x-y|_p$. Since $d(x,z) \leq \max\{d(x,y), d(y,z)\}$. any two disks $D_i := \{ a \in \mathbb{Z}_p \mid |a - a_i|_p < r_i \} \subset \mathbb{Z}_p$ are either disjoint, or one contains the other.

$\Rightarrow$ disks are both open and closed

$\Rightarrow$ $\mathbb{Z}_p$ totally disconnected, ie. the only non-empty connected subsets are singletons.

Rem One can show that for any top gp G, TFAE:

a) G is profinite

b) G is cpact, Hausdorff, and $1 \in G$ has a nbhood basis of open normal subgps $H \trianglelefteq G$.

c) G is cpact, Hausdorff & totally disconnected.

Def For any gp G, define the profinite topology on G by taking as a nbhood basis the cosets $g \cdot N$ for all normal subgps $N \trianglelefteq G$ w/ $[G:N] < \infty$.

We get a natural hom

$$G \to \hat{G} := \varprojlim_{N} G/N \quad \text{"profinite completion"}$$

sth for every profinite gp H:

$$\mathrm{Hom}(G, H) \simeq \mathrm{Hom}_{\mathrm{cont}}(\hat{G}, H)$$

Caution We can have $G \neq \hat{G}$ even for G profinite:

The topology on a profinite gp $G = \varprojlim G_i$ can be strictly coarser than the profinite one!

Our main example:

$G = \mathrm{Gal}(\tilde{k}/k)$ for a Galois extension $\tilde{k}/k$ of (possibly) infinite degree

We define the Krull topology on $G = \mathrm{Gal}(\tilde{k}/k)$ by taking as a nbhood basis the cosets

$$g \cdot \mathrm{Gal}(\tilde{k}/K) \subset G$$

for K/k a finite Galois extension w/ $K \subset \tilde{k}$.

$$\Rightarrow G \xrightarrow{\sim} \varprojlim_{K/k} \mathrm{Gal}(K/k) \text{ as top. gp}$$

↑ finite Galois w/ $K \subset \tilde{k}$

(The map $G \to \varprojlim \mathrm{Gal}(K/k)$ is surjective since compatible systems of $\sigma_K \in \mathrm{Gal}(K/k)$ fit together to $\sigma \in \mathrm{Gal}(\tilde{k}/k)$ because $\tilde{k} = \bigcup_{K/k} K$. The map is injective since $\sigma|_K = 1 \ \forall K$ implies $\sigma = 1$. The claim about the topology is clear from the def^n because $\mathrm{Gal}(\tilde{k}/K) = \ker(G \to \mathrm{Gal}(K/k))$.)

Ex $k = \mathbb{F}_p \subset \tilde{k} = \overline{\mathbb{F}_p}$

$\Rightarrow G := \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \simeq \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ (gen^{td} by $x \mapsto x^p$)

$\simeq \varprojlim_n \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}$

Note: $N := \mathbb{Z} \subset G = \hat{\mathbb{Z}}$ subgp

w/ fixed field $\tilde{k}^N = k$ but $N \neq G$,

so the naive Galois correspondence fails!

Ex $k = \mathbb{Q} \subset \tilde{k} = \mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n \geq 1} \mathbb{Q}(\zeta_{p^n})$

$\Rightarrow G := \mathrm{Gal}(\tilde{k}/k) \simeq \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$

$\simeq \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^* = \mathbb{Z}_p^*$

For $p \neq 2$ we have $\mathbb{Z}_p^* \simeq \mathbb{F}_p^* \times \underbrace{(1+p\mathbb{Z}_p)^*}_{\simeq (\mathbb{Z}_p, +)}$

Again

$N := \mathbb{F}_p^* \times \mathbb{Z} \subset G = \mathbb{F}_p^* \times \mathbb{Z}_p$ is a subgp

w/ $\tilde{k}^N = k$ but $N \neq G$: No naive Galois corresp.!

In both cases the Krull topology is the profinite one, and the subgp $N \subset G$ is dense. So the problem is that passing from N to its closure in G doesn't change the fixed field. Indeed that's the only problem:

Thm ("infinite Galois correspondence")

Let $\tilde{k}/k$ be a Galois extension (possibly infinite) & $G := \mathrm{Gal}(\tilde{k}/k)$. Then $\exists$ inclusion-reversing bijections

$$\begin{array}{ccc} \{ \text{subextensions } K/k \text{ of } \tilde{k}/k \} & \xrightarrow{\sim} & \{ \text{closed subgps of } G \} \\ \cup & K \mapsto G_K,\ \tilde{k}^H \mapsfrom H & \cup \\ \{ \text{finite subext. } K/k \text{ of } \tilde{k}/k \} & \xrightarrow{\sim} & \{ \text{open subgps of } G \} \end{array}$$

where $G_K := \mathrm{Gal}(\tilde{k}/K) \subset G$.

Pf. • For K/k finite subext. of $\tilde{k}/k$,

let N/k be its Galois hull

$\Rightarrow$ each $g \in G_K$ has the open nbhood

$$g \cdot G_N \subset G_K$$

$\Rightarrow$ G_K open in G for the Krull top.

• Open subgps $H \subset G$ in any top gp are closed,

since $G \setminus H = \bigcup_{g \in G \setminus H} g \cdot H$ is an open subset of G.

$\Rightarrow$ For K/k any subext of $\tilde{k}/k$:

$$G_K = \bigcap_{\substack{K_0 \subset K \\ K_0/k \text{ finite}}} G_{K_0}$$

• The map $K \mapsto G_K \subset G$ is injective

since $K = \{ a \in \tilde{k} \mid \sigma a = a \text{ for all } \sigma \in G \}$.

• For surjectivity let $H \leq G$ be a closed subgp.

We claim $H = G_K$ for $K := \tilde{k}^H$.

The inclusion $H \subset G_K$ is trivial.

Conversely, let $\sigma \in G_K$. We want $\sigma \in H$.

Since $H \subset G$ is closed, it suffices to show that any

basic open $\sigma \cdot G_F$ (with F/k finite) intersects H.

Put $L := F \cdot K$, so L/K is finite w/ $\sigma G_F \supset \sigma G_L$.

Now $H \twoheadrightarrow \mathrm{Gal}(L/K)$ is surjective by Galois theory

for finite extensions, as the image of H in $\mathrm{Gal}(L/K)$

has fixed field $L^H = L \cap \tilde{k}^H = K$.

Pick $\tau \in H$ w/ $\tau|_L = \sigma|_L$

$\Rightarrow$ $\tau \in H \cap \sigma \cdot G_L$ as desired

• Open subgps have finite index in G:

Any open subgp H is closed, so $H = G_K$ w/ $k \subset K \subset \tilde{k}$.

But G is profinite, hence cpact, so it is covered by

fin. many translates of the open subgp $H \subset G$.

$\Rightarrow [G : H] < \infty$ & hence $[K : k] < \infty$. $\square$

Caution The Krull topology on $\mathrm{Gal}(\tilde{k}/k)$ can be strictly coarser than the profinite one, i.e. there may be non-open subgps of finite index:

e.g. take

$k = \mathbb{Q} \subset \tilde{k} = \mathbb{Q}(\sqrt{p} \mid p \in S)$

w/ $S := \{-1\} \cup \{\text{prime numbers}\}$.

$$\Longrightarrow \mathrm{Gal}(\tilde{k}/k) \simeq \prod_{p \in S} \mathbb{Z}/2\mathbb{Z}$$

$\uparrow$ dense

$$H := \bigoplus_{p \in S} \mathbb{Z}/2\mathbb{Z}$$

Axiom of choice: $\exists$ many proper subgps $N \subsetneq G$ of finite index w/ $H \subset N$. Those can't be open!

Rem If a profinite gp G is top. fin. gen, i.e. contains a dense fin. gen. subgp, then every subgp of finite index in G is open. That's a difficult thm!

(Nikolov-Segal, Annals of Math 165 (2007))

An example how to use the Galois correspondence:

Lemma Let $k \subset K_i \subset \tilde{k}$ for $i = 1, \dots, n$.

a) The composite $K := K_1 \cdots K_n \subset \tilde{k}$ has $G_K = G_{K_1} \cap \cdots \cap G_{K_n} \subset G$.

b) The intersection $L := K_1 \cap \cdots \cap K_n \subset \tilde{k}$ has $G_L =$ closure of $\langle G_1, \dots, G_n \rangle \subset G$.

Pf. a) $K_i \subset K \Rightarrow G_K \subset H_i := G_{K_i}$ for all i

$\Rightarrow G_K \subset H_1 \cap \cdots \cap H_n$ (*)

But both sides of (*) are closed in G & $K \subset \tilde{k}^{H_1 \cap \cdots \cap H_n} \underset{(*)}{\subset} \tilde{k}^{G_K} = K$ $\Rightarrow$ equality

b) Let $H :=$ closure of $\langle H_1, \dots, H_n \rangle \subset G$.

Each H_i acts trivially on $L \Rightarrow \langle H_1, \dots, H \rangle \subset G_L$

$\Rightarrow H \subset G_L$ because G_L is closed in G

$\Rightarrow L = \tilde{k}^{G_L} \subset \tilde{k}^{H} \subset \tilde{k}^{H_1} \cap \cdots \cap \tilde{k}^{H_n} =: L$

$G_L \supset H$ $\quad$ $H \supset H_i$ for all i $\Rightarrow$ equality $\square$

3. The axioms of CFT

Fix • $k \subset \bar{k}$ a Galois extension of fields

• $G := \mathrm{Gal}(\bar{k}/k)$ w/ Krull topology:

Closed subgps $G_K := \mathrm{Gal}(\bar{k}/K)$ w/ $k \subset K \subset \bar{k}$,

open subgps those where $[K:k] < \infty$.

Rem More generally one can take G to be any profinite gp, label its open subgps as G_K w/ indices K. Write $K \subset L$ if $G_L \subset G_K$, and define

• $K_1 \cdots K_n$ by $G_{K_1 \cdots K_n} := G_{K_1} \cap \cdots \cap G_{K_n} \subset G$

• $K_1 \cap \cdots \cap K_n$ by $G_{K_1 \cap \cdots \cap K_n} := \overline{\langle G_{K_1}, \ldots, K_n \rangle} \subset G$

• K/k to be normal / cyclic / ... if $G_K \subset G$ is normal / with cyclic quotient / ...

⇒ In abstract CFT we'll deal with the purely group-theoretic part of CFT !

Def We call $A \in \mathrm{Mod}(G)$ a continuous G-module if it satisfies the following equivalent conditions:

a) The action $G \times A \to A$ is continuous when A is given the discrete top.

b) For any $a \in A$ the stabilizer $\mathrm{Stab}_G(a) := \{ g \in G \mid ga = a \} \subset G$ is open

c) We have $A = \bigcup_{\substack{H \subset G \\ \text{open}}} A^H$.

We then put $A_K := A^{G_K}$ for $k \subset K \subset \tilde{k}$ (finite).

Note For $k \subset K \subset L \subset \tilde{k}$ we get $A_K \subset A_L$.

If L/K is normal, put $G_{L/K} := G_K / G_L$ (a finite gp since $[G:G_L] < \infty$), then we get

$$A_L \in \mathrm{Mod}(G_{L/K}).$$

Basic example. $G = \mathrm{Gal}(\tilde{k}/k) \circlearrowright A = \tilde{k}^* \Rightarrow A_L = L^*$

Functoriality of gp coh

- For L/K normal put $H^i(L/K) := H^i_T(G_{L/K}, A_L)$.
- For $K \subset L \subset M$ w/ M/K normal ($\Rightarrow M/L$ normal):
  - $H^i(M/K) \underset{\text{cores}}{\overset{\text{res}}{\rightleftarrows}} H^i(M/L)$ as $G_{M/L} \subset G_{M/K}$
  - inf: $H^i(L/K) \longrightarrow H^i(M/K)$ if L/K also normal

    $\| \qquad\qquad \|$

    $H^i(G_{L/K}, A_L) \longrightarrow H^i(G_{M/K}, A_M)$ $\quad A_L = (A_M)^{G_{M/L}}$, $G_{L/K} = G_{M/K}/G_{M/L}$
- For L/K normal and $\sigma \in G$:

$$\begin{array}{ccc} H & \xrightarrow{c_\sigma} & \sigma H \sigma^{-1} \\ \curvearrowright & & \curvearrowright \\ B & \xrightarrow{\sigma \cdot} & \sigma \cdot B \end{array} \quad \text{w/} \quad \begin{array}{l} H := G_{L/K} \\ B := A_L \\ c_\sigma := \sigma(-)\sigma^{-1} \end{array}$$

Get $\sigma^* : H^i(L/K) \xrightarrow{\sim} H^i(\sigma L/\sigma K)$

by the univ. property of derived functors:

$H^i(H, -) \xrightarrow{\exists!} H^i(\sigma H \sigma^{-1}, \sigma(-))$

derived fctor of $(-)^H$ $\qquad$ δ-functor extending $(-)^H$

For $\sigma H \sigma^{-1} = H$ & $\sigma B = B$ we have $\sigma^* = id$

(exercise, for instance use dim shifting)

Def We call (G, A) a field formation if "Hilbert 90 holds" in the sense that

$$H^1(L/K) = \{1\} \text{ for all } K \subset L.$$

In that case the inflation-restriction sequence for $K \subset L \subset M$ w/ M/K and L/K normal starts in degree 2:

$$1 \to H^2(L/K) \xrightarrow{\text{inf}} H^2(M/K) \xrightarrow{\text{res}} H^2(M/L)$$

$\Rightarrow$ inf: $H^2(L/K) \hookrightarrow H^2(M/K)$ injective

Def In general we put

$$H^i(K) := \varinjlim_{L/K} H^i(L/K) \overset{\text{exercise}}{\simeq} H^i_{\text{cont}}(G_K, A_K)$$

w/ the limit via the inflation maps.

Ex Let (G, A) be a field formation.

$\Rightarrow$ $H^2(L/K) \hookrightarrow H^2(K)$ injective,

and for L/K normal $\exists$ exact sequence

$1 \to H^2(L/K) \xrightarrow{\inf} H^2(K) \xrightarrow{\text{res}} H^2(L)$.

For CFT we want more:

Tate's thm requires for any normal L/K that

a) $H^1(L/K) = 1$ ("field formation")

b) $H^2(L/K)$ is cyclic of order $[L:K] := |G_{L/K}|$.

We also want b) compatible in towers $K \subset L \subset M \subset \cdots$

ie.

$$\begin{array}{ccccccc} H^2(L/K) & \to & H^2(M/K) & \to \cdots \to & H^2(K) & & \\ \downarrow s & & \downarrow s & & & \searrow s & \\ \mathbb{Z}/_{[L:K]} & \dashrightarrow & \mathbb{Z}/_{[M:K]} & & & & \\ \| & & \| & & & & \\ \frac{1}{[L:K]}\mathbb{Z}/_{\mathbb{Z}} & \hookrightarrow & \frac{1}{[M:K]}\mathbb{Z}/_{\mathbb{Z}} & \hookrightarrow \cdots \hookrightarrow & \mathbb{Q}/_{\mathbb{Z}} & & \end{array}$$

Def Let A be a continuous G-module. We call (G, A) a class formation if for all K:

a) $H^1(K) = 1$ $\left(\Leftrightarrow H^1(L/K) = 0 \ \forall \ {}^{L/K}_{\text{normal}}\right)$

b) $\exists$ iso $\text{inv}_K : H^2(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$

(called the "invariant map" for K)

sth for all normal L/K we have:

denote this iso by $\text{inv}_{L/K}$

$$\begin{array}{ccc} H^2(L/K) & \xrightarrow{\sim} & \frac{1}{[L:K]}\mathbb{Z}/_{\mathbb{Z}} \\ \inf \downarrow & & \downarrow \\ H^2(K) & \xrightarrow[\text{inv}_K]{\sim} & \mathbb{Q}/_{\mathbb{Z}} \\ \text{res} \downarrow & & \downarrow [L:K]\cdot \text{id} \\ H^2(L) & \xrightarrow[\text{inv}_L]{\sim} & \mathbb{Q}/_{\mathbb{Z}} \end{array}$$

Ex $G = \mathrm{Gal}(\bar{k}/k)$ for a field k

a) $k = \mathbb{F}_p$, $A = \mathbb{Z}$ w/ trivial G-action

For $K = \mathbb{F}_q$ ($q = p^\nu$) we have

$$H^i(G_K, A_K) := \varinjlim_n H^i(\underbrace{\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)}_{\cong \mathbb{Z}/n\mathbb{Z}}, \mathbb{Z})$$

$\cong \mathbb{Z}/n\mathbb{Z}$ gen'd by Frobenius $\mathrm{Frob}_q = (\mathrm{Frob}_p)^\nu$

For $i > 0$ $\exists$ natural iso

$$H^i(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \simeq \begin{cases} \frac{1}{n}\mathbb{Z}/\mathbb{Z}, & 2 \mid i \\ 0, & 2 \nmid i \end{cases}$$

$\Rightarrow$ $H^1(G_K, A_K) = 0$

$$\begin{array}{ccc} H^2(G_K, A_K) & \xrightarrow{\sim} & \mathbb{Q}/\mathbb{Z} \\ \cup & & \cup \\ H^2(G_{L/K}, A) & \xrightarrow{\sim} & \frac{1}{m}\cdot\mathbb{Z}/\mathbb{Z} \end{array}$$

for $L = \mathbb{F}_{q^m} \supset K = \mathbb{F}_q$

$\Rightarrow$ (G, A) is a class formation.

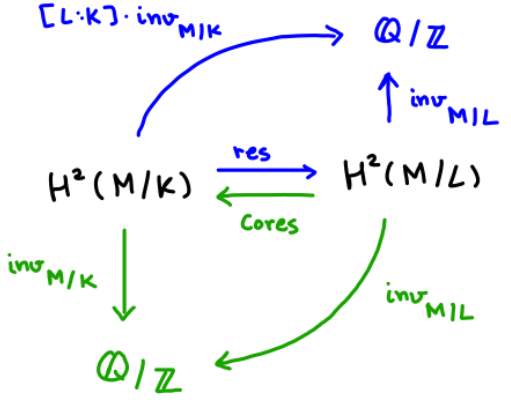
b) Local CFT: $k/\mathbb{Q}_p$ finite, $A_k = K^*$

c) Global CFT: $k/\mathbb{Q}$ finite, $A_k = C_k$ (C_k = idele class gp)

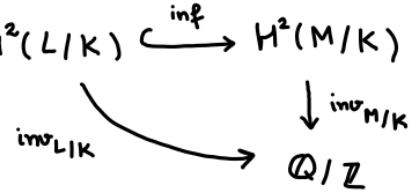
} see later...

Summary of functoriality for a class formation:

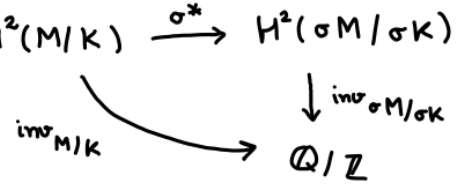
a) For any $K \subset L \subset M$ w/ M/L normal:



b) If L/K is also normal:



c) For $\sigma \in G$:



Pf. • For inf and res: clear by class formation axiom.

• For cores use that by the axiom res is surjective,
so for $c \in H^2(M,L)$ $\exists\, \tilde{c} \in H^2(M,K)$ w/ $c = \operatorname{res}\tilde{c}$

$$\Rightarrow \quad \operatorname{inv}(\operatorname{cores} c)$$

$$= \operatorname{inv}_{M/K}(\underbrace{\operatorname{cores}(\operatorname{res}(\tilde{c}))}_{= \tilde{c}^{[L:K]} \text{ in multiplicative notation}})$$

$$= [L:K] \cdot \operatorname{inv}_{M/K} \tilde{c}$$

$$= \operatorname{inv}_{M/L}(\underbrace{\operatorname{res}\tilde{c}}_{=c}) \quad \text{by the axiom for res.}$$

• For σ^* consider the base field k (given by $G_k = G$).
Let N/k be the normal closure of N/k.

$$\Rightarrow \sigma N \sigma^{-1} = N \;\&\; \sigma A_N = A_N$$

$$\Rightarrow \quad \sigma^* = \mathrm{id} : H^2(N/k) \xrightarrow{\sim} H^2(\sigma N/\sigma k) = H^2(N/k)$$

$$\Rightarrow \operatorname{inv}_{\sigma M/\sigma K}(\sigma^* c) = \operatorname{inv}_{N/\sigma K}(\sigma^* c)$$

$$= \operatorname{inv}_{N/k}(\underbrace{\operatorname{cores}\sigma^* c}_{= \sigma^* \operatorname{cores} c = \operatorname{cores} c})$$

$$= \operatorname{inv}_{N/k} \operatorname{cores} c$$

$$= \operatorname{inv}_{N/K} c$$

$$= \operatorname{inv}_{M/K} c \qquad \square$$

4. The Artin isomorphism

Let $(G, A, \operatorname{inv})$ be a class formation.

Def For L/K normal, the fundamental class $u_{L/K}$ is defined by

$$\begin{array}{ccc} u_{L/K} & \in & H^2(L/K) \\ \downarrow & & \downarrow \operatorname{inv}_{L/K} \\ \frac{1}{[L:K]} & \in & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \end{array}$$

Basic properties For $K \subset L \subset M$ w/ M/K normal,

a) $\operatorname{res}(u_{M/K}) = u_{M/L}$,

$\operatorname{cores}(u_{M/L}) = (u_{M/K})^{[L:K]}$

b) If L/K is also normal,

$u_{L/K} = (u_{M/K})^{[N:L]}$

c) For $\sigma \in G$,

$\sigma^* u_{M/K} = u_{\sigma M/\sigma K}$.

Pf. Apply $\operatorname{inv}(-)$ & use the "summary" above.

For instance

$$\operatorname{inv}_{L/K}(\operatorname{res} u_{M/K}) = [L:K] \cdot \operatorname{inv}_{M/K}(u_{M/K})$$
$$= \frac{[L:K]}{[M:K]} + \mathbb{Z}$$
$$= \frac{1}{[M:L]} + \mathbb{Z} = \operatorname{inv}_{M/L}(u_{M/L}).$$

The other parts are similar. □

For L/K normal, Tate's thm gives a canonical iso

$$u_{L/K} \cup (-): \; H_T^i(G_{L/K}, \mathbb{Z}) \xrightarrow{\sim} H_T^{i+2}(L/K)$$

Special case: For $i = -2$ we get

$$\begin{array}{ccc} H_T^{-2}(G_{L/K}, \mathbb{Z}) & \xrightarrow{u_{L/K} \cup (-)} & H_T^0(L/K) \\ \| & & \| \\ \theta_{L/K}: \; G_{L/K}^{ab} & \xrightarrow{\sim} & A_K/N_{L/K}(A_L) \end{array}$$

We call $\theta_{L/K}$ the "Nakayama map"

Rem For $u_{L/K} = [u]$ w/ $u \in Z^2(G_{L/K}, A_L)$ and $[g] \in G_{L/K}^{ab}$ we have

$$\theta_{L/K}([g]) = \prod_{h \in G_{L/K}} u(h, g) \bmod N_{L/K}(A_L)$$

by the formula for cup products in low degree from the end of the previous chapter.

Def The Artin map (or reciprocity map) for a normal extension L/K is the inverse

$$\mathrm{Art}_{L/K} := \theta_{L/K}^{-1} : A_K/N_{L/K}(A_L) \xrightarrow{\sim} G_{L/K}^{ab}.$$

The norm residue symbol $(\cdot, L/K)$ is defined by

$$\begin{array}{ccc} A_K & \xrightarrow{(\cdot, L/K)} & \\ \downarrow & & \\ A_K/N_{L/K}(A_L) & \xrightarrow[\mathrm{Art}_{L/K}]{\sim} & G_{L/K}^{ab} \end{array}$$

Thus for $a \in A_K$:

$$a \in N_{L/K}(A_L) \iff (a, L/K) = 1.$$

(slogan: $(a, L/K)$ captures the "residue class of a mod norms")

Next we'll put together the $(\cdot, L/K)$ to a homom. $A_K \to G_K^{ab} = \varprojlim G_{L/K}^{ab}$. For this we need to check compatibility of norm residue symbols in towers...

5. Compatibilities in towers

Let L/K be normal.

To control $(\cdot, L/K) : A_K \to G_{L/K}^{ab}$ we test w/ characters

$$\chi \in \hat{G}_{L/K} := \mathrm{Hom}(G_{L/K}^{ab}, \mathbb{Q}/\mathbb{Z}) = H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z})$$

(for $g \in G_{L/K}^{ab}$ we have: $g = 1 \iff \forall \chi : \chi(g) = 1$)

Lemma For $\chi \in \hat{G}_{L/K}$ consider $\delta\chi \in H^2(G_{L/K}, \mathbb{Z})$

($\delta : H^1(G_{L/K}, \mathbb{Q}/\mathbb{Z}) \xrightarrow[\text{map}]{\text{boundary}} H^2(G_{L/K}, \mathbb{Z})$)

Then the diagram below commutes:

$$\begin{array}{ccc} A_K & \xrightarrow{(\cdot, L/K)} & G_{L/K}^{ab} \\ \downarrow{\scriptstyle (-)\cup\delta\chi} & & \downarrow{\scriptstyle \chi} \\ H^2(L/K) & \xrightarrow{\mathrm{inv}_{L/K}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Pf. Put $\sigma_a := (a, L/K) \longmapsto \bar{\sigma}_a$

$$\begin{array}{ccc} \cap & & \cap \\ G_{L/K}^{ab} & \xrightarrow{\sim} & H_T^{-2}(G_{L/K}, \mathbb{Z}) \end{array}$$

By def of $(\cdot, L/K)$ we have

$$[a] = u_{L/K} \cup \bar{\sigma}_a \in H_T^0(G_{L/K}, A_L) = A_L/\dots$$

$$\Rightarrow [a] \cup \delta\chi = (u_{L/K} \cup \bar{\sigma}_a) \cup \delta\chi$$

$$= u_{L/K} \cup (\bar{\sigma}_a \cup \delta\chi)$$

$$= u_{L/K} \cup \delta(\bar{\sigma}_a \cup \chi)$$

(since $\cup$ is compatible w/ boundary map)

$$= u_{L/K} \cup \delta(\chi(\sigma_a))$$

(by formula for cup product in low degree, here $\bar{\sigma}_a \in H_T^{-2}$ and $\chi \in H_T^1 \dots$)

Put $n = [L:K]$

$$\Rightarrow \begin{array}{ccccc} H_T^{-1}(G_{L/K}, \mathbb{Q}/\mathbb{Z}) & = & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & \ni & \chi(\sigma_a) =: \frac{r}{n} + \mathbb{Z} \\ \downarrow \delta & & \downarrow \cdot n & & \\ H_T^0(G_{L/K}, \mathbb{Z}) & = & \mathbb{Z}/n\mathbb{Z} & & \\ \downarrow u_{L/K} \cup (-) & & \downarrow \cdot 1/n & & \\ H_T^2(G_{L/K}, \mathbb{Z}) & \xrightarrow[inv_{L/K}]{} & \frac{1}{n}\mathbb{Z}/\mathbb{Z} & & \end{array} \quad \text{id}$$

□

Cor Let $K \subset L \subset M$ with M/K and L/K normal, then the following diagram commutes:

$$\begin{array}{ccc} & & G_{M/K}^{ab} \\ & \overset{(\cdot, M/K)}{\nearrow} & \downarrow pr \\ A_K & \xrightarrow[(\cdot, L/K)]{} & G_{L/K}^{ab} \end{array}$$

Pf. Apply arbitrary characters $\chi \in \hat{G}_{L/K} \subset \hat{G}_{M/K}$ via the previous lemma & use compatibilities of inv_K. □

Passing to $G_K^{ab} = \left(\varprojlim_M G_{M/K}\right)^{ab} = \varprojlim_M G_{M/K}^{ab}$ we thus get a map

$$(\cdot, K) : A_K \longrightarrow G_K^{ab}$$

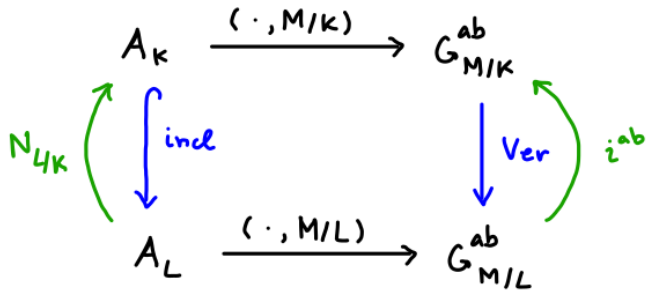
called the "universal norm residue symbol" sth for all normal L/K:

$$\begin{array}{ccccc} A_K & \xrightarrow{(\cdot, K)} & G_K^{ab} & \xrightarrow{pr} & G_{L/K}^{ab} \\ & \searrow & & \nearrow & \\ & & (\cdot, L/K) & & \end{array}$$

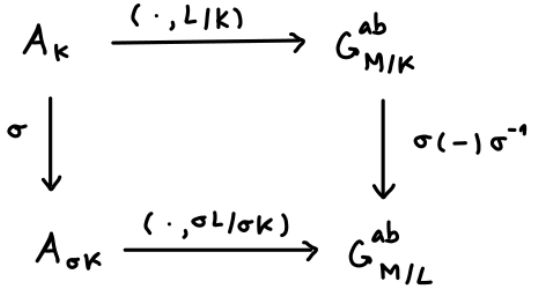
Further compatibilities:

a) For $K \subset L \subset M$ w/ M/L normal,

$i: G_{M/L} \hookrightarrow G_{M/K}$, the diagrams using either the blue or the green arrows commute:



b) For $\sigma \in G$ we have:



Pf. Exercise – here you don't need the lemma. □

6. Norm groups

CFT gives an "intrinsic" description of

G_K^{ab} (= Galois gp of the maximal abelian extension of K if $G_K = \mathrm{Gal}(\bar{K}/K)$)

in terms of subgps of A_K (eg $= K^*$ in local CFT & $= C_K$ in global CFT)

Def A subgp $H \subset A_K$ is called a norm subgp if $\exists$ normal L/K sth

$$H = N_{L/K}(A_L) \ (= \ker(\cdot, L/K)).$$

We then get an iso

$$\mathrm{Art}_{L/K} : A_K/H \xrightarrow{\sim} G^{ab}_{L/K}.$$

Def The universal norm subgp for K is

$$N_K := \bigcap_{L/K} N_{L/K}(A_L) \subset A_K.$$

Thm ("Artin reciprocity, universal version")

The universal norm residue symbol $(\cdot, K)$ has kernel $\ker(\cdot, K) = N_K$, hence it induces a diagram

$$\begin{array}{ccc} A_K/N_K & \xrightarrow[\mathrm{Art}_K]{} & G_K^{ab} \\ \downarrow{\scriptstyle pr} & & \downarrow{\scriptstyle pr} \\ A_K/N_{L/K}(A_L) & \xrightarrow[\mathrm{Art}_{L/K}]{\sim} & G_{L/K}^{ab} \end{array}$$

where Art_K is an embedding w/ dense image.

Ex $G = \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \curvearrowright A = \mathbb{Z}$

Say $K = \mathbb{F}_q \subset L = \mathbb{F}_{q^m}$:

$$\begin{array}{ccccc} A_K/N_K = \mathbb{Z} & \xrightarrow{\text{dense}} & G_K^{ab} & = & \hat{\mathbb{Z}} \\ \downarrow & & & & \downarrow \\ A_K/N_{L/K}A_L = \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\sim} & G_{L/K}^{ab} & = & \hat{\mathbb{Z}}/m\hat{\mathbb{Z}} \end{array}$$

Pf of the thm.

- $(a, K) = 1 \in \varprojlim G_{L/K}^{ab}$

  $\Leftrightarrow \forall\, L/K$ normal : $(a, L/K) = 1$

  $\Leftrightarrow \forall\, L/K$ normal : $a \in N_{L/K}(A_L)$

  $\Leftrightarrow a \in N_K$

- Density of image of $(\cdot, K) : A_K \to G_K^{ab}$:

  Let $\sigma \in G_K^{ab}$

  The σH w/ $H \subset G_K^{ab}$ open subgp form a nbhood basis of σ in G_K^{ab}

  For any such H, $\exists\, L/K$ normal (& finite) s.th. $G_K/H \simeq G_{L/K}$.

  But $(\cdot, L/K) : A_K \twoheadrightarrow G_{L/K}$ epi

  $\Rightarrow \exists a \in A_K : (a, L/K) = \sigma H$ in G_K/H

□

Upshot The abelian extensions L/K are completely determined by the norm subgroups of A_K.

We can't do any better, nonabelian extensions are not seen by norm subgps:

Cor ("norm restriction thm")
For L/K normal let $M = L \cap K^{ab} \subset L$ denote the max. abelian extension of K in L, then $N_{L/K}(A_L) = N_{M/K}(A_M)$ in A_K.

Pf. "$\subset$" clear since $N_{L/K} = N_{M/K} \circ N_{L/M}$.

"$=$" then follows from Artin reciprocity:

$$A_K/N_{L/K}(A_L) \simeq G_{L/K}^{ab} = G_{M/K} \simeq A_K/N_{M/K}(A_M)$$

$$\Rightarrow [A_K : N_{L/K}(A_L)] = [A_K : N_{M/K}(A_M)] < \infty$$

□

Thus norm subgps detect if an extension is abelian:

Cor $[A_K : N_{L/K}(A_L)]$ divides $[L : K]$.
Both are equal iff L/K is abelian.

Pf. For $M = L \cap K^{ab}$ the previous corollary gives $[A_K : N_{L/K}(A_L)] = [M : K]$. □

Cor Get an inclusion-reversing bijection

$$\left\{ \begin{array}{l} \text{abelian} \\ \text{ext}^{\text{s}} \text{ of } K \end{array} \right\} \longrightarrow \left\{ \begin{array}{r} \text{norm subgps} \\ \text{of } A_K \end{array} \right\}$$

$$L/K \longmapsto N(L) := N_{L/K}(A_K).$$

sth
- $N(L_1 \cdot L_2) = N(L_1) \cap N(L_2)$,
- $N(L_1 \cap L_2) = N(L_1) \cdot N(L_2)$.

Pf. Exercise. □

The only question left for a description of abelian extensions L/K in terms intrinsic to K is:

Q: Which subgps of A_K are norm subgps?

In local & global CFT the gp A_K will come w/ a natural topology:

- $A_K = K^*$ for a local field K w/ p-adic top
- $A_K = C_K$ idèle class gp w/ top from idèles.

In both cases the answer will be:

Thm ("existence thm") In those cases, the norm subgps are precisely the closed subgps $N \subset A_K$ of finite index.

This can again be axiomatized, but we'll check it by hand in the two cases.
"Existence" refers to $\exists L/K$ w/ given norm subgp

III. Local CFT

1. Motivation: Brauer gps ← (not needed in what follows)

k any field

$\bar{k}/k$ algebraic closure

$G = Gal(\bar{k}/k)$

Which $A \in Mod(G)$ should we take?

Rem $A := (\bar{k}, +)$ (additive gp) gives nothing,

since $H^\bullet(G, (\bar{k}, +)) = 0$.

Pf. Let L/K Galois w/ $k \subset K \subset L \subset \bar{k}$.

Normal basis thm: $\exists a \in L$ s.th. $(\sigma(a))_{\sigma \in G_{L/K}}$

is a basis of the K-vector space L

$\Rightarrow (L, +) = \bigoplus_\sigma K \cdot \sigma(a) = \bigoplus_\sigma \sigma \cdot (K \cdot a) = Ind_1^{G_{L/K}}(K)$ □

How about $A = \bar{k}^*$ (multiplicative gp)?

Hilb 90 $\Rightarrow H^1(G_{L/K}, L^*) = 0 \ \forall L/K$

$\Rightarrow (G, \bar{k}^*)$ is a field formation.

Here H^2 has an interpretation via csa:

Def A k-algebra A (associative unital of $\dim < \infty$) is called

- central if it has center $Z(A) = k$,
- simple if it has no 2-sided ideals $\neq 0, A$.

If both properties are satisfied, we call A a central simple algebra (csa) over the field k.

Ex

- $A = \mathbb{C}$ is a csa over $\mathbb{C}$ but not over $\mathbb{R}$.
- $A = \mathbb{H}$ (quaternions) is a csa / $\mathbb{R}$ but not / $\mathbb{C}$.
- $A = Mat_{n \times n}(k)$ is a csa over k (any $n \in \mathbb{N}$).

More generally, let $\mathbb{D}$ be a division algebra over k

(ie a k-algebra sth $\forall a \in \mathbb{D}\setminus\{0\}\ \exists\, b \in \mathbb{D} : ab = ba = 1$)

$\Rightarrow$ $A := \mathrm{Mat}_{n\times n}(\mathbb{D})$ is a simple k-algebra

Pf. $J \trianglelefteq A$ 2-sided ideal & $0 \neq M = (m_{ij}) \in J$

$\Rightarrow$ $\exists\, i_0, j_0 : m_{i_0 j_0} \neq 0$

But $E_{ii_0} \cdot M \cdot E_{j_0 j} = m_{i_0 j_0} \cdot E_{ij}$ lies in J

(E_{ii_0}: elementary matrix w/ 1 in position (i,i_0), 0 everywhere else)

$\Rightarrow$ $E_{ij} \in J$ for all i,j, hence $J = A$. $\square$

Conversely one has:

Thm (Artin-Wedderburn) Any simple k-algebra A is $\simeq \mathrm{Mat}_{n\times n}(\mathbb{D})$ for a unique (up to iso) division algebra $\mathbb{D}$ and a unique $n \in \mathbb{N}$.

It is a csa over k iff $Z(\mathbb{D}) = k$.

Pf. $\dim_k A < \infty \Rightarrow \exists$ minimal left ideal $0 \neq J \trianglelefteq A$

Then J is a simple A-module

$\Rightarrow$ $\tilde{\mathbb{D}} := \mathrm{End}_A(J)$ is a division algebra

(by "Schur's lemma":

$f \in \tilde{\mathbb{D}}\setminus\{0\} \Rightarrow f : J \to J$ nonzero,

$\Rightarrow \ker f = 0,\ \mathrm{im} f = J$

because J is simple

$\Rightarrow f$ iso, ie $\exists f^{-1} \in \tilde{\mathbb{D}}$)

Since $\dim_k J < \infty$,

J is a fin. gen. module over $\tilde{\mathbb{D}}$,

so $J \simeq \tilde{\mathbb{D}}^n$ for some n (same pf over division algebras as over fields)

$\Rightarrow$ $\mathrm{End}_{\tilde{\mathbb{D}}}(J) \simeq \mathrm{Mat}_{n\times n}(\mathbb{D})$ for $\mathbb{D} := \tilde{\mathbb{D}}^{op}$

Here

$\mathrm{End}_{\tilde{D}}(J) \subset E := \mathrm{End}_k(J)$

is the centralizer

$C_E(\tilde{D}) := \{ f \in E \mid \forall d \in \tilde{D} : df = fd \}$.

Likewise $\tilde{D} = \mathrm{End}_A(J) = C_E(A)$.

$\Rightarrow \quad A \overset{\simeq}{} C_E(C_E(A)) = \mathrm{End}_{\tilde{D}}(J) = \mathrm{Mat}_{n\times n}(D)$

by "double centralizer thm":

A simple k-algebra,

$M \in \mathrm{Mod}(A)$ faithful (ie $A \hookrightarrow \mathrm{End}_A(M)$ inj.)

and simple (ie M has no A-submodule $\neq 0, M$)

$\Rightarrow$ For $E := \mathrm{End}_k(M)$, have iso

$$A \xrightarrow{\sim} C_E(C_E(A))$$

(Proof is linear algebra, see e.g. Milne, CFT, th. IV.1.14)

Uniqueness of D:

The minimal left ideals of $\mathrm{Mat}_{n\times n}(D)$ are

$J_\nu := \{$ matrices that are zero outside the ν-th column $\}$

for $1 \le \nu \le n$, all $\simeq D^n$ as $\mathrm{Mat}_{n\times n}(D)$-modules.

$\Rightarrow$ If $A \simeq \mathrm{Mat}_{n\times n}(D)$, then

$D^{op} \simeq \mathrm{End}_{\mathrm{Mat}_{n\times n}(D)}(D^n) \simeq \mathrm{End}_A(J)$

for any minimal left ideal $J \trianglelefteq A$

$\Rightarrow$ $D = (D^{op})^{op}$ unique up to iso

& then n is determined by

$\dim_k A = n^2 \cdot \dim_k D$. $\square$

Def Two csa A, B over k are <u>equivalent</u>

(notation: $A \sim B$) if $\exists\, m, n$:

$A \simeq \mathrm{Mat}_{m\times m}(D)$ for the same central

$B \simeq \mathrm{Mat}_{n\times n}(D)$ division algebra D.

Fact For any csa A, B over k,

- $A \otimes_k B$ is again a csa over k,
- $B \sim C \Rightarrow A \otimes_k B \sim A \otimes_k C$
- $A \otimes A^{op} \sim k$

(indeed $A \otimes_k A^{op} \simeq \mathrm{End}_k(A) \simeq \mathrm{Mat}_{n\times n}(k)$ for $n = \dim_k A$)

Cor $\mathrm{Br}(k) := \{\text{csa over } k\}/\sim$

is an abelian gp wrt "$\otimes$"

We call it the <u>Brauer group</u> of k.

Thm $\exists$ natural iso

$$\varphi: H^2(k) := H^2(\mathrm{Gal}(\bar{k}/k), \bar{k}^*) \xrightarrow{\sim} \mathrm{Br}(k)$$

obtained as follows:

Given $[c] \in H^2(G, K^*) \subset H^2(k)$

for K/k finite Galois w/ gp G & $c \in Z^2(G, K^*)$,

put

$$A := \bigoplus_{\sigma \in G_{K/k}} K \cdot e_\sigma \quad \text{as vector space } / k,$$

(e_σ: formal basis vector)

w/ multiplication

$$e_\sigma \cdot a := (\sigma(a)) \cdot e_\sigma \qquad (a \in K,$$

$$e_\sigma \cdot e_\tau := c(\sigma,\tau) \cdot e_{\sigma\tau} \qquad \sigma, \tau \in G)$$

Then A is a csa over k, and we put

$$\varphi([c]) := [A] \in \mathrm{Br}(k).$$

(Proof e.g. in Milne, CFT, sect. IV.3)

Ex $k = \mathbb{R}$, $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z} = \langle \sigma \rangle$ (cplex conjugation)

$\Rightarrow H^2(G, \mathbb{C}^*) \simeq \{\pm 1\}$

generated by $c \in Z^2(G, \mathbb{C}^*)$

w/

$$c(g,h) := \begin{cases} -1 & \text{if } g = h = \sigma \\ +1 & \text{else} \end{cases}$$

$\Rightarrow \exists!$ nontrivial central division algebra / $\mathbb{R}$

The theorem describes it as $A := \mathbb{C} \cdot e_1 \oplus \mathbb{C} \cdot e_\sigma$

w/ multiplication given by (for $a \in \mathbb{C}$):

$\cdot$	a	e_1	e_σ
e_1	$a e_1$	e_1	e_σ
e_σ	$\bar{a} e_\sigma$	e_σ	$-e_1$

$\Rightarrow A \simeq \mathbb{H} = \mathbb{C} \oplus \mathbb{C} \cdot j$ w/ $ij = -ji$, $j^2 = -1$.

$e_1 \mapsto 1$

$e_\sigma \mapsto j$

(the quaternions)

Ex ("Splitting fields")

The description of φ in the thm gives for any finite extension K/k a comm. diagram:

$$\begin{array}{ccccc} H^2(k) & \xrightarrow{\sim} & \mathrm{Br}(k) & \ni & [A] \\ \downarrow & & \downarrow & & \downarrow \\ H^2(K) & \xrightarrow{\sim} & \mathrm{Br}(K) & \ni & [A \otimes_k K] \end{array}$$

$\Rightarrow$ From $H^2(k) = \bigcup_{K/k} H^2(K/k)$ we get

$$\mathrm{Br}(k) = \bigcup_{K/k} \mathrm{Br}(K/k)$$

w/ $\mathrm{Br}(K/k) := \ker(\mathrm{Br}(k) \to \mathrm{Br}(K))$.

$\Rightarrow$ For any csa A over k, $\exists$ finite K/k sth

$$A \otimes_k K \simeq \mathrm{Mat}_{n \times n}(K) \quad (\text{w/ } n^2 = \dim_k A).$$

In particular $\mathrm{Br}(k) = 0$ for k alg. closed.

Towards local CFT (historic view):

- Let k be finite extension of $\mathbb{Q}_p$,
  w/ discrete valuation $v : k^* \twoheadrightarrow \mathbb{Z}$.
- For any finite ext^n K/k, the valuation v
  extends to a unique discrete val $v : K^* \to \mathbb{Q}$,
  and K/k is unramified iff $v(K^*) = \mathbb{Z}$.
- For a central division algebra D over k,
  any $a \in D^*$ lies in the field $K = k[a] \subset D$
  & we define $v(a) \in \mathbb{Q}$ as above.

  $\Rightarrow$ We get a homom. $v : D^* \to \mathbb{Q}$.

Fact $\exists$ subfield $K \subset D$ sth
a) K/k is unramified, and
b) K is a splitting field for D.

By a) $\exists$ Frobenius $\sigma \in \mathrm{Aut}(K/k)$.

Now apply Noether-Skolem thm:

> S simple k-alg, A csa over k, then any
> two k-algebra hom $f, g : S \to A$ are conjugate:
> $\exists\, a \in A^* \;\; \forall\, x \in S : \quad g(x) = a \cdot f(x) \cdot a^{-1}$

Taking $S = K \xrightarrow[g = f \circ \sigma]{f} A = D$ we get:

$\exists\, a \in D^* \;\; \forall\, x \in K : \quad \sigma(x) = a\, x\, a^{-1}$

We then define $\mathrm{inv}(D) := (v(a) + \mathbb{Z}) \in \mathbb{Q}/\mathbb{Z}$

(note: if also $\sigma(x) = \tilde{a}\, x\, \tilde{a}^{-1}$ for all $x \in K$,
then $\tilde{a}/a \in K^*$ & hence $v(\tilde{a}) \equiv v(a) \bmod \mathbb{Z}$)

$\rightsquigarrow$ $\mathrm{inv} : \mathrm{Br}(k) \to \mathbb{Q}/\mathbb{Z}$, $[D] \mapsto \mathrm{inv}(D)$.

... many things to check on the way.
We'll stay with gp cohom & not use $\mathrm{Br}(k)$!

2. The multiplicative gp of local fields

k finite extension of $\mathbb{Q}_p$

$v : k \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ discrete valuation

$\mathcal{O}_k = \{x \in k \mid v(x) \geq 0\}$

$\cup$

$\mathfrak{p} = \{x \in k \mid v(x) > 0\} = (\pi)$ (any $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$)

$\mathbb{F}_k = \mathcal{O}_k / \mathfrak{p}$ ("residue field")

Absolute value ($\rightsquigarrow$ topology on k)

$|x|_{\mathfrak{p}} := q^{v(x)}$ w/ $q := |\mathbb{F}_k| = [\mathcal{O}_k : \mathfrak{p}]$

$= \frac{1}{N(x)}$ w/ $N(x) := [\mathcal{O}_k : x\mathcal{O}_k]$

↑ for $x \in \mathcal{O}_k$

Have split exact sequence

$$1 \to \mathcal{O}_k^* \to k^* \xrightarrow{v} \mathbb{Z} \to 0$$

$p^n \hookleftarrow n$

The unit gp $U := \mathcal{O}_k^*$ can be understood via the exact sequence

reduction mod $\mathfrak{p}$

$$1 \to U_1 \to U \xrightarrow{\varsigma} \mathbb{F}^* \to 1$$

$U_1 = 1 + \mathfrak{p}$ "group of 1-units"

$\mathbb{F}^* = \mathbb{F}_k^*$

Rem $\exists$ canonical splitting $U \simeq U_1 \times \mathbb{F}^*$:

On $\mu_{q-1}(k) = \{a \in U \mid a^{q-1} = 1\} \subset U$

the reduction map ς restricts to an iso

$$\varsigma : \mu_{q-1}(k) \xrightarrow{\sim} \mathbb{F}^*$$

(apply Hensel's lemma to $f(x) = x^{q-1} - 1$).

Its inverse $\tau : \mathbb{F}^* \xrightarrow{\sim} \mu_{q-1}(k) \subset U$

is called the Teichmüller lift.

The next layer are the "higher unit gps":

$$U = \mathcal{O}_k^* \supset U_1 = 1+\mathfrak{p} \supset \cdots \supset U_n = 1+\mathfrak{p}^n \supset \cdots$$

$\| \qquad\qquad \| \qquad\qquad\qquad\qquad \|$

$U(k) \qquad U_1(k) \qquad\qquad U_n(k)$

Lemma $U_n/U_{n+1} \simeq (\mathbb{F}, +)$ for all $n \geq 1$.

Pf. By def^n

$U_n \twoheadrightarrow (\mathbb{F},+)$, $1+a\pi^n \mapsto a$ w/ $\ker = U_{n+1}$

(note $(1+a\pi^n)(1+b\pi^n) \equiv 1+(a+b)\pi^n \bmod \pi^{n+1} \ldots$) □

Cor $U \subset k^*$ is a compact open,

hence k^* is locally compact.

Pf. By the above the U/U_n are finite gps.

$\Rightarrow U = \varprojlim U/U_n$ profinite, hence cpact.

By def^n U is also open in k^*. □

The complete description:

Thm ("structure of local unit gps")

$\exists$ iso of top gps

$$k^* \simeq \mathbb{Z} \times \mu(k) \times \mathbb{Z}_p^{\oplus r}$$

w/ $r = [k : \mathbb{Q}_p]$

& $\mu(k) = \{a \in k^* \mid \exists\, v : a^v = 1\}$

finite cyclic of order $(q-1)\cdot p^s$ (some s).

Pf. For $u \in U_1$ and $a = \lim_{n\to\infty} a_n \in \mathbb{Z}_p$ $(a_n \in \mathbb{Z})$, put

$$u^a := \lim_{n\to\infty} u^{a_n} \in U_1 = \varprojlim_n U_1/U_n.$$

$\rightsquigarrow U_1$ a continuous $\mathbb{Z}_p$-module via exponentiation

We'll show via p-adic Lie theory that it is fin. gen, hence a direct sum of a torsion part and a free $\mathbb{Z}_p$-module of finite rank.

Claim: For $x \in \mathcal{O}_k$, the series

- $\log(1+x) := \sum_{a \geq 1} (-1)^{a+1} \cdot \frac{x^a}{a}$ converges for $v(x) > 0$,
- $\exp(x) := \sum_{a \geq 0} \frac{x^a}{a!}$ converges for $v(x) > \frac{v(p)}{p-1}$,

and for $n \gg 0$ large enough they give continuous isos of $\mathbb{Z}_p$-modules

$$U_n \underset{\exp}{\overset{\log}{\rightleftarrows}} p^n$$

U_n: multiplicative gp; p^n: additive gp

Indeed, this follows since for $a = p^e b$ $(p \nmid b)$,

- $v(a) = e \cdot v(p) \leq v(p) \cdot \log_p(a)$

  $\Rightarrow v(\frac{x^a}{a}) \geq a \cdot v(x) - v(p) \cdot \log_p(a) \to \infty$ if $v(a) > 0$

- $v(a!) = v(p) \cdot (\lfloor \frac{a}{p} \rfloor + \lfloor \frac{a}{p^2} \rfloor + \cdots) \leq v(p) \cdot \frac{a/p}{1-1/p} = \frac{v(p) \cdot a}{p-1}$

  $\Rightarrow v(\frac{x^a}{a!}) \geq a \cdot (v(x) - \frac{v(p)}{p-1}) \to \infty$ if $v(x) > \cdots$

& using the strong triangle inequality.

Upshot: $U_n \simeq p^n$ for $n \gg 0$

But $p^n \xrightarrow{\sim} \mathcal{O}_k$ via $a \mapsto a/\pi^n$

& $\mathcal{O}_k \simeq \mathbb{Z}_p^{\oplus r}$ as $\mathbb{Z}_p$-module, for $r = [k : \mathbb{Q}_p]$.

$\Rightarrow U_n$ is a free $\mathbb{Z}_p$-module of rank r (for $n \gg 0$)

But $[U_1 : U_n] < \infty$ for all n (previous lemma),

so we get:

$U_1 \supset$ free $\mathbb{Z}_p$-submodule of rk r w/ finite index

$\Rightarrow U_1$ fin. gen. $\mathbb{Z}_p$-module

whose free part has rank r

& whose torsion part is cyclic (since $\subset k^*$)

of the form $\mathbb{Z}_p/p^s\mathbb{Z}_p \simeq \mathbb{Z}/p^s\mathbb{Z}$ for some s.

This finishes the pf as $k^* \simeq \mathbb{Z} \times \mu_{q-1}(k) \times U_1$. $\square$

Cor Let $m > 0$ & $v := v(m)$. For all $n \gg 0$

have iso $U_n \xrightarrow{\sim} U_{n+v}$, $x \mapsto x^m$.

Pf. Applying log on both sides for $n \gg 0$,

we have $\mathfrak{p}^n \xrightarrow{\sim} \mathfrak{p}^{n+v}$, $y \mapsto m \cdot y$. □

Cor The m-th powers are open subgps $k^{*m} \subset k^*$

of index $[k^* : k^{*m}] = m \cdot q^{v(m)} \cdot |\mu_m(k)|$

Pf. By the thm
$$\begin{array}{ccc} k^* & \simeq & \mathbb{Z} \times \mu(k) \times \mathbb{Z}_p^r \\ \cup & & \\ k^{*m} & \simeq & m\mathbb{Z} \times \mu(k)^m \times m\mathbb{Z}_p^r \end{array}$$

w/ $[\mu(k) : \mu(k)^m] = |\mu_m(k)|$

$[\mathbb{Z}_p^r : m\mathbb{Z}_p^r] = p^{v_p(m) \cdot r} = q^m$

$r = [k : \mathbb{Q}_p] = e \cdot f$ for $q = p^f$ and $v(m) = e \cdot v_p(m)$

□

3. Local CFT : The unramified case

$\mathbb{Q}_p \subset k \subset K$ finite extensions

Recall :

- inertia degree $f_{K/k} := [\mathbb{F}_K : \mathbb{F}_k]$

  w/ $\mathbb{F}_k = \mathcal{O}_k / \mathfrak{p}_k \hookrightarrow \mathbb{F}_K = \mathcal{O}_K / \mathfrak{p}_K$

- ramification index $e_{K/k} \geq 0$

  defined by the comm. diagram of normalized discrete valuations:

$$\begin{array}{ccc} K^* & \xrightarrow{v_K} & \mathbb{Z} \\ \uparrow & & \uparrow \cdot e_{K/k} \\ k^* & \xrightarrow{v_k} & \mathbb{Z} \end{array}$$

- Basic formula: $[K : k] = e_{K/k} \cdot f_{K/k}$.

Def We call K/k **unramified**

if $e_{K/k} = 1$, i.e. $f_{K/k} = [K : k]$.

Unramified extensions are described completely by extensions of the residue field:

Thm a) For any finite extension $\mathbb{F}/\mathbb{F}_k$, $\exists$ unique (up to iso) finite unramified extension K/k with $\mathbb{F}_K = \mathbb{F}$.

This K/k is Galois and the reduction map is an iso

$$\mathrm{Gal}(K/k) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_K/\mathbb{F}_k).$$

b) For K/k finite unramified & L/K finite, $\exists$ natural iso

$$\mathrm{Hom}_{k\text{-alg}}(K,L) \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{F}_k\text{-alg}}(\mathbb{F}_K, \mathbb{F}_L)$$

Pf. a) By the primitive element thm, $\mathbb{F} = \mathbb{F}_k(\bar{\alpha})$ for some $\bar{\alpha} \in \mathbb{F}$. Let $\bar{f} \in \mathbb{F}_k[x]$ be the minimal polynomial of $\bar{\alpha}$ & $f \in k[x]$ a monic lift.

$\Rightarrow f \in k[x]$ irreducible since $\bar{f} \in \mathbb{F}_k[x]$ is

$\Rightarrow K := k[x]/(f)$ extension field of k

w/ $[K:k] = \deg f = \deg \bar{f} = [\mathbb{F}_K : \mathbb{F}_k]$,

ie. K/k is unramified w/ $\mathbb{F}_K \simeq \mathbb{F}$

For uniqueness & Galois property we first prove b):

Write $K = k(\alpha)$ for a primitive element $\alpha \in \mathcal{O}_K$.
Let $f \in k[x]$ be the minimal polynomial of α.
Since K/k is unramified, we have

$$[\mathbb{F}_K : \mathbb{F}_k] = [K:k] = \deg f$$

But $\mathbb{F}_K = \mathbb{F}_k(\bar{\alpha})$ where $\bar{\alpha} := \alpha \bmod \wp$ is a zero of the reduction $\bar{f} := f \bmod \wp \in k[x]$.

$\Rightarrow \bar{f} \in k[x]$ is still irreducible & $\mathbb{F}_K \simeq \mathbb{F}_k[x]/(\bar{f})$

So $\mathrm{Hom}_{k\text{-alg}}(K,L) = \{a \in L : f(a) = 0\}$

$\downarrow$ $\wr$ bijective by Hensel

$\mathrm{Hom}_{k\text{-alg}}(\mathbb{F}_K, \mathbb{F}_L) = \{\bar{a} \in \mathbb{F}_L : \bar{f}(\bar{a}) = 0\}$

This proves b).

To see uniqueness in a),

let K/k, L/k be finite unramified w/ $\mathbb{F}_K \simeq \mathbb{F}_L \simeq \mathbb{F}$,

then by b) this iso lifts to an iso $K \xrightarrow{\sim} L$.

The Galois property follows similarly. □

Rem For K/k and L/k finite extensions inside a fixed algebraic closure $\bar{k}/k$, we have:

K/k unramified $\Rightarrow KL/L$ unramified

Hence if K, L are both unramified over k, then so is the composite KL/k.

Def $k^{ur} := \bigcup_{\substack{K/k \text{ finite} \\ \text{unramified} \\ \text{subext}^n \text{ of } \bar{k}/k}} K$ the "maximal unramified extension of k"

By construction

$$\begin{array}{ccc} \mathrm{Gal}(k^{ur}/k) & \xrightarrow{\sim} & \mathrm{Gal}(\bar{\mathbb{F}}_k/\mathbb{F}_k) \\ \downarrow & & \downarrow \\ \mathrm{Gal}(K/k) & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_K/\mathbb{F}_k) \end{array} \quad \text{for } K/k \text{ finite unramified}$$

Def For any unramified K/k, the Frobenius is the unique $\varphi_{K/k} \in \mathrm{Gal}(K/k)$ which on residue fields induces

$\bar{\varphi}_{K/k} = (x \mapsto x^q) \in \mathrm{Gal}(\mathbb{F}_K/\mathbb{F}_k)$, $q = |\mathbb{F}_k|$.

For $k \subset K \subset L$ unramified we have

$\varphi_{K/k} = (\varphi_{L/k})|_K$, so the Frobenii fit together to an automorphism

$$\varphi_k = \varprojlim_K \varphi_{K/k} \in \mathrm{Gal}(k^{ur}/k).$$

Rem For K/k finite unram, $\varphi_K = \varphi_k^{[K:k]}$.

In abstract CFT we showed that for finite fields $\mathbb{F}$ the pair $(\mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}), \mathbb{Z})$ is a class formation.

Can we transfer this to $(\underbrace{\mathrm{Gal}(k^{ur}/k)}_{\simeq \mathrm{Gal}(\overline{\mathbb{F}}_k/\mathbb{F}_k)}, A)$

where

$A := (k^{ur})^*$

$\simeq U(k^{ur}) \times \mathbb{Z}$ w/ $U(k^{ur}) := \mathcal{O}_{k^{ur}}^*$?

The key point is:

Thm Let $G := \mathrm{Gal}(k^{ur}/k) \circlearrowright U = U(k^{ur})$, then

$$H_T^i(G, U) = 0 \text{ for all } i \in \mathbb{Z}.$$

Pf. We must show

$$H_T^i(\mathrm{Gal}(K/k), U(K)) = 0$$

for all finite unramified K/k and all $i \in \mathbb{Z}$.

Consider $U := U(K) \supset U_1 := U_1(K) \supset \cdots$

& the exact sequence $1 \to U_1 \to U \to \mathbb{F}_K^* \to 1$

of modules for $G := \mathrm{Gal}(K/k) \simeq \mathrm{Gal}(\mathbb{F}_K/\mathbb{F}_k)$.

Since G is cyclic, its Tate cohomology is 2-periodic, so Hilbert 90 gives for all $i \in \mathbb{Z}$:

$$H_T^i(G, \mathbb{F}_K^*) = H_T^i(\mathrm{Gal}(\mathbb{F}_K/\mathbb{F}_k), \mathbb{F}_K^*) = 0$$

$$\Rightarrow \quad H_T^\bullet(G, U) \simeq H_T^\bullet(G, U_1),$$

Since K/k is unramified, a generator $\pi \in \mathcal{O}_k$ of the max. ideal of $\mathcal{O}_k$ will also generate the maximal ideal of $\mathcal{O}_K$. Then for $n \geq 2$ we get a map of G-modules (since $\pi \in k = K^G$):

$$U_{n-1} \longrightarrow (\mathbb{F}_K, +), \quad 1 + a\pi^{n-1} \longmapsto (a \bmod \pi)$$

$\Rightarrow$ exact sequence of G-modules

$$1 \longrightarrow U_n \longrightarrow U_{n-1} \longrightarrow (\mathbb{F}_k, +) \longrightarrow 0$$

$\Rightarrow$ $H^\bullet_T(G, U_n) \simeq H^\bullet_T(G, U_{n-1})$ for all n

by "additive Hilbert 90": $H^\bullet_T(G, \mathbb{F}_K) = 0$

$\Rightarrow$ $H^\bullet_T(G, U_n) \xrightarrow{\sim} H^\bullet_T(G, U)$ via $U_n \hookrightarrow U$

But we know for any $m \in \mathbb{N}$ $\exists n \gg 0$:

$$[m]: U_n \xrightarrow{\sim} U_{n+v(m)}, \quad x \mapsto x^m$$

$\Rightarrow$

$$\begin{array}{ccc} H^\bullet_T(G, U_n) & \xrightarrow{\sim} & H^\bullet_T(G, U) \\ {\scriptstyle [m]}\downarrow\wr & \circlearrowright & \downarrow{\scriptstyle [m]} \\ H^\bullet_T(G, U_{n+v(m)}) & \xrightarrow{\sim} & H^\bullet_T(G, U) \end{array}$$

$\Rightarrow$ $[m]: H^\bullet_T(G, U_1) \xrightarrow{\sim} H^\bullet_T(G, U_1)$ iso

Taking m divisible by $|G|$, we get $H^\bullet_T(G, U_1) = 0$. $\square$

<u>Cor 1</u> For K/k unramified, $U(k) = N_{K/k}(U_K)$.

Pf. Take $i = 0$ in the above. $\square$

<u>Cor 2</u> $(G, A) := (\mathrm{Gal}(k^{ur}/k), (k^{ur})^*)$ is a class formation.

Pf. $H^1(G, A) = 0$ holds by Hilbert 90.

We want for all $k \subset K \subset k^{ur}$ a natural iso

$$\mathrm{inv}_K : H^2(G_K, (k^{ur})^*) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

w/ $G_K := \mathrm{Gal}(k^{ur}/K)$, sth for all normal unramified L/K the following commutes:

$$\begin{array}{ccc} H^2(G_K, (k^{ur})^*) & \xrightarrow[\mathrm{inv}_K]{\sim} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \mathrm{res}}\downarrow & & \downarrow{\scriptstyle [L:K]\cdot \mathrm{id}} \\ H^2(G_L, (k^{ur})^*) & \xrightarrow[\mathrm{inv}_L]{\sim} & \mathbb{Q}/\mathbb{Z} \end{array}$$

But this follows directly from the case of finite fields that we discussed in abstract CFT, using

$$\begin{array}{ccccc} H^2(\mathrm{Gal}(\overline{\mathbb{F}}_k/\mathbb{F}_K),\mathbb{Z}) & \simeq & H^2(G_K,\mathbb{Z}) & \underset{(*)}{\simeq} & H^2(G_K,(k^{ur})^*) \\ \downarrow \mathrm{res} & & \downarrow & & \downarrow \mathrm{res} \\ H^2(\mathrm{Gal}(\overline{\mathbb{F}}_k/\mathbb{F}_L),\mathbb{Z}) & \simeq & H^2(G_L,\mathbb{Z}) & \underset{(*)}{\simeq} & H^2(G_L,(k^{ur})^*) \end{array}$$

where $(*)$ uses

$$H^\bullet(G_K,(k^{ur})^*) = \varinjlim_{\substack{M/K \\ \text{unram.}}} H^\bullet(\mathrm{Gal}(M/K),M^*)$$

$\simeq H^\bullet(\mathrm{Gal}(M/K),\mathbb{Z})$ as $H^\bullet(\mathrm{Gal}(M/K),U(M))=0$ by the previous theorem

$$\simeq \varinjlim_{\substack{M/K \\ \text{unram.}}} H^\bullet(\mathrm{Gal}(M/K),\mathbb{Z})$$

$$= H^\bullet(G_K,\mathbb{Z}) \quad \& \text{ ditto for } L.$$

□

From abstract CFT we therefore get for every finite unramified L/K an Artin iso and norm residue symbol:

$$\begin{array}{ccc} K^* & \xrightarrow{(\cdot,L/K)} & \\ \downarrow & & \\ K^*/N_{L/K}(L^*) & \xrightarrow[\mathrm{Art}_{L/K}]{\sim} & \mathrm{Gal}(L/K) \end{array}$$

(note this group is already abelian...)

Passing to $\mathrm{Gal}(K^{ur}/K) = \varprojlim_L \mathrm{Gal}(L/K)$ we get the universal norm residue symbol

$$\begin{array}{ccccc} (\cdot,K^{ur}/K): & K^* & \longrightarrow & \mathrm{Gal}(K^{ur}/K). \\ & \wr & & \wr \\ & U(K)\times\mathbb{Z} & & \mathrm{Gal}(\overline{\mathbb{F}}_K/\mathbb{F}_K)=\widehat{\mathbb{Z}} \end{array}$$

In fact everything is completely explicit in this case:

Rem For $a \in K^*$ with valuation $v(a) \in \mathbb{Z}$ we have

$$(a, K^{ur}/K) = \varphi_K^{v(a)}$$

for the Frobenius $\varphi_K \in Gal(K^{ur}/K)$.

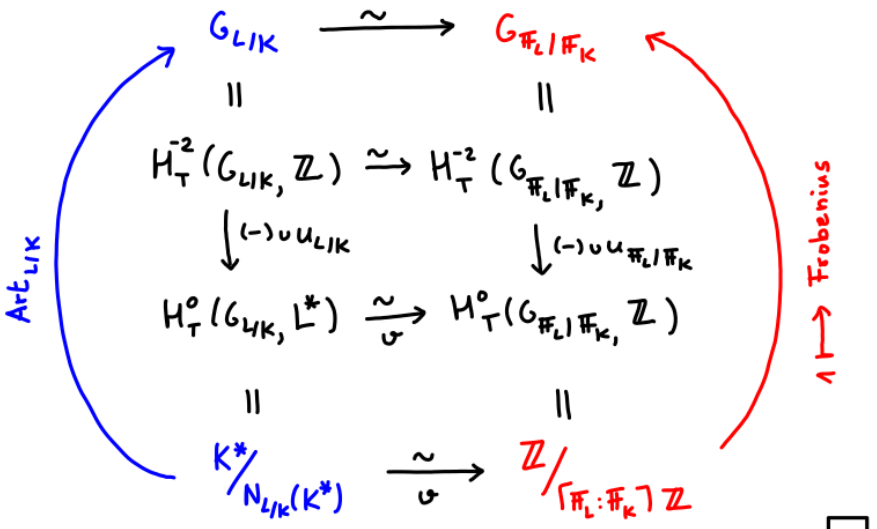
Pf. The Artin symbol in abstract CFT was defined using cup product w/ the fundamental classes

$$\begin{array}{ccccc} u_{L/K} & \in & H^2(Gal(L/K), L^*) \simeq H^2(Gal(\mathbb{F}_L/\mathbb{F}_K), \mathbb{Z}) & \ni & u_{\mathbb{F}_L/\mathbb{F}_K} \\ \downarrow & & \downarrow inv_{L/K} \quad (*) & & \downarrow inv_{\mathbb{F}_L/\mathbb{F}_K} \\ \frac{1}{[L:K]} & \in & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} = \frac{1}{[\mathbb{F}_L:\mathbb{F}_K]}\mathbb{Z}/\mathbb{Z} & \ni & \frac{1}{[\mathbb{F}_L:\mathbb{F}_K]} \end{array}$$

Note:

- The top row is induced by $v: L^* \twoheadrightarrow \mathbb{Z}$ (L/K unramified...)
- We defined inv_K & inv_L so that (*) commutes!

So the claim follows from the diagram



□

Upshot • $Art_K: K^*/U(K) \xrightarrow{\text{dense}} Gal(K^{ur}/K)$

$\mathbb{Z} \hookrightarrow \hat{\mathbb{Z}}$

• For L/K the unramified ext^n of degree $f \in \mathbb{N}$,

$$N_{L/K}(L^*) = U(K) \times f\mathbb{Z} \hookrightarrow K^* = U(K) \times \mathbb{Z}.$$

Rem This could be done without gp cohomology... But the ramified case will be much less explicit, there gp cohom will be very useful!

4. Local CFT : The ramified case

k finite extension of $\mathbb{Q}_p$

$\bar{k}$ an algebraic closure

For L/K normal w/ $k \subset K \subset L \subset \bar{k}$, $[L:k] < \infty$ (possibly ramified!)

we put

$G_{L/K} := \mathrm{Gal}(L/K)$, $H^i(L/K) := H_T^i(G_{L/K}, L^*)$ $(i \in \mathbb{Z})$

$G_K := \mathrm{Gal}(\bar{k}/K)$, $H^j(K) := H^j(G_K, \bar{k}^*)$ $(j \geq 0)$

Hilbert 90 : $H^1(K) = 0$

$\Rightarrow (G_k, \bar{k}^*)$ is a field formation.

We want to show it is a class formation !

Recall the key input in unramified local CFT was $H_T^*(G_{L/K}, U(L)) = 1$. This is no longer true in the ramified case, but we have :

Prop $\exists$ open subgp $V \subset U(L)$ sth

- V is stable under the action of $G_{L/K}$
- $H^i(G_{L/K}, V) = 0$ for all $i > 0$.

Pf.

1) We first construct an open subgp $W \subset \mathcal{O}_L$ $G_{L/K}$-stable w/ $H^i(G_{L/K}, W) = 0$ for all $i > 0$:

By Galois theory ("normal basis thm"),

$\exists\, a \in L$ sth $(\sigma(a))_{\sigma \in G_{L/K}}$ is a K-basis of L.

Clearing denominators we may assume $a \in \mathcal{O}_L$.

Then $W := \bigoplus_{\sigma \in G} \mathcal{O}_K \cdot \sigma(a) \subset \mathcal{O}_L$ is stable under the action of $G_{L/K}$, and

$W \simeq \mathrm{Ind}_1^{G_{L/K}}(\mathcal{O}_K)$ as a $G_{L/K}$-module.

$\Rightarrow H^i(G_{L/K}, W) = 0 \ \forall\, i > 0$.

2) Replacing W by $p^n \cdot W$ for $n \gg 0$,

we may assume the exponential series converges

on W and induces an iso $\exp : W \xrightarrow{\sim} V$

onto an open subgp of O_L^*, whence the claim $\square$

Using this we show that for L/K cyclic,

the gp $H^2(L/K)$ has the size expected from

the class field axiom (ie $H^2(L/K) \simeq \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$).

Put $h^i(L/K) := \# H_T^i(L/K)$, then we have:

<u>Cor</u> For L/K cyclic, $h^2(L/K) = [L:K]$.

Pf. Pick an open subgp $V \subset U(L)$

w/ $H^i(G_{L/K}, V) = 0 \quad \forall i > 0$

$\Rightarrow H_T^i(G_{L/K}, V) = 0 \quad \forall i \in \mathbb{Z}$

($G_{L/K}$ finite cyclic, so Tate coh. is 2-periodic)

$\Rightarrow H_T^i(G_{L/K}, U(L)) \xrightarrow{\sim} H_T^i(G, M) \quad \forall i \in \mathbb{Z}$ (*)

for $M := U(L)/V$

Now M is finite & $G_{L/K}$ finite cyclic

$\Rightarrow$ Herbrand quotient

$$h(M) := \frac{h^{2i}(M)}{h^{2i-1}(M)} = 1$$

(see the section about Herbrand quotients)

$\Rightarrow$ By (*) also $h(U(L)) = h(M) = 1$

Thus from $1 \to U(L) \to L^* \to \mathbb{Z} \to 0$ we get

$$\begin{aligned} h^2(L^*) &= h(L^*) && \text{by Hilbert 90 : } h^1(L^*) = 0 \\ &= h(U(L)) \cdot h(\mathbb{Z}) && \text{by the above sequence} \\ &= h(\mathbb{Z}) && \text{because } h(U(L)) = 1 \\ &= h_T^0(\mathbb{Z}) && \text{since } H_T^1(\mathbb{Z}) = \underbrace{\mathrm{Hom}(G_{L/K}, \mathbb{Z})}_{\text{finite}} = 0 \\ &= |\mathbb{Z}/|G_{L/K}|\mathbb{Z}| \\ &= [L:K]. \end{aligned}$$

$\square$

In fact $h^2(L|K) = [L:K]$ also holds for non-cyclic extensions. We first show:

Prop ("first inequality") For any finite normal $L|K$,

$$h^2(L|K) \text{ divides } [L:K].$$

Pf. Enough to show $\forall$ primes p:

$|\underbrace{H^2(L|K)_p}_{\text{p-part of } H^2(L|K)}|$ divides the p-part of $[L:K]$

Let $G_p \subset G := G_{L|K}$ be a p-Sylow.

From $\text{cores}^G_{G_p} \circ \text{res}^G_{G_p} = [G:G_p] \cdot \text{id}$ we know that

$\text{res}^G_{G_p} : H^\bullet_T(G, L^*)_p \hookrightarrow H^\bullet_T(G_p, L)$ is injective.

$\cap$

$H^\bullet_T(G, L^*)$ $\nearrow$

$\Rightarrow$ may replace G by G_p

(and $K = L^G \hookrightarrow L$ by $L^{G_p} \hookrightarrow L$)

So now assume $G = G_{L|K}$ is a p-group.

$\Rightarrow \exists$ cyclic quotient $G \twoheadrightarrow \mathbb{Z}/p\mathbb{Z}$,

hence $K \underset{\text{Galois cyclic}}{\hookrightarrow} \exists K' \hookrightarrow L$ w/ $[K':K] = p$

Consider

$$1 \to H^2(K'|K) \to H^2(L|K) \xrightarrow{\text{res}} H^2(L|K')$$

$\uparrow$ exact since $H^1(L|K') = 0$ by Hilb 90

$\Rightarrow h^2(L|K)$ divides $\underbrace{h^2(K'/K)}_{=[K':K] \text{ by cyclic case}} \cdot \underbrace{h^2(L|K')}_{\text{divides } [L:K'] \text{ by induction on } [L:K']}$

$\Rightarrow h^2(L|K)$ divides $[L:K'] \cdot [K':K] = [L:K]$.

□

Rem Instead of the Sylow argument, one can get a cyclic quotient of $G_{L/K}$ directly by noting that for any finite Galois extension L/K of a local field K, the gp $G_{L/K}$ is solvable (write $L \supseteq M \supseteq K$, exercise).

($L \supseteq M$: totally ram.; $M \supseteq K$: unram.)

We can now show $h^2(L/K) = [L:K]$, this follows directly from:

Thm ("reduction to the unramified case")

For any finite normal L/K, let M/K be the unique unramified extension w/ $[M:K] = [L:K]$. Then

$$H^2(L/K) = H^2(M/K) \text{ inside } H^2(K).$$

Pf. Enough to show $H^2(M/K) \subset H^2(L/K)$ (*), since then we get the "second inequality"

$$[L:K] = [M:K] = h^2(M/K) \leq h^2(L/K)$$

($=$: unramified CFT; $\leq$: (*))

& then the claim follows by the first inequality.

To prove (*) consider

(note: M/K unram. $\Rightarrow LM/L$ unram. & in particular normal)

$$\begin{array}{ccccccc} 1 & \to & H^2(L/K) & \to & H^2(LM/K) & \xrightarrow{\text{res}} & H^2(LM/L) \\ & & \text{UI} & & (**) & & \downarrow \text{inv}_{LM/L} \\ & & H^2(M/K) & & \dashrightarrow & & \mathbb{Q}/\mathbb{Z} \end{array}$$

$[M:K]\cdot \text{inv}_{M/K}$ = zero map!

We claim $\text{res}|_{H^2(M/K)} = 0$ ($\Rightarrow$ (*)):

Indeed the lemma below shows that the square (**) commutes, and $[M:K]\cdot \text{inv}_{M/K} = 0$ since $\text{inv}_{M/K}$ takes values in $\frac{1}{[M:K]}\mathbb{Z}/\mathbb{Z}$. □

We have used:

Lemma ("local invariant map & composites")

Let N/K be a finite normal extension

and $K \subset L, M \subset N$

two subextensions

w/ M/K unramified

($\Rightarrow LM/L$ unramified)

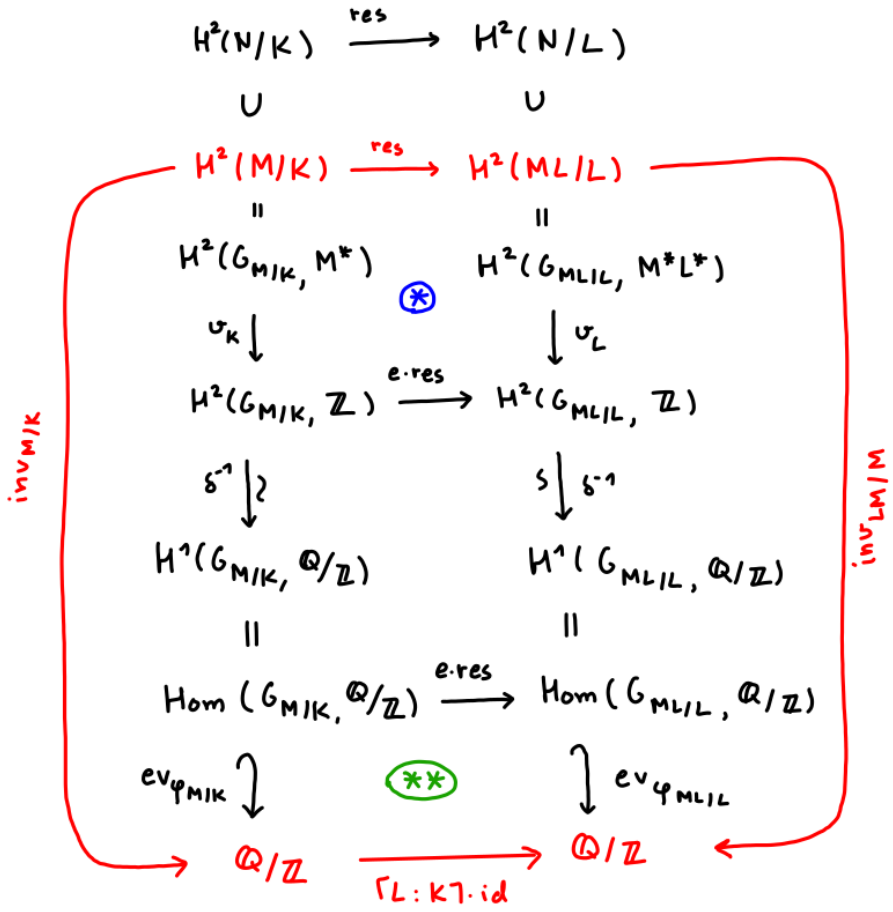
Then the following diagram commutes:

need to go to N/K here since LM/K need not be normal...

$$\begin{array}{ccc} H^2(N/K) & \xrightarrow{\text{res}} & H^2(N/L) \\ \cup & & \cup \\ H^2(M/K) & \dashrightarrow & H^2(LM/L) \\ \| & & \downarrow inv_{LM/L} \\ H^2(M/K) & \xrightarrow[[L:K]\cdot inv_{M/K}]{} & \mathbb{Q}/\mathbb{Z} \end{array}$$

LM/L is unramified, hence normal

Pf. The local invariant maps are given by:



⊛ commutes for $e = e_{L|K}$ the ramification index

⊛⊛ commutes because $[L:K] = e \cdot f$ and

$(\varphi_{ML|L})|_M = (\varphi_{M|K})^f$ for $f = f_{L|K}$

□

Summary

$$\begin{array}{ccc} H^2(K) & \xrightarrow{\sim} & H^2(K^{ur}/K) \\ \| & & \| \\ \bigcup_{L/K \text{ finite}} H^2(L/K) & & \bigcup_{L/K \text{ finite}} H^2(L/K) \\ & & \text{unramified} \end{array}$$

Rem Using $H^2(K) \simeq Br(K)$, $H^2(L/K) \simeq Br(L/K)$, we can interpret this as saying that every csa A over K splits over a finite unramified extension:

$\exists\, L/K$ unramified w/ $A \otimes_K L \simeq Mat_{n\times n}(L)$.

We will not use this in what follows.

Cor $\exists$ natural iso $inv_K : H^2(K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$.

Pf. Take

$$inv_K : H^2(K) \simeq H^2(K^{ur}/K) \xrightarrow{\sim} \mathbb{Q}/\mathbb{Z}$$

($\wr$: unramified local CFT)

□

Thm Put $G_K = Gal(\bar{k}/K) \subset A_K = \bar{k}^*$.

Then (G_K, A_K, inv_K) is a class formation.

Pf. $H^1(K) = 0$ by Hilb 90.

We want that for all normal L/K the diagram below commutes:

$$\begin{array}{ccc} H^2(K) & \xrightarrow[\sim]{inv_K} & \mathbb{Q}/\mathbb{Z} \\ \downarrow \text{res} & & \downarrow [L:K]\cdot id \\ H^2(L) & \xrightarrow[\sim]{inv_L} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Since $H^2(K) = H^2(K^{ur}/K)$

$$H^2(L) = H^2(L^{ur}/L) = H^2(K^{ur}\cdot L/L)$$

($L^{ur} = K^{ur}\cdot L$ (exercise))

this amounts to

$$\begin{array}{ccc} H^2(M/K) & \xrightarrow{[L:K]\cdot inv_{M/K}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow \text{res} & \circlearrowright & \\ H^2(LM/L) & \xrightarrow[inv_{LM/L}]{} & \end{array}$$

for all unramified M/K, and this we know from the previous lemma.

□

In particular, for L/K normal we get a map

$$\begin{array}{ccc} \mathrm{inv}_{L/K}: H^2(L/K) & \xrightarrow{\sim} & \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \\ \downarrow & & \downarrow \\ H^2(K) & \xrightarrow[\mathrm{inv}_K]{\sim} & \mathbb{Q}/\mathbb{Z} \\ \downarrow \mathrm{res} & & \downarrow [L:K]\cdot \mathrm{id} \\ H^2(L) & \xrightarrow[\mathrm{inv}_L]{\sim} & \mathbb{Q}/\mathbb{Z} \end{array}$$

Cor ("main thm of local CFT")

For any normal L/K, have a natural iso $\forall\, i \in \mathbb{Z}$:

$$u_{L/K} \cup (-): H_T^i(G_{L/K}, \mathbb{Z}) \xrightarrow{\sim} H_T^{i+2}(L/K)$$

for the fundamental class $u_{L/K}$ defined by

$$\begin{array}{ccc} u_{L/K} & \in & H^2(L/K) \\ \downarrow & & \downarrow 2\ \mathrm{inv}_{L/K} \\ \frac{1}{[L:K]} & \in & \frac{1}{[L:K]}\cdot\mathbb{Z}/\mathbb{Z} \end{array}$$

Cor ("Local reciprocity") For every finite normal L/K

$$\exists \text{ natural iso } \mathrm{Art}_{L/K}: K^*/N_{L/K}(L^*) \xrightarrow{\sim} G_{L/K}^{ab}.$$

Pf. Take the inverse of $u_{L/K} \cup (-): H^{-2}(G_{L/K}, \mathbb{Z}) \xrightarrow{\sim} H^0(L/K)$ from the previous corollary. □

As before define the norm residue symbol $(\cdot, L/K)$ as the composite:

$$\begin{array}{ccc} K^* & & \\ \downarrow & \searrow^{(\cdot, L/K)} & \\ K^*/N_{L/K}(L^*) & \xrightarrow[\mathrm{Art}_{L/K}]{\sim} & G_{L/K}^{ab} \end{array}$$

These are compatible in towers $K \subset L \subset M \subset \cdots$ so we get the universal norm residue symbol

$$(\cdot, K): K^* \longrightarrow G_K^{ab} = \varprojlim_{L/K \text{ finite Galois}} G_{L/K}^{ab}$$

For every uniformizer $\pi \in \mathcal{O}_K$ we have

$$(\pi, K)|_{K^{ur}} = \varphi_K \in \mathrm{Gal}(K^{ur}/K).$$

In contrast to the unramified case where the unit gp $U(K)$ was the kernel, we now have:

Prop The univ. norm residue symbol is an injective hom. w/ dense image

$$(\cdot, K): K^* \hookrightarrow G_{L|K}^{ab}.$$

Pf. As in abstract CFT,

$$\ker(\cdot, K) = \bigcap_{L|K} N_{L|K}(L^*) =: N_K \subset K^*$$

("universal norm subgp")

We claim that $N_K = \{1\}$:

This will follow from the existence thm, which says that every finite index subgp $U \subset K^*$ is a norm subgp $N_{L|K}(L^*)$ for some L.

(to be proven independently in the next section)

Recall that $(K^*)^m \subset K^*$ has finite index $\forall m$, as we checked in the discussion of multiplicative gps of local fields (sect. III.2). Thus

$$N_K \subset \bigcap_{m \geq 1} (K^*)^m \underset{\text{III.2}}{=} \{1\}. \qquad \square$$

5. The existence thm

We have set up an inclusion-reversing bijection

$$\left\{\begin{array}{c}\text{finite abelian extensions} \\ \text{of } K \text{ inside } \bar{k}\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\text{norm subgps} \\ \text{of } K^*\end{array}\right\}$$

$$L|K \longmapsto N_{L|K}(L^*)$$

Rem If $H \subset K^*$ is a norm subgp, then so is any subgp $H_1 \subset K^*$ containing H.

$$\left[\begin{array}{lcll} H = N_{L|K}(L^*): & K^*/H & \xrightarrow[\text{Art}]{\sim} & G_{L|K} \\ \exists\, L_1 \subset L \text{ by} & \downarrow & & \downarrow \quad N_{L_1|K}(L_1^*) \\ \text{Galois corresp.} & K^*/H_1 & \xrightarrow{\sim} & G_{L_1|K} \quad = H_1 \end{array}\right]$$

Thm ("existence thm") For subgps $H \subset K^*$ TFAE:

a) H is a norm subgp, ie

$H = N_{L|K}(L^*)$ with $L|K$ finite Galois.

b) $H \subset K^*$ is an open (hence closed)

subgp of finite index.

Pf. a) $\Rightarrow$ b):

$H = N_{L|K}(L^*)$ with $L|K$ finite Galois

$\Rightarrow K^*/H \xrightarrow{\sim} G_{L|K}^{ab}$ by the reciprocity law

$\Rightarrow H \subset K^*$ of finite index since $|G_{L|K}^{ab}| < \infty$

Put $n := [K^* : H]$

$\Rightarrow K^{*n} \subset H$

$\Rightarrow H \subset K^*$ open because $K^{*n} \subset K^*$ open

b) $\Rightarrow$ a):

$H \subset K^*$ open of finite index, say index n

$\Rightarrow K^{*n} \subset H$

$\Rightarrow$ enough to show $K^{*n} \subset K^*$ is a norm subgp

(then so is H by the remark preceding the thm)

Case 1: K contains all n-th roots of 1, ie $\mu_n(\bar{K}) \subset K$:

Put $L = \bigcup_{a \in K^*} K(\sqrt[n]{a})$.

K^*/K^{*n} finite $\Rightarrow L|K$ finite abelian extension

We have

$$\underbrace{N_{L|K}(L^*)}_{=: N(L^*)} = \bigcap_{a \in K^*} \underbrace{N_{K(\sqrt[n]{a})|K}(K(\sqrt[n]{a})^*)}_{=: N(K(\sqrt[n]{a})^*)}.$$

We claim $K^* = N(L^*)$:

For $a \in K^*$ clearly

$K^{*d} \subset N(K(\sqrt[n]{a}))$ w/ $d := [K(\sqrt[n]{a}) : K]$

But $d \mid n$

$\Rightarrow K^{*n} \subset N(K(\sqrt[n]{a}))$ for all a

$\Rightarrow K^{*n} \subset N(L)$

To show equality it then suffices to check that

$$|K^*/K^{*n}| \leq \underbrace{|K^*/N(L)|}_{\simeq G_{L|K} \text{ by Artin iso}}$$

This follows from "Kummer theory":

Since $\mu_n := \mu_n(\bar{K}) \subset K$, we have a well-defined hom.

$$K^*/_{K^{*n}} \longrightarrow \mathrm{Hom}(G_{L|K}, \mu_n)$$

$$a \longmapsto \left(\sigma \mapsto \frac{\sigma(\sqrt[n]{a})}{\sigma(a)}\right)$$

which is injective by construction,

and $|\mathrm{Hom}(G_{L|K}, \mu_n)| = |G_{L|K}|$ since $G_{L|K}$ is a finite abelian n-torsion gp

Rem. By the above then in fact

$K^*/_{K^{*n}} \xrightarrow{\sim} \mathrm{Hom}(G_{L|K}, \mu_n)$ is an iso.

Case 2: If $K \not\supset \mu_n := \mu_n(\bar{K})$:

Put $K_1 := K(\mu_n)$.

By case 1, $\exists\, L_1/K_1$ finite w/ $K_1^{*n} = N(L_1)$

(where $N(L_1) := N_{L_1|K_1}(L_1^*)$)

Put $\tilde{L} :=$ normal closure of L_1/K

$$\Rightarrow N_{\tilde{L}|K}(\tilde{L}^*) = N_{K_1|K}(N_{\tilde{L}|K_1}(\tilde{L}^*))$$

$$\subset N_{K_1|K}(N_{L_1|K_1}(L_1^*))$$

$$= N_{K_1|K}(K_1^{*n})$$

$$= (N_{K_1|K}(K_1^*))^n$$

$$\subset K^{*n}$$

$\Rightarrow K^{*n}$ is a norm subgp of K^* $\square$

Cor For any subgp $H \subset K^*$ TFAE:

a) H is a norm subgp
(ie $\exists$ finite $L|K$ sth $H = N_{L|K}(L^*)$)

b) $H \subset K^*$ is open of finite index.

c) $H \subset K^*$ is closed of finite index.

d) $H \subset K^*$ is of finite index.

e) H contains $\pi^m \cdot U_n(K)$, some $m,n \in \mathbb{N}$.
($\pi \in \mathcal{O}_K$ a uniformizer)

Pf. a) $\Leftrightarrow$ b) by the thm

b) $\Leftrightarrow$ c) because of finite index

b) $\Leftrightarrow$ d) because any finite index $H \subset K^*$ contains K^{*n} for some n and hence is automatically open

b) $\Leftrightarrow$ e) because $K^* = U(K) \times \{\pi^m \mid m \in \mathbb{Z}\}$ and the $U_n(K)$ form a basis of open nbhoods of 1 in $U(K)$. $\square$

6. Lubin-Tate theory I: Formal modules

K finite extension of $\mathbb{Q}_p$

Local CFT gives a continuous hom.

$K^* \hookrightarrow \mathrm{Gal}(K^{ab}/K)$ w/ dense image

$\hat{K}^*$ $\exists!$ continuous hom.

for the profinite completion

$\hat{K}^* := \varprojlim_{H \subset K^* \text{ of finite index (hence open by corollary)}} K^*/H$

Here $K^* \simeq U(K) \times \mathbb{Z}$, $\hat{K}^* \simeq U(K) \times \hat{\mathbb{Z}}$

We get:

$$\begin{array}{ccccccccc} 1 & \to & U(K) & \longrightarrow & \hat{K}^* & \longrightarrow & \hat{K}^*/U(K) & \to & 1 \\ & & \downarrow \wr & & \downarrow \wr & & \downarrow \wr \text{ unramified local CFT} & & \\ 1 & \to & I & \longrightarrow & \mathrm{Gal}(K^{ab}/K) & \longrightarrow & \mathrm{Gal}(K^{ur}/K) & \to & 1 \end{array}$$

I: "inertia gp" $= \mathrm{Gal}(K^{ab}/K^{ur})$

$\mathrm{Gal}(K^{ur}/K) = \mathrm{Gal}(\overline{\mathbb{F}}_K/\mathbb{F}_K)$

Q Unramified local CFT is completely explicit using the Frobenius. How about

$$\mathrm{Art}_K|_{U(K)} : U(K) \xrightarrow{\sim} I \subset \mathrm{Gal}(K^{ab}/K) \ ?$$

Rem Choosing a uniformizer $\pi \in \mathcal{O}_K$, we get a (non-canonical) splitting

$$U(K) \times \hat{\mathbb{Z}} \xrightarrow{\sim} \hat{K}^*$$
$$(u, n) \longmapsto u \cdot \pi^n$$

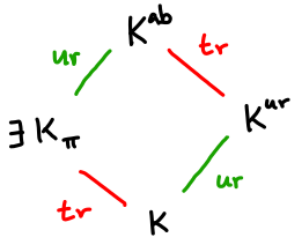
$\Rightarrow$ $\exists$ (non-canonical) epi $\hat{K}^* \twoheadrightarrow U(K)$

$\Rightarrow$ By Galois theory this gives a subfield $K_\pi \subset K^{ab}$ with

$$\begin{array}{ccc} \hat{K}^* & \xrightarrow[(\cdot,K)]{\sim} & \mathrm{Gal}(K^{ab}/K) \\ \downarrow & & \downarrow \ \text{depends on choice of } \pi \\ U(K) & \xrightarrow{\sim} & \mathrm{Gal}(K_\pi/K) \end{array}$$

By construction $K^{ab} = K_\pi \cdot K^{ur}$ & $K_\pi \cap K^{ur} = K$.

Upshot:



ur : unramified
tr : totally ramified

How to construct a totally ramified K_π / K explicitly ?

Attempt 1: Try $\bigcup_{n \geq 0} K(\sqrt[n]{\pi})$

Pb: $K(\sqrt[n]{\pi})$ not Galois in general. Its Galois closure is $K_n(\sqrt[n]{\pi})$ for $K_n := K(\mu_n)$, $\mu_n := \mu_n(\bar{K})$.
But K_n is unramified over K for $p \nmid n$ ↯

Attempt 2: For $K = \mathbb{Q}_p$ the local Kronecker-Weber thm says that $\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\mu_\infty) = \mathbb{Q}_p(\mu_{p^\infty}) \cdot \mathbb{Q}_p^{ur}$ w/ $\mu_\infty := \bigcup_{n \geq 0} \mu_n$ & $\mu_{p^\infty} := \bigcup_{n \geq 0} \mu_{p^n}$. But Kronecker-Weber doesn't hold over $K \neq \mathbb{Q}_p$... ↯

Lubin-Tate: For $K \neq \mathbb{Q}_p$, replace $\mu_n = \mathbb{G}_m(\bar{K})[n]$ by the n-torsion in suitable formal gps...

Def A (1-dimensional commutative) formal gp law over a comm. ring R is a power series $F \in R[\![X,Y]\!]$ sth

a) $F(X,Y) \equiv X+Y \mod (X,Y)^2$

b) $F(X,F(Y,Z)) = F(F(X,Y),Z)$

c) $F(X,Y) = F(Y,X)$.

Ex • The additive formal gp law $\hat{\mathbb{G}}_a$
w/ $\hat{\mathbb{G}}_a(X,Y) := X+Y$

• The multiplicative formal gp law $\hat{\mathbb{G}}_m$
w/ $\hat{\mathbb{G}}_m(X,Y) := X+Y+XY$
$= (1+X)(1+Y)-1$

("express multiplication in small nbhood of 1")

Exercise For any formal gp law F,

a) $F(X,0) = X$, $F(0,Y) = Y$.

b) $\exists!\ i \in TR[\![T]\!]$: $F(X, i(X)) = 0$

Def A homomorphism $\Phi : F \to G$ of formal gp laws is a power series $\Phi \in TR[\![T]\!]$ sth $\Phi(F(X,Y)) = G(\Phi(X), \Phi(Y))$.

We call Φ an isomorphism if $\exists\, \Psi : G \to F$ with $\Psi(\Phi(T)) = \Phi(\Psi(T)) = T$.

For $G = F$ we call Φ an endomorphism.

Exercise The set $\mathrm{End}(F)$ of endomorphisms is a ring wrt

$(\Phi \mathbin{\dot{+}} \Psi)(T) := F(\Phi(T), \Psi(T))$

$(\Phi \circ \Psi)(T) := \Phi(\Psi(T))$.

Def A formal R-module is a formal gp law F over R together w/ a ring hom. $\iota: R \longrightarrow \mathrm{End}(F)$ that "lifts the R-module structure on A" in the sense that

$$\iota(a) \equiv a \cdot T \mod T^2.$$

We write $[a] := [a]_F := \iota(a) \in T \cdot R[\![T]\!]$

Now take $R = \mathcal{O}_K$ for a finite extension $K/\mathbb{Q}_p$. For any formal $\mathcal{O}_K$-module F its reduction mod $\wp$ is a formal gp law $\overline{F}$ over $\mathbb{F}_K = \mathcal{O}_K/\wp$. It comes w/ a Frobenius $\varphi(T) := T^q \in \mathrm{End}(\overline{F})$ $(q := |\mathbb{F}_K|)$

Def A Lubin-Tate module over $\mathcal{O}_K$ for a chosen uniformizer $\pi \in \mathcal{O}_K$ is a formal $\mathcal{O}_K$-module F sth

$$[\pi]_F(T) \equiv T^q \mod \pi$$

(ie $[\pi]_F$ induces the Frobenius on $\overline{F}$)

Ex Over $R = \mathbb{Z}_p$, the formal gp law $\hat{\mathbb{G}}_m$ is a Lubin-Tate module for $\pi := p$ w/

$$[a] := (1+T)^a - 1 = \sum_{n \geq 1} \binom{a}{n} \cdot T^n$$

$\binom{a}{n} \in \mathbb{Z}_p$ for $a \in \mathbb{Z}_p$

(note: This only works for $R = \mathbb{Z}_p$ since then $q = p$)

To classify Lubin-Tate modules we fix the action of a uniformizer $\pi \in \mathcal{O}_K$: For any LT module F for π, the power series $e := [\pi]_F \in T\mathcal{O}_K[\![T]\!]$ must satisfy

a) $e \equiv \pi T \mod (T^2)$

b) $e \equiv T^q \mod (\pi)$ w/ $q := |\mathbb{F}_K|$.

Put $\mathcal{E}_\pi := \{ e \in T\mathcal{O}_K[\![T]\!] \mid a), b) \text{ hold} \}$.

Ex

- If $K = \mathbb{Q}_p$ and $\pi = p$, then $e := (1+T)^p - 1 \in \mathcal{E}_\pi$.
- In general always $e := \pi T + T^q \in \mathcal{E}_\pi$.

Different elements of $\mathcal{E}_\pi$ are related by:

Key lemma For any $e, \tilde{e} \in \mathcal{E}_\pi$ and any linear form $\ell(x_1,\dots,x_n) = \sum_i a_i x_i$ $(a_i \in \mathcal{O}_K)$,

$\exists!\ F \in \mathcal{O}_K[\![x_1,\dots,x_n]\!]$ sth

- $F \equiv \ell \mod (x_1,\dots,x_n)^2$
- $e(F(x_1,\dots,x_n)) = F(\tilde{e}(x_1),\dots,\tilde{e}(x_n))$.

Pf. Put $X = (X_1,\dots,X_n)$,

$\tilde{e}(X) = (\tilde{e}(X_1),\dots,\tilde{e}(X_n))$ etc.

Ansatz: $F(X) = \sum_{\nu=1}^{\infty} F_\nu(X)$ ↳ homogeneous of degree ν

For the partial sums $G_r(X) := \sum_{\nu=1}^{r} F_\nu(X)$ we then want:

- $G_1(X) = \ell(X)$
- $e(G_r(X)) \equiv G_r(\tilde{e}(X)) \mod (X)^{r+1} \quad \forall\, r \geq 1$

We find such F_ν by induction:

For $\nu = 1$ take $G_1(X) := F_1(X) := \ell(X)$.

If $G_1,\dots,G_r$ have been found w/ the above properties, we want F_{r+1} hom. of deg $r+1$ sth $G_{r+1} := F_{r+1} + G_r$ has

$$\underbrace{e(G_{r+1}(X))}_{\equiv\, \pi\cdot F_{r+1}(X) + e(G_r(X)) \mod (X)^{r+2}} \equiv \underbrace{G_{r+1}(\tilde{e}(X))}_{= G_r(\tilde{e}(X)) + \underbrace{F_{r+1}(\tilde{e}(X))}_{\equiv\, \pi^{r+1} F_{r+1}(X) \mod (X)^{r+2}}} \mod (X)^{r+2}$$

$$\iff F_{r+1}(X) \equiv \underbrace{\frac{e(G_r(X)) - G_r(\tilde{e}(X))}{\pi^{r+1} - \pi}}_{=:\, Q_r(X)} \mod (X)^{r+2}$$

(F_{r+1} homog. of deg $r+1$)

$$\iff F_{r+1}(X) = \text{leading term of } Q_r(X)$$

Note: $Q_r(X) \in \mathcal{O}_K[X]$ as $e(G_r(X)) \equiv G_r(\tilde{e}(X)) \mod \pi$

□

We can now classify all Lubin-Tate modules:

Thm Fix a uniformizer $\pi \in \mathcal{O}_K$.

a) The map

$$\{ \text{LT-modules for } \pi \} \xrightarrow{\sim} \mathcal{E}_\pi \quad \text{is a bijection.}$$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ (F, [\cdot]_F) =: F & \longmapsto & e_F(T) := [\pi]_F(T) \end{array}$$

b) For any LT-modules F, G for π,

$\exists$ natural iso of gps (Hom in LT-mod over $\mathcal{O}_K$ for π)

$$[\cdot]_{F,G} : \mathcal{O}_K \xrightarrow{\sim} \mathrm{Hom}_{\text{LT-mod}}(F, G)$$

sth

$$[b]_{G,H} \circ [a]_{F,G} = [ba]_{F,H} \quad \forall\, a, b \in \mathcal{O}_K.$$

In particular

$$\mathcal{O}_K \xrightarrow{\sim} \mathrm{End}_{\text{LT-mod}}(F) \quad \text{iso of rings.}$$

(shouldn't be too surprising:
LT modules are "formal modules of rk 1" ...)

Pf. If F is a LT-mod for π,

then by defn $e_F := [\pi]_F \in \mathcal{E}_\pi$.

Conversely, given any $e \in \mathcal{E}_\pi$,

by the key lemma (w/ $\tilde{e} := e$) $\exists!\ F = F_e \in \mathcal{O}_K[\![x,y]\!]$

sth

- $F(x,y) \equiv x + y \mod (x,y)^2$
- $e(F(x,y)) = F(e(x), e(y))$.

Uniqueness in the key lemma implies:

$$F(X,Y) = F(Y,X)$$

$$F(X, F(Y,Z)) = F(F(X,Y), Z)$$

$\Rightarrow$ F is a formal gp law.

Similarly, for any $e, f \in \mathcal{E}_\pi$ and $a \in \mathcal{O}_K$,

by the key lemma $\exists!\ [a]_{e,f} \in \mathcal{O}_K[\![T]\!]$

- $[a]_{e,f}(T) \equiv \pi T \mod T^2$
- $f([a]_{e,f}(T)) = [a]_{e,f}(e(T))$

Uniqueness in the key lemma shows:

$$[a]_{e,f}(F_e(x,y)) = F_f([a]_{e,f}(x), [a]_{e,f}(y))$$

$$[a+b]_{e,f}(x) = F_f([a]_{e,f}(x), [b]_{e,f}(x))$$

$$[a\cdot b]_{e,g}(x) = [a]_{f,g}([b]_{e,f}(x))$$

$$[\pi]_{e,e}(x) = e(x)$$

$\Rightarrow$ F_e is a LT module w/ $[\cdot]_e := [\cdot]_{e,e}$

and we get gp hom.

$$[\cdot]_{e,f} : \mathcal{O}_K \longrightarrow \mathrm{Hom}_{\text{LT-mod}}(F_e, F_f)$$

compatible w/ composition

By the above the map $\{\text{LT-mod for } \pi\} \longrightarrow \mathcal{E}_\pi$

is surjective: $e = e_{F_e}$

Similarly it is injective: $F = F_{e_F}$ $(\Rightarrow a))$

and the map

$\mathcal{O}_K \xrightarrow{\sim} \mathrm{Hom}_{\text{LT-mod}}(F_e, F_f)$ is an iso $(\Rightarrow b))$. □

Cor All LT-modules for a given π are isomorphic.

Pf. Take $a \in \mathcal{O}_K^* \Rightarrow [a]_{F,G} : F \xrightarrow{\sim} G$. □

Caution. If $\pi \neq \tilde{\pi} \in \mathcal{O}_K$ are different uniformizers, the associated LT-modules are NOT isomorphic / $\mathcal{O}_K$!

But they are isomorphic / $\mathcal{O}_{\hat{K}}$ ← $\hat{K}$:= completion of K^{ur}

The point is:

Prop The Frobenius $\varphi \in \mathrm{Gal}(K^{ur}/K)$ extends to $\hat{\varphi} \in \mathrm{Gal}(\hat{K}/K)$ & ∃ s.e.s.

a) $$0 \to \mathcal{O}_K \to \mathcal{O}_{\hat{K}} \twoheadrightarrow \mathcal{O}_{\hat{K}} \to 0$$
$$x \longmapsto \varphi(x) - x$$

b) $$1 \to \mathcal{O}_K^* \to \mathcal{O}_{\hat{K}}^* \twoheadrightarrow \mathcal{O}_{\hat{K}}^* \to 1$$
$$x \longmapsto \varphi(x)/x$$

Pf. Exercise, use $\hat{K} \twoheadrightarrow \overline{\mathbb{F}}_q$ (find solutions mod φ^n and let $n \to \infty$)

$\hat{K}$: complete; $\overline{\mathbb{F}}_q$: alg. closed □

Thm Let $\pi, \tilde{\pi} = u\pi \in \mathcal{O}_K$ ($u \in \mathcal{O}_K^*$) be any uniformizers and $e \in \mathcal{E}_\pi$, $\tilde{e} \in \mathcal{E}_{\tilde{\pi}}$. Then

a) $\exists\, \theta(T) = \varepsilon T + \cdots \in \mathcal{O}_{\hat{K}}[\![T]\!]$ w/ $\varepsilon \in \mathcal{O}_{\hat{K}}^*$ s.th. applying φ to the coefficients of θ we get:

- $\theta^\varphi(T) = \theta([u]_e(T))$,
- $\theta^\varphi(e(T)) = \tilde{e}(\theta(T))$.

b) Any such θ gives an isomorphism of formal $\mathcal{O}_K$-modules $\theta : F_e \xrightarrow{\sim} F_{\tilde{e}}$.

Pf. For b) put $F_e^\theta(X,Y) := \theta(F_e(\theta^{-1}(X), \theta^{-1}(Y)))$.

- Clearly $F_e^\theta(X,Y) \equiv X + Y \bmod (X,Y)^2$
- Claim: $F_e^\theta \in \mathcal{O}_K[\![X,Y]\!]$, and

$$\tilde{e}(F_e^\theta(X,Y)) = F_e^\theta(\tilde{e}(X), \tilde{e}(Y))$$

$\Rightarrow F_e^\theta = F_{\tilde{e}}$ by uniqueness in key lemma

$\Rightarrow \theta(F_e(X,Y)) = F_{\tilde{e}}(\theta(X), \theta(Y))$

$\Rightarrow \theta$ iso of formal gps. $\mathcal{O}_K$-linearity is similar.

For the claim,

write $(F_e \circ \theta)(X,Y) := F_e(\theta(X), \theta(Y))$ etc.

Then:

- $F_e \in (\mathcal{O}_{\hat{K}}[\![X,Y]\!])^\varphi \overset{\text{by the prop.}}{=} \mathcal{O}_K[\![X,Y]\!]$:

$$\begin{aligned}(F_e^\theta)^\varphi &= (\theta \circ F_e \circ \theta^{-1})^\varphi \\ &= \theta^\varphi \circ F_e \circ \theta^{-\varphi} \\ &= \theta \circ \underbrace{[u]_e \circ F_e \circ [u]_e^{-1}}_{= F_e} \circ \theta^{-1} = F_e^\theta\end{aligned}$$

($=$ by a))

- $\tilde{e} \circ F_e^\theta = \tilde{e} \circ \theta \circ F_e \circ \theta^{-1}$
  $= \theta^\varphi \circ e \circ F_e \circ \theta^{-1}$ by a)
  $= \theta^\varphi \circ F_e \circ e \circ \theta^{-1}$ since $e \circ F_e = F_e \circ e$
  $= \theta^\varphi \circ F_e \circ \theta^{-\varphi} \circ \tilde{e}$ by a)
  $= F_e^\theta \circ \tilde{e}$

a) Step 1: $\exists\ \alpha(T) \in \mathcal{O}_{\hat{K}}[\![T]\!]$ w/

- $\alpha(T) \equiv \varepsilon T \bmod (T^2)$, $\varepsilon \in \mathcal{O}_{\hat{K}}^*$
- $\alpha^{\varphi}(T) = \alpha([u]_e(T))$.

(construct partial sums $\alpha_r(T) = \sum_{i=1}^{r} a_i T^i$ by ind^n on r using the proposition, then let $r \to \infty$)

Step 2: $\exists \beta(T) = T + b_2 T^2 + \cdots \in \mathcal{O}_K[\![T]\!]$

sth $\theta(T) := \beta(\alpha(T))$

(which still has the properties from step 1)
moreover satisfies

$$\theta^{\varphi}(e(T)) = \tilde{e}(\theta(T)).$$

(put $f := \alpha^{\varphi} \circ e \circ \alpha^{-1}$ then $\begin{cases} f \equiv \tilde{\pi} T \bmod T^2 \\ f \equiv T^q \bmod \pi \end{cases}$
Now inductively construct
a series $\beta \in \mathcal{O}_K[\![T]\!]$ w/ $\tilde{e} \circ \beta = \beta \circ f$) $\square$

Lubin-Tate theory II: Fields of torsion pt's

Let $\mathcal{O}_{\bar{K}} := \{a \in \bar{K} \mid v_K(a) \geq 0\}$
$\cup$
$m_{\bar{K}} := \{a \in \bar{K} \mid v_K(a) > 0\}$

For any $s,t \in m_{\bar{K}}$, any power series $F \in \mathcal{O}_K[\![X,Y]\!]$ converges at (s,t) to a value $F(s,t) \in m_{\bar{K}}$.

(note: $\mathcal{O}_{\bar{K}}$ is not complete. But any $s,t \in \mathcal{O}_{\bar{K}}$ lie in the complete DVR $\mathcal{O}_L$ for some finite $L|K$ and the series converges to $F(s,t) \in m_L \subset m_{\bar{K}}$)

Apply this to F a formal $\mathcal{O}_K$-module:

Def
- $F(m_{\bar{K}}) := m_{\bar{K}}$ seen as $\mathcal{O}_K$-module
  w/ $s \overset{+}{_F} t := F(s,t) \in m_{\bar{K}}$ for $s,t \in m_{\bar{K}}$
  $a \overset{\cdot}{_F} s := [a]_F(s)$ for $a \in \mathcal{O}_K$, $s \in m_{\bar{K}}$.
- For $n \in \mathbb{N}$ we define the π^n-torsion submodule
  $F[n] := \{s \in m_{\bar{K}} \mid [\pi^n](s) = 0\} \subset F(m_{\bar{K}})$.
  ↑ an $\mathcal{O}_K$-submodule

For LT-modules: $F = F_e$ with $e \in \mathcal{E}_\pi$

$$\Rightarrow F[n] = \{ s \in \overline{K} \mid \underbrace{(e \circ \cdots \circ e)}_{n}(s) = 0 \}$$

(use $e(s) \equiv s^q \bmod \pi$ to see that solutions in $\overline{K}$ are in $\mathcal{O}_{\overline{K}}$)

Ex $K = \mathbb{Q}_p$, $e = (1+T)^p - 1$, ie $F_e = \hat{\mathbb{G}}_m$

$$\Rightarrow \underbrace{e \circ \cdots \circ e}_{n} = (1+T)^{p^n} - 1$$

$$\Rightarrow \hat{\mathbb{G}}_m[n] = \{ s \in \overline{\mathbb{Q}}_p \mid (1+s)^{p^n} = 1 \}$$

$$= \{ \zeta - 1 \mid \zeta \in \underbrace{\mu_{p^n}(\overline{\mathbb{Q}}_p)}_{=: \mu_{p^n}} \} \simeq \mu_{p^n}$$

with $\mathbb{Z}/p^n\mathbb{Z}$-module structure $a \dot{+}_F \zeta := \zeta^a$

Note: $\mathbb{Q}_p(\hat{\mathbb{G}}_m[n]) = \mathbb{Q}_p(\mu_{p^n})$

the totally ramified abelian extension

we wanted to see for Kronecker-Weber!

This generalizes to arbitrary $K/\mathbb{Q}_p$ as follows:

Lemma Let F be a LT-module for π. Then

$F[n]$ is a free module of rk 1 over $\mathcal{O}_K/\mathfrak{p}^n$.

In particular $\exists$ canonical iso

$$\mathcal{O}_K/\mathfrak{p}^n \xrightarrow{\sim} \mathrm{End}_{\mathcal{O}_K}(F[n])$$

$$\mathcal{O}_K^*/U_n(K) \xrightarrow{\sim} \mathrm{Aut}_{\mathcal{O}_K}(F[n])$$

Pf. All LT-modules for π are isomorphic / $\mathcal{O}_K$

$\Rightarrow$ WLOG $F = F_e$ with $e := \pi T + T^q \in \mathcal{E}_\pi$

(unlike $(1+T)^p - 1$, this e works for any $K/\mathbb{Q}_p$)

Then $F[n] = \{ s \in \overline{K} \mid e_n(s) = 0 \}$

w/ $e_n(T) := \underbrace{(e \circ \cdots \circ e)}_{n}(T) \in K[T]$

By ind^n on n, the polyn. e_n is separable

$\Rightarrow |F[n]| = \deg(e_n) = q^n = |\mathcal{O}_K/\mathfrak{p}^n|$

But for any $s \in F[n] \setminus F[n-1]$ we have

$\mathcal{O}_K/\mathfrak{p}^n \hookrightarrow F[n]$, $a \mapsto a \dot{+}_F s$ $\Rightarrow$ iso

□

Def For a uniformizer $\pi \in \mathcal{O}_K$,

pick any LT-module $F = F_e$ $(e \in \mathcal{E}_\pi)$

and put $K_{\pi,n} := K(F[\pi^n]) \subset \bar{K}$.

↑ depends only on π, not on F

Thm a) $K_{\pi,n} / K$ is totally ramified Galois

b) $\mathrm{Gal}(K_{\pi,n}/K) \xrightarrow{\sim} \mathrm{Aut}_{\mathcal{O}_K}(F[\pi^n]) = \mathcal{O}_K^* / U_n(K)$,

so $\forall \sigma \in \mathrm{Gal}(K_{\pi,n}/K)$ $\exists!\ u \in \mathcal{O}_K^*/U_n(K)$

sth $\sigma(\lambda) = u \underset{F}{\cdot} \lambda$ for all $\lambda \in F[\pi^n]$.

c) For any $\lambda \in F[\pi^n] \setminus F[\pi^{n-1}]$ we have:

- $K_{\pi,n} = K(\lambda)$
- $\lambda \in \mathcal{O}_{K_{\pi,n}}$ is a uniformizer for $K_{\pi,n}$ w/ minimal polynomial

$$\phi_n(x) = \frac{e_n(x)}{e_{n-1}(x)} = x^{q^{n-1}(q-1)} + \cdots + \pi$$

- In particular $N_{K_{\pi,n}/K}(-\lambda) = \pi$.

Pf. Any $e \in \mathcal{E}_\pi$ has the form

$$e(x) = x^q + a_{q-1}x^{q-1} + \cdots + a_2 x^2 + \pi x \quad \text{w/ } a_i \in \mathfrak{p}$$

$$\Rightarrow \phi_n(x) := \frac{e_n(x)}{e_{n-1}(x)}$$

$$= \frac{e(f(x))}{f(x)} \quad \text{for } f(x) := e_{n-1}(x)$$

$$= f(x)^{q-1} + a_{q-1} f(x)^{q-2} + \cdots + a_2 f(x) + \pi$$

$\Rightarrow \phi_n(x)$ is an Eisenstein polynomial

w/ $\deg(\phi_n) = q^n(q-1) = |\mathcal{O}_K^*/U_n(K)|$.

Any $\lambda \in F[\pi^n] \setminus F[\pi^{n-1}]$ is a root of $\phi_n(x)$,

hence $K(\lambda)/K$ is totally ram. of deg $\deg(\phi_n)$.

Since $\mathrm{Aut}(K_{\pi,n}) \hookrightarrow \mathrm{Aut}(F[\pi^n]) = \mathcal{O}_K^*/U_n(K)$

and $K(\lambda) \subset K_{\pi,n}$, the claim follows. □

For different choices of uniformizers $\tilde{\pi} \neq \pi \in \mathcal{O}_K$ usually $K_{\pi,n} \neq K_{\tilde{\pi},n}$ (as subfields of $\bar{K}$), but:

Prop $K^{ur} \cdot K_{\pi,n} = K^{ur} \cdot K_{\tilde{\pi},n}$ (inside $\bar{K}$).

Pf. Let $F, \tilde{F}$ be LT-modules for $\pi, \tilde{\pi}$ resp.

By the previous section $\exists\, \theta = \varepsilon T + \cdots \in \mathcal{O}_{\hat{K}}[\![T]\!]$

($\varepsilon \in \mathcal{O}_{\hat{K}}^*$; $\hat{K} :=$ completion of K^{ur})

giving an iso

$\theta : F \xrightarrow{\sim} \tilde{F}$ of formal $\mathcal{O}_K$-modules

$\Rightarrow$ iso $\theta : F[n] \xrightarrow{\sim} \tilde{F}[n]$ of $\mathcal{O}_K$-modules

(Note: A priori $\theta(F[n]) \subset \hat{\bar{K}} :=$ completion of $\bar{K}$, but in fact $\theta(F[n]) \subset \bar{K}$ because it is the set of zeroes of a polynomial $\tilde{e} \circ \cdots \circ \tilde{e}$ w/ $\tilde{e} \in \mathcal{E}_{\tilde{\pi}}$)

$\Rightarrow \tilde{F}[n] = \theta(F[n]) \subseteq (K^{ur} \cdot K_{\pi,n})^{\wedge} \cap \bar{K} = K^{ur} \cdot K_{\pi,n}$ (completion)

$\Rightarrow K^{ur} \cdot K_{\tilde{\pi},n} \subseteq K^{ur} \cdot K_{\pi,n}$

$\Rightarrow$ equality by symmetry.

(use that completion doesn't change the value gp, and that $K^{ur} \cdot K_{\pi,n} = (K_{\pi,n})^{ur}$)

□

Put $L_n := K^{ur} \cdot K_{\pi,n} \subset \bar{K}$ (independent of π).

Since $K^{ur} \cap K_{\pi,n} = K$ (look at ramificat^n), we get

$$\mathrm{Gal}(L_n/K) \xrightarrow{\sim} \mathrm{Gal}(K^{ur}/K) \times \mathrm{Gal}(K_{\pi,n}/K)$$
$$\alpha \longmapsto (\alpha|_{K^{ur}}, \alpha|_{K_{\pi,n}}).$$

($K_{\pi,n}$ depending on π)

Def Fix a uniformizer $\pi \in \mathcal{O}_K$.

Define $\omega_\pi : K^* \to \mathrm{Gal}(L_n/K)$

by putting for $a = u\pi^v$ w/ $u \in \mathcal{O}_K^*$:

- $\omega_\pi(a)|_{K^{ur}} := \varphi^v$
- $\omega_\pi(a)|_{K_{\pi,n}} := \sigma_{\pi,u}$

for the unique $\sigma_{\pi,u} \in \mathrm{Gal}(K_{\pi,n})$ sth $\sigma_{\pi,u}(\lambda) = u^{-1} \underset{F}{\circ} \lambda$ for all $\lambda \in F[n]$, where F is a LT module for π.

We can now describe the norm residue symbol on $L_n = K^{ur} \cdot K_{\pi,n}$ explicitly:

Thm $(-, L_n/K) = \omega_{\pi,n}$.

Pf. K^* is generated by uniformizers $\tilde{\pi}$

$\Rightarrow$ enough to check $(\tilde{\pi}, L_n/K) = \omega_{\pi,n}(\tilde{\pi})$

1) On K^{ur} we have

$$(\tilde{\pi}, L_n/K)|_{K^{ur}} = (\tilde{\pi}, K^{ur}/K) = \varphi = \omega_\pi(\pi)|_{K^{ur}}$$

2) On $K_{\tilde{\pi},n}$ we have

$$(\tilde{\pi}, L_n/K)|_{K_{\tilde{\pi},n}} = (\tilde{\pi}, K_{\tilde{\pi},n}) = id$$

$\Rightarrow$ remains to check $\omega_\pi(\tilde{\pi})|_{K_{\tilde{\pi},n}} = id$.

Let F be a LT-mod for π

& $\tilde{F}$ ——//—— $\tilde{\pi}$

Want: $\omega_\pi(\tilde{\pi})(\tilde{\lambda}) = \tilde{\lambda}$ for all $\tilde{\lambda} \in \tilde{F}[n]$.

By the previous section

$\exists\ \theta : F \xrightarrow{\sim} \tilde{F}$ over $\mathcal{O}_{\hat{K}}$

w/ $\theta^\varphi(T) = \theta([u]_F(T))$ for $u = \tilde{\pi}/\pi$ (*)

$\Rightarrow$ iso $\theta : F[n] \xrightarrow{\sim} \tilde{F}[n]$

ψ ψ

$\exists\ \lambda \longmapsto \tilde{\lambda}$

$\Rightarrow \omega_\pi(\tilde{\pi})(\tilde{\lambda})$

$= \omega_\pi(\tilde{\pi})(\theta(\lambda))$

$= \theta^\varphi(\omega_\pi(\tilde{\pi})(\lambda))$ since $\omega_\pi(\tilde{\pi})|_{K^{ur}} = \varphi$

$= \theta^\varphi(\sigma_u(\lambda))$ since $\omega_\pi(\tilde{\pi})|_{K_{\pi,n}} = \sigma_u$

$= \theta^\varphi(u^{-1} \cdot_F \lambda)$

$= \theta(\lambda)$ by (*)

$= \tilde{\lambda}$

□

Cor The norm group for $K_{\pi,n}/K$ is

$$N_{K_{\pi,n}/K}(K_{\pi,n}^*) = U_n(K)\cdot\pi^{\mathbb{Z}} \subset K^*$$

Pf. Let F be a LT-module for π.

For $a = u\pi^v \in K^*$ w/ $u \in \mathcal{O}_K^*$ the thm says

$$(a, K_{\pi,n}/K)(\lambda) = u^{-1} \underset{F}{\cdot} \lambda, \quad \text{all } \lambda \in F[n].$$

So

$$a \in N(K_{\pi,n}^*) \overset{\text{local CFT}}{\iff} (a, K_{\pi,n}/K) = \mathrm{id}$$

$$\iff u^{-1} \underset{F}{\cdot} \lambda = \lambda \quad \forall\, \lambda \in F[n]$$

$$\iff u^{-1} \underset{F}{\cdot} (-) = \mathrm{id} \in \mathrm{End}_{\mathcal{O}_K}(F[n])$$

$$\iff u \in U_n(K)$$

↑ since $F[n] \simeq \mathcal{O}_K/\wp^n$ as $\mathcal{O}_K$-module by the previous section

□

Cor Let L/K be the unique unramified extension of degree f. Then $M := L\cdot K_{\pi,n}$ has

$$N_{M/K}(M^*) = U_n(K)\cdot\pi^{f\mathbb{Z}}.$$

Pf.

$$N_{M/K}(M^*) = N_{L/K}(L^*) \cap N_{K_{\pi,n}/K}(K_{\pi,n}^*)$$

$$= (\mathcal{O}_K^*\cdot\pi^{f\mathbb{Z}}) \cap \underbrace{(U_n(K)\cdot\pi^{\mathbb{Z}})}_{\text{by previous cor.}}$$

$$= U_n(K)\cdot\pi^{f\mathbb{Z}}$$

□

Cor ("Explicit local reciprocity law")

Put $K_\pi := \bigcup_{n\geq 1} K_{\pi,n} \subset \bar{K}$, then $K^{ab} = K^{ur}\cdot K_\pi$

and hence

$$(\cdot, K): K^* = \mathcal{O}_K^* \times \pi^{\mathbb{Z}} \xrightarrow{\sim} G_K^{ab} = \mathrm{Gal}(K^{ur}/K) \times \mathrm{Gal}(K_\pi)$$

$$\psi \qquad\qquad\qquad\qquad \psi$$

$$u\cdot\pi^m \longmapsto (\varphi^m, \sigma_u)$$

Pf. We only need to show any abelian M/K is contained in some $L \cdot K_{\pi,n}$ with L/K unram, $n \in \mathbb{N}$.

To see this, note:

$N_{M/K}(M^*) \subset K^*$ open subgp

$\Rightarrow N_{M/K}(M^*) \supset U_n(K) \cdot \pi^{f\mathbb{Z}}$ for some n, f

$\| $

$N_{LK_{\pi,n}}((L \cdot K_{\pi,n})^*)$ by previous cor

w/ L/K unramified of degree f

$\Rightarrow M \subset L \cdot K_{\pi,n}$ by local CFT correspondence

□

IV. Global CFT

Goal: For any # field K,

$$\exists\ (\cdot, K) : C_K \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(K^{ab}/K)$$

inducing for every finite abelian ext^n L/K an iso ("Artin reciprocity")

$$\mathrm{Art}_{L/K} : C_K/N_{L/K}(C_L) \xrightarrow{\sim} \mathrm{Gal}(L/K)$$

& we get a bijection ("existence thm")

$$\left\{\begin{array}{l}\text{closed subgps of}\\ \text{finite index in } C_K\end{array}\right\} \xleftrightarrow{\sim} \left\{\begin{array}{l}\text{finite abelian}\\ \text{extensions of } K\end{array}\right\}$$

Here C_K is the idèle class gp (see below), which takes the role that K^* had in local CFT.

1. Idèles

K number field

Recall: A place $\wp$ of K is one of the following:

a) A max. ideal $\wp \trianglelefteq \mathcal{O}_K$, w/ discrete valuation $v_\wp : K^* \twoheadrightarrow \mathbb{Z}$ and absolute value $|\cdot|_\wp := |\mathbb{F}_\wp|^{-v_\wp(\cdot)}$. — Write $\wp \nmid \infty$

b) A real embedding $K \hookrightarrow \mathbb{R}$, we then put $|\cdot|_\wp := |\iota(\cdot)|$.

c) A pair of cplex conj. emb. $\iota \neq \bar{\iota} : K \hookrightarrow \mathbb{C}$, we then put $|\cdot|_\wp := |\iota(\cdot)|^2$.

— Write $\wp \mid \infty$

This normalization leads to the **Product formula**:

$$\prod_\wp |a|_\wp = 1 \quad \text{for all } a \in K^*$$

We put $K_\wp :=$ completion of K wrt $|\cdot|_\wp$.

Def For a finite set S of places containing all $\wp \mid \infty$,

the <u>gp of S-idèles</u> is

$$\mathbb{I}_{K,S} := \prod_{\wp \in S} K_\wp^* \times \prod_{\wp \notin S} \mathcal{O}_{K_\wp}^* \subset \prod_\wp K_\wp^*$$

The <u>gp of idèles</u> is $\mathbb{I}_K := \bigcup_{\substack{S \\ \text{finite}}} \mathbb{I}_{K,S} \subset \prod_\wp K_\wp^*$

We have a natural embedding $K^* \hookrightarrow \mathbb{I}_K$, $x \longmapsto (x)$

where $(x) \in \mathbb{I}_K$ is the "diagonal" idèle with components $(x)_\wp := x \in K_\wp$ for all $\wp$.

<u>Ex</u> For $S \supset S_\infty := \{\text{places } \wp \mid \infty\}$,

the gp of S-units in K is

$$\mathcal{O}_{K,S}^* = K^* \cap \mathbb{I}_{K,S} = \{a \in K^* \mid \forall \wp \notin S : a \in \mathcal{O}_{K_\wp}^*\}.$$

Def The <u>idèle class gp</u> of K is $C_K := \mathbb{I}_K / K^*$.

Compare w/ the ideal class gp $\mathcal{C}\ell_K := I_K / P_K$

where $I_K := \{\text{fractional ideals of } K\}$,

$P_K := \{\text{principal fractional ideals of } K\}$:

$$\exists \text{ epi } \mathbb{I}_K \twoheadrightarrow I_K, \quad a \longmapsto \prod_{\wp \nmid \infty} \wp^{v_\wp(a_\wp)}$$

giving a comm. diagram w/ exact rows:

$$\begin{array}{ccccccccc} 1 & \to & \mathcal{O}_K^* & \to & K^* & \to & P_K & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & \mathbb{I}_{K,S_\infty} & \to & \mathbb{I}_K & \to & I_K & \to & 1 \end{array}$$

$$\Rightarrow \quad C_K \twoheadrightarrow \mathcal{C}\ell_K$$

$$C_K \twoheadrightarrow \mathbb{I}_K / K^* \cdot \mathbb{I}_{K,S_\infty} \hookrightarrow \mathcal{C}\ell_K$$

Cor For all large enough S:

a) $\mathbb{I}_K = K^* \cdot \mathbb{I}_{K,S}$,

b) $C_K \simeq \mathbb{I}_{K,S} / \mathcal{O}_{K,S}^*$.

Pf. The ideal class gp $\mathcal{C}\ell_K$ is finite

Pick ideals $\mathfrak{a}_1, \dots, \mathfrak{a}_n \triangleleft \mathcal{O}_K$ representing all its elements,

and let $S_0 := \{ \mathfrak{p} : \exists i \text{ with } \mathfrak{p} \mid \mathfrak{a}_i \}$.

$\Rightarrow \quad \mathbb{I}_{K,S_0} \twoheadrightarrow \mathcal{C}\ell_K$

$\Rightarrow \quad \mathbb{I}_K = \mathbb{I}_{K,S_0} \cdot \underbrace{\ker(\mathbb{I}_K \twoheadrightarrow \mathcal{C}\ell_K)}_{= K^* \cdot \mathbb{I}_{K,S_\infty}}$

$= K^* \cdot \mathbb{I}_{K,S}$ by the above

for $S := S_0 \cup S_\infty$

This proves a), and b) follows via

$C_K = \mathbb{I}_K / K^* = K^* \cdot \mathbb{I}_{K,S} / K^* \simeq \mathbb{I}_{K,S} / \underbrace{K^* \cap \mathbb{I}_{K,S}}_{= \mathcal{O}_{K,S}^*}$ □

Now take a finite extension L/K. Then:

- We get an embedding $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$

  $a \longmapsto b$ where

  $b_\mathfrak{P} := a_\mathfrak{p} \in K_\mathfrak{p} \subset L_\mathfrak{P}$ for $\mathfrak{P} \mid \mathfrak{p}$

  w/ image $= \{ b \in \mathbb{I}_L \mid \forall \mathfrak{P}, \mathfrak{Q} \text{ above } \mathfrak{p}: b_\mathfrak{P} = b_\mathfrak{Q} \in K_\mathfrak{p} \}$

- For L/K Galois, the gp $G := \mathrm{Gal}(L/K)$ acts on $\mathbb{I}_L$ via

  $$(g \cdot b)_\mathfrak{P} := g(b_{g^{-1}(\mathfrak{P})}) \in L_\mathfrak{P} \quad (g \in G).$$

Lemma For L/K Galois w/ gp $G = \mathrm{Gal}(L/K)$, we have

$$\mathbb{I}_K = \mathbb{I}_L^G.$$

Pf. "$\subset$": For $g \in G$ have $\sigma : L_{\sigma^{-1}\mathfrak{P}} \xrightarrow{\sim} L_\mathfrak{P}$

If $b \in \mathbb{I}_L$ is the image of $a \in \mathbb{I}_K$, then

$(g \cdot b)_\mathfrak{P} = g(b_{g^{-1}\mathfrak{P}}) \overset{\uparrow}{=} g(a_\mathfrak{p}) = a_\mathfrak{p} = b_\mathfrak{P} \quad \forall \mathfrak{P}$

$g^{-1}\mathfrak{P} \cap K =: \mathfrak{p}$ $\Rightarrow g \cdot b = b$

"$\supset$": Let $b \in \mathbb{I}_L$ with $g \cdot b = b$ for all $g \in G$.

$\Rightarrow$ $g(b_{g^{-1}\mathfrak{P}}) = b_{\mathfrak{P}}$ in $L_{\mathfrak{P}}$ for all $\mathfrak{P}$

- Take $g \in G_{\mathfrak{P}} := \{ g \in G \mid g\mathfrak{P} = \mathfrak{P} \} \simeq \mathrm{Gal}(L_{\mathfrak{P}} | K_{\mathfrak{p}})$ $(\mathfrak{p} := \mathfrak{P} \cap K)$

  $\Rightarrow$ $g(b_{\mathfrak{P}}) = b_{\mathfrak{P}}$ $\forall g \in \mathrm{Gal}(L_{\mathfrak{P}} | K_{\mathfrak{p}})$

  $\Rightarrow$ $b_{\mathfrak{P}} \in K_{\mathfrak{p}}$

- Now take $g \in G$ arbitrary:

  $\forall$ $\mathfrak{P}, \mathfrak{Q}$ above the same $\mathfrak{p}$ $\exists g \in G$: $\mathfrak{Q} = g\mathfrak{P}$

  $\Rightarrow$ $b_{\mathfrak{P}} = g(b_{\mathfrak{P}}) = g(b_{g^{-1}\mathfrak{Q}}) = (g \cdot b)_{\mathfrak{Q}} = b_{\mathfrak{Q}}$

  ($b_{\mathfrak{P}} \in K_{\mathfrak{p}}$; $\mathfrak{P} = g^{-1}\mathfrak{Q}$; def^n of action; $g \cdot b = b$)

  $\Rightarrow$ $b \in \mathbb{I}_K$ by previous descript^n of $\mathbb{I}_K \subset \mathbb{I}_L$. $\square$

The same works for idèle class gps:

Prop a) For any finite L/K the map $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ induces an embedding $C_K \hookrightarrow C_L$.

b) If L/K is Galois w/ gp $G = \mathrm{Gal}(L/K)$, then G naturally acts on C_L such that its invariants are $C_K = C_L^G$.

Pf. a) We must show $\mathbb{I}_K \cap L^* = K^*$ in $\mathbb{I}_L$.

Let M/K be the Galois hull of L/K

$\mathbb{I}_K \subset \mathbb{I}_L \subset \mathbb{I}_M$ $\Rightarrow$ enough to prove claim for M/K

So wlog $L = M$. Put $G = \mathrm{Gal}(L/K)$.

$\Rightarrow$ $\mathbb{I}_K = \mathbb{I}_L^G$ by previous lemma

$\Rightarrow$ $\mathbb{I}_K \cap L^* = \mathbb{I}_L^G \cap L^* = (L^*)^G = K^*$

b) The embedding $L^* \hookrightarrow \mathbb{I}_L$ is G-equivariant

$\Rightarrow$ G-action descends to the quotient $C_L = \mathbb{I}_L / L^*$.

From $1 \to L^* \to \mathbb{I}_L \to C_L \to 1$ we get

$$1 \to \underset{\| \; K^*}{L^{*G}} \to \underset{\| \; \mathbb{I}_K}{\mathbb{I}_L^G} \to C_L^G \to \underset{\| \; 0}{H^1(G, L^*)}$$

□

Rem So far we only looked at $\mathbb{I}_K \subset \mathbb{I}_L$ as abstract groups (no topology involved).

That's in fact enough to prove Artin reciprocity, which will take up most of this section. Only for the existence thm ("norm subgps = closed subgps of finite index") we'll use topology. However, we discuss the idèle topology now for later reference:

Topology on idèles:

View $\mathbb{I}_K$ as a top gp wrt the topology induced by the product topology on $\prod_p K_p^*$ via the embedding

$$\mathbb{I}_K = \bigcup_{S \text{ finite}} \mathbb{I}_{K,S} \hookrightarrow \prod_p K_p^*.$$

Explicitly, a basis of open subsets is given by the subsets

$\prod_p W_p \subset \mathbb{I}_K$ w/ • $W_p \subset K_p^*$ open for all p,

• $W_p = \mathcal{O}_{K_p}^*$ for almost all p.

(i.e. all but finitely many)

$\Rightarrow$ $\mathbb{I}_K$ is a locally cpact Hausdorff gp.

Ex The epi $p: \mathbb{I}_K \twoheadrightarrow I_K$ is continuous for the discrete topology on $I_K = \prod_{p \nmid \infty} \mathbb{Z}$

(since $p^{-1}(\alpha) = x \cdot \prod_p \mathcal{O}_{K_p}^*$ for any $x \in p^{-1}(\alpha)$).

Lemma $K^* \hookrightarrow \mathbb{I}_K$ is a discrete subgp.

Pf. Enough to find $U \subset \mathbb{I}_K$ open w/ $K^* \cap U = \{1\}$.

Try

$$U := \prod_{p \in S} W_p \times \prod_{p \notin S} \mathcal{O}_{K_p}^*$$

w/ $S \supset S_\infty$ finite set of places,

$$W_p = \{ a \in K_p : |a_p - 1|_p < \varepsilon \} \quad \text{for } 0 < \varepsilon < 1.$$

For $a \in K^* \cap U$ then $|a-1|_p \leq 1$ for all p,

and strict inequality holds for all $p \in S \neq \emptyset$.

$\Rightarrow \prod_p |a-1|_p < 1$

$\Rightarrow a = 1$, else this contradicts the product formula. $\square$

Cor $K^* \hookrightarrow \mathbb{I}_K$ is closed, so $C_K = \mathbb{I}_K / K^*$

is again a Hausdorff top gp (& loc. cpact). $\square$

Rem C_K is NOT compact:

The "absolute norm"

$$N : \mathbb{I}_K \twoheadrightarrow \mathbb{R}_{>0}^*, \quad (a_p)_p \mapsto \prod_p |a_p|_p^{-1}$$

descends by the product formula to a continuous epi

$$N : C_K = \mathbb{I}_K / K^* \twoheadrightarrow \mathbb{R}_{>0}^*.$$

But one can show that

$$C_K^0 := \ker (N : C_K \twoheadrightarrow \mathbb{R}_{>0}^*) \text{ is compact.}$$

This implies both the finiteness of Cl_K and the Dirichlet unit thm, but its proof uses similar ideas as those two. We won't need it for now (maybe discuss it later).

2. Cohomology of the idèles

L/K finite abelian Galois extension

$G := \mathrm{Gal}(L/K)$

Goal: Understand $H^\bullet(G, C_L)$ for CFT

Since $C_L = \mathbb{I}_L / K^*$, we begin w/ $H^\bullet(G, \mathbb{I}_L)$!

Note: $\mathbb{I}_L = \bigcup_S \mathbb{I}_{L,S}$ (with $S \supset S_\infty$ running through all finite sets of places of K)

where

$$\mathbb{I}_{L,S} := \prod_{\mathfrak{p} \in S} \underbrace{\prod_{\mathfrak{P}|\mathfrak{p}} L_{\mathfrak{P}}^*}_{=: \mathbb{I}_L^{\mathfrak{p}}} \times \prod_{\mathfrak{p} \notin S} \underbrace{\prod_{\mathfrak{P}|\mathfrak{p}} \mathcal{O}_{L_{\mathfrak{P}}}^*}_{=: \mathbb{U}_L^{\mathfrak{p}}}$$

The G-action preserves the factors $\mathbb{I}_L^{\mathfrak{p}}$ & $\mathbb{U}_L^{\mathfrak{p}}$,

it is given by $(g \cdot a)_{\mathfrak{P}} := g(a_{g^{-1}\mathfrak{P}})$ for $g \in G$.

Prop For any place $\mathfrak{p}$ of K,

fix $\mathfrak{P}|\mathfrak{p}$ w/ decomposition gp $G_{\mathfrak{P}} \subset G$.

Then $H^\bullet(G, \mathbb{I}_L^{\mathfrak{p}}) \simeq H^\bullet(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*)$,

$H^\bullet(G, \mathbb{U}_L^{\mathfrak{p}}) \simeq H^\bullet(G_{\mathfrak{P}}, \mathcal{O}_{L_{\mathfrak{P}}}^*)$,

and ditto for Tate cohomology.

Pf. $\mathbb{I}_L^{\mathfrak{p}} = \prod_{g \in G/G_{\mathfrak{P}}} g(L_{\mathfrak{P}}^*) \simeq \mathrm{Ind}_{G_{\mathfrak{P}}}^G (L_{\mathfrak{P}}^*)$

& $\mathbb{U}_L^{\mathfrak{p}} = \prod_{g \in G/G_{\mathfrak{P}}} g(\mathcal{O}_{L_{\mathfrak{P}}}^*) \simeq \mathrm{Ind}_{G_{\mathfrak{P}}}^G (\mathcal{O}_{L_{\mathfrak{P}}}^*)$

$\Rightarrow$ Done by Shapiro's lemma. $\square$

Rem If $\mathfrak{p}$ is unramified in L/K,

we know from unramified local CFT

that

$$H_T^\bullet(G_{\mathfrak{P}}, \mathcal{O}_{L_{\mathfrak{P}}}^*) = 0.$$

Cor $H^\bullet_T(G, \mathbb{I}_L) = \bigoplus_{\mathfrak{p}} H^\bullet_T(G_{\mathfrak{P}}, L^*_{\mathfrak{P}})$

$\mathfrak{p}$ runs through all places of K; $\mathfrak{P}$ any chosen place above $\mathfrak{p}$

Pf. $\mathbb{I}_L = \bigcup_S \mathbb{I}_{L,S}$

$\Rightarrow H^i_T(G, \mathbb{I}_L) = \varinjlim_S H^i_T(G, \mathbb{I}_{L,S})$

$= \prod_{\mathfrak{p}\in S} H^i_T(G, \mathbb{I}_L^{\mathfrak{p}}) \times \prod_{\mathfrak{p}\notin S} H^i_T(G, U_L^{\mathfrak{p}})$

$= \prod_{\mathfrak{p}\in S} H^i_T(G_{\mathfrak{P}}, L^*_{\mathfrak{P}}) \times \prod_{\mathfrak{p}\notin S} H^i_T(G_{\mathfrak{P}}, \mathcal{O}^*_{L\mathfrak{p}})$

by the proposition

For $\varinjlim_S$ any large enough S contains all places $\mathfrak{p}$ that ramify in $L|K$, hence $H^i_T(G_{\mathfrak{P}}, \mathcal{O}^*_{L\mathfrak{p}}) = 0 \ \forall \mathfrak{p} \notin S$.

$\Rightarrow H^i_T(G, \mathbb{I}_L) = \varinjlim_S \prod_{\mathfrak{p}\in S} H^i_T(G_{\mathfrak{P}}, L^*_{\mathfrak{P}}) = \bigoplus_{\mathfrak{p}} H^i_T(G_{\mathfrak{P}}, L^*_{\mathfrak{P}})$ □

Rem The above decomposition is canonical:

If $\mathfrak{P}, \mathfrak{Q}$ are any two choices of primes above $\mathfrak{p}$, pick $g \in G$ with $\mathfrak{Q} = g\mathfrak{P}$ to get an iso

$g_*: H^\bullet(G_{\mathfrak{P}}, L^*_{\mathfrak{P}}) \xrightarrow{\sim} H^\bullet(G_{\mathfrak{Q}}, L^*_{\mathfrak{Q}})$

$$\begin{bmatrix} G_{\mathfrak{P}} & \xrightarrow{\sim} & G_{\mathfrak{Q}} \\ \circlearrowright & & \circlearrowright \\ L^*_{\mathfrak{P}} & \xrightarrow{\sim} & L^*_{\mathfrak{Q}} \end{bmatrix}$$

$x \mapsto gxg^{-1}$; $a \mapsto ga$

If $\mathfrak{Q} = \mathfrak{P}$ (i.e. $g \in G_{\mathfrak{P}}$), then $g_* = \mathrm{id}$ by the discussion of functoriality in section II.3

$\Rightarrow$ For arbitrary $\mathfrak{P}, \mathfrak{Q}$ above $\mathfrak{p}$ & $g, h \in G$ w/ $g\mathfrak{P} = h\mathfrak{P} = \mathfrak{Q}$:

$g_* = h_*$ ($g = h \cdot \sigma$ w/ $\sigma \in G_{\mathfrak{P}}$, ie $\sigma_* = \mathrm{id}$)

$\Rightarrow g_*: H^\bullet(G_{\mathfrak{P}}, L^*_{\mathfrak{P}}) \xrightarrow{\sim} H^\bullet(G_{\mathfrak{Q}}, L^*_{\mathfrak{Q}})$

canonical iso (independent of g w/ $\mathfrak{Q} = g\mathfrak{P}$)!

Ex The corollary implies:

a) $H^1(G, \mathbb{I}_L) = \bigoplus_{\wp} H^1(G_\wp, L_\wp^*) = 0$

b) $H^2(G, \mathbb{I}_L) \xrightarrow{\sim} \bigoplus_{\wp} \frac{1}{[L_\wp : L_\wp]}\mathbb{Z}/\mathbb{Z}$

(local CFT)

where in the direct sums $\wp$ denotes any place above $\wp$.

Similarly we get:

Lemma Let L/K be cyclic ($\Rightarrow H_T^\bullet(G,-)$ 2-periodic).
Then for any finite set S of places of K,
we have the Herbrand quotient

$$h(\mathbb{I}_{L,S}) = \prod_{\wp \in S} [L_\wp : K_\wp]$$

($\wp$ any $\wp$ above $\wp$)

$h = \frac{\#H_T^2(\mathbb{I}_{L,S})}{\#H_T^1(\mathbb{I}_{L,S})}$

defined if G is cyclic
and $\#H_T^i(\mathbb{I}_{L,S}) < \infty$ (true for $\mathbb{I}_{L,S}$, not for $\mathbb{I}_L$)

Pf. By the proposition

$$\mathbb{I}_{L,S} = \prod_{\wp \in S} \mathbb{I}_L^\wp \times \prod_{\wp \notin S} U_L^\wp$$

- $H_T^\bullet(G, U_L^\wp) \simeq H_T^\bullet(G_\wp, \mathcal{O}_{L_\wp}^*)$ (any $\wp | \wp$)

  As we saw on the way to local CFT,

  $\exists$ finite index subgp $U_\wp \subset \mathcal{O}_{L_\wp}^*$ w/ $H_T^\bullet(G_\wp, U_\wp) = 0$

  $$\Rightarrow h(\mathcal{O}_{L_\wp}^*) = h(U_\wp) = 0$$

  (finite index doesn't change Herbrand quotient)

- $H_T^\bullet(G, \mathbb{I}_L^\wp) \simeq H_T^\bullet(G_\wp, L_\wp^*)$

  $$\simeq \begin{cases} 0, & \bullet = 1 \quad (\text{H90}) \\ \frac{1}{[L_\wp : K_\wp]}\mathbb{Z}/\mathbb{Z}, & \bullet = 2 \quad (\text{local CFT}) \end{cases}$$

$$\Rightarrow h(G, \mathbb{I}_L^\wp) = [L_\wp : K_\wp].$$

□

3. Cohomology of the units

L/K Galois extension of number fields w/ gp G

For any finite set $S \supset S_\infty$ of places in K, let

$$\mathcal{O}^*_{L,S} := \{ a \in L^* \mid \forall \mathfrak{p} \notin S : v_{\mathfrak{p}}(a) \geq 0 \}.$$

$$\Rightarrow C_L \simeq \underbrace{\mathbb{I}_{L,S}}_{\text{previous section}} / \underbrace{\mathcal{O}^*_{L,S}}_{\text{now}}$$

Prop Let L/K be cyclic. Then for any S as above the Herbrand quotient $h(\mathcal{O}^*_{L,S})$ is defined, and

$$h(\mathcal{O}^*_{L,S}) = \frac{1}{[L:K]} \cdot \prod_{\mathfrak{p} \in S} [L_{\mathfrak{p}} : K_{\mathfrak{p}}].$$

($\mathfrak{p}$: any $\mathfrak{P} \mid \mathfrak{p}$)

Pf. Let $T := \{ \mathfrak{P} \text{ place of } L \mid \mathfrak{P} \cap K \in S \}$

$$\Rightarrow V := \mathbb{R}^T = \bigoplus_{\mathfrak{P} \in T} \mathbb{R}$$

has a natural G-action defined by

$$(g \cdot a)_{\mathfrak{P}} := a_{g^{-1}\mathfrak{P}} \quad \text{for } g \in G,\ \mathfrak{P} \in T,\ a \in V$$

We consider two G-stable lattices in V:

1) The "standard lattice"

$$\Lambda_1 := \mathbb{Z}^T \subset V = \mathbb{R}^T$$

Since $T \simeq \coprod_{\mathfrak{p} \in S} G/G_{\mathfrak{P}}$ as a set w/ G-action, ($\mathfrak{P}$: any $\mathfrak{P} \mid \mathfrak{p}$)

we have

$$\Lambda_1 \simeq \bigoplus_{\mathfrak{p} \in S} \mathrm{Ind}_{G_{\mathfrak{P}}}^{G}(\mathbb{Z})$$

$$\Rightarrow h(G, \Lambda_1) = \prod_{\mathfrak{p} \in S} h(G_{\mathfrak{P}}, \mathbb{Z}) = \prod_{\mathfrak{p} \in S} [L_{\mathfrak{P}} : K_{\mathfrak{p}}]$$

($\mathfrak{P}$: any $\mathfrak{P} \mid \mathfrak{p}$)

2) The "lattice of S-units":

Consider the G-equivariant map

$$\begin{aligned} \mathrm{Log}: \mathcal{O}_{L,S}^* &\longrightarrow V = \mathbb{R}^T \\ a &\longmapsto (\log |a|_\mathfrak{p})_{\mathfrak{p}\in T} \end{aligned}$$

w/ image $\subset V_0 := \{(a_\mathfrak{p})_\mathfrak{p} \in V \mid \sum_\mathfrak{p} a_\mathfrak{p} = 0\}$

(product formula)

Dirichlet's unit thm shows

- $\mathrm{Log}(\mathcal{O}_{L,S}^*)$ is a lattice in V_0
- $\ker(\mathrm{Log}) = \mu(L) := \{\zeta \in L \mid \exists n \in \mathbb{N}: \zeta^n = 1\}$

(a finite group!)

Put $v := (1,1,\dots,1) \in V$

$$\Rightarrow \Lambda_2 := \mathrm{Log}(\mathcal{O}_{L,S}^*) \oplus \mathbb{Z}\cdot v$$

is a lattice in $V = V_0 \oplus \mathbb{R}\cdot v$

and $\exists$ exact sequence of G-modules

$$0 \to \underbrace{\mu(L)}_{\text{finite}} \to \mathcal{O}_{L,S}^* \to \Lambda_2 \to \mathbb{Z} \to 0$$

$$\Rightarrow h(\Lambda_2) = h(\mathcal{O}_{L,S}^*) \cdot \underbrace{h(\mathbb{Z})}_{=|G|=[L:K]} \cdot \underbrace{h(\mu(L))^{-1}}_{=1}$$

$$= [L:K] \cdot h(\mathcal{O}_{L,S}^*)$$

Conclusion:

We have two G-stable lattices $\Lambda_1, \Lambda_2 \subset V$

sth $h(\Lambda_1) = \prod_{\mathfrak{p}\in S} [L_\mathfrak{p} : K_\mathfrak{p}]$,

$h(\Lambda_2) = [L:K] \cdot h(\mathcal{O}_{L,S}^*)$.

$\Rightarrow$ Done by the next lemma! $\square$

Lemma Let V be a fin. dim. $\mathbb{R}$-space over $\mathbb{R}$

w/ a linear action of a finite cyclic gp G.

Let $\Lambda_1, \Lambda_2 \subset V$ be G-stable lattices.

If $h(\Lambda_1)$ is defined, then so is $h(\Lambda_2)$

and we have

$$h(\Lambda_1) = h(\Lambda_2).$$

Pf. Put $\Lambda_{i,R} := \Lambda_i \otimes_{\mathbb{Z}} R$ for comm. rings R.

① Claim: $\Lambda_{1,\mathbb{Q}} \simeq \Lambda_{2,\mathbb{Q}}$ as $\mathbb{Q}[G]$-module

Indeed: $\Lambda_{i,\mathbb{R}} := \Lambda_i \otimes_{\mathbb{Z}} \mathbb{R} \xrightarrow{\sim} V$ ($\Lambda_i \subset V$ lattices)

$\Rightarrow \Lambda_{1,\mathbb{R}} \simeq \Lambda_{2,\mathbb{R}}$ as $\mathbb{R}[G]$-module (*)

Linear algebra:

$$\mathrm{Hom}_{\mathbb{R}[G]}(\Lambda_{1,\mathbb{R}}, \Lambda_{2,\mathbb{R}}) = \mathrm{Hom}_{\mathbb{Q}[G]}(\Lambda_{1,\mathbb{Q}}, \Lambda_{2,\mathbb{Q}}) \otimes_{\mathbb{Q}} \mathbb{R}$$

[works for $\mathbb{R}/\mathbb{Q}$ replaced by any field extension K/k:
For any $k[G]$-modules M_1, M_2,
$\mathrm{Hom}_{K[G]}(M_{1,K}, M_{2,K}) \subset \mathrm{Hom}_K(M_{1,K}, M_{2,K})$
$= \mathrm{Hom}_k(M_1, M_2) \otimes_k K$
is cut out by eqs $f \cdot (g_1(g) \otimes \mathrm{id}) = (g_2(g) \otimes \mathrm{id}) \cdot f$
in the matrix $f = (f_{\alpha\beta})$ w/ coeffs $(g_i(g))_{\alpha\beta} \in k$]

Pick a basis $\varphi_1, \dots, \varphi_n$ of $\mathrm{Hom}_{\mathbb{Q}[G]}(\Lambda_{1,\mathbb{Q}}, \Lambda_{2,\mathbb{Q}})$

By (*) $\exists \lambda_1, \dots, \lambda_n \in \mathbb{R}$: $\det(\sum_i \lambda_i \varphi_i) \neq 0$.

$\Rightarrow \det(\sum_i x_i \varphi_i) \neq 0$ in $\mathbb{Q}[x_1, \dots, x_n]$

$\Rightarrow \exists \mu_1, \dots, \mu_n \in \mathbb{Q}$: $\det(\sum_i \mu_i \varphi_i) \neq 0$

$\Rightarrow \exists$ iso $\Lambda_{1,\mathbb{Q}} \xrightarrow{\sim} \Lambda_{2,\mathbb{Q}}$ as claimed

② Compare Herbrand quotients:

Λ_i fin. gen. $\mathbb{Z}$-mod $\Rightarrow$ $\mathrm{Tors}(\Lambda_i)$ finite

$\Rightarrow h(\Lambda_i) = h(\underbrace{\Lambda_i / \mathrm{Tors}(\Lambda_i)}_{=: \Lambda_i^*})$

By ① $\exists$ iso $\varphi : \Lambda_{1,\mathbb{Q}}^* \xrightarrow{\sim} \Lambda_{2,\mathbb{Q}}^*$

Λ_1^*, Λ_2^* are lattices in these $\mathbb{Q}$-vector spaces

$\Rightarrow \exists n \in \mathbb{N}$: $n \cdot \varphi(\Lambda_1^*) \subset \Lambda_2^*$

(this is why we had to pass from $\mathbb{R}$ to $\mathbb{Q}$!)

We get (since $n\varphi(\Lambda_1^*)$ is again a lattice)

$$0 \to \Lambda_1^* \xrightarrow{n \cdot \varphi} \Lambda_2^* \to \text{finite} \to 0$$

$\Rightarrow$ If $h(\Lambda_1^*)$ is defined, then so is $h(\Lambda_2^*)$

and $h(\Lambda_1^*) = h(\Lambda_2^*)$. □

4. The first inequality

L/K Galois extension of number fields w/ gp G

Motivation: The CFT axioms require

- $H^1(G, C_L) = 1$
- $H^2(G, C_L) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$

If G is cyclic, both axioms together give the Herbrand quotient $h(C_L) = [L:K]$. We verify this first:

Prop For L/K cyclic we have:

a) The Herbrand quotient of C_L is defined, and

$$h(C_L) = [L:K].$$

b) In particular:

$$\#H^2(G, C_L) = [C_K : N_{L/K}(C_L)] \geq [L:K]$$

$\| \; !!$

$h^2(G, C_L)$

("first inequality")

Pf. a) Pick a finite set $S \supset S_\infty$ of places of K s.th. the $\mathfrak{P}$ w/ $\mathfrak{P} \cap K = \mathfrak{p}$ generate Cl_K

$$\Rightarrow \quad C_L \simeq \mathbb{I}_{L,S} / \mathcal{O}^*_{K,S}$$

$$\Rightarrow \quad h(C_L) = h(\mathbb{I}_{L,S}) / h(\mathcal{O}^*_{K,S})$$

$$= \prod_{\mathfrak{p}\in S} [L_\mathfrak{p} : K_\mathfrak{p}] \cdot \frac{[L:K]}{\prod_{\mathfrak{p}\in S}[L_\mathfrak{p}:K_\mathfrak{p}]} = [L:K]$$

(previous sections)

b) Clear from a) and

$$h^2(-) = h^0(-) \geq \frac{h^0(-)}{h^1(-)} =: h(-). \qquad \square$$

Rem If we already knew $H^1(G, C_L) = 1$, then equality would follow in b). But we don't know a direct proof of $H^1(G, C_L) = 1$, so this has to wait until the next section!

The first inequality in particular implies

$$L = K \iff N_{L|K}(C_L) = C_K$$
$$\iff K^* \cdot N_{L|K}(\mathbb{I}_L) = \mathbb{I}_K$$

as predicted by CFT. In fact density suffices:

(i.e. Galois w/ $G = \mathrm{Gal}(L|K)$ solvable, for instance abelian)

<u>Cor</u> Let $L|K$ be a solvable extension.

If $K^* \cdot N_{L|K}(\mathbb{I}_L) \subset \mathbb{I}_K$ is dense, then $L = K$.

Pf. If $L \neq K$, then by solvability $\exists$ subfield $M \subset K$ with $K \subsetneq M$ and M/K cyclic. Then

$$N_{L|K}(\mathbb{I}_L) = N_{M|K}(N_{L|M}(\mathbb{I}_L)) \subset N_{M|K}(\mathbb{I}_M)$$

$\Rightarrow K^* \cdot N_{M|K}(\mathbb{I}_M) \subset \mathbb{I}_K$ dense subgp

$\Rightarrow$ wlog $L = M$ cyclic

But $N_{L|K}(\mathbb{I}_L) \subset \mathbb{I}_K$ is an open subgp

(it contains $N_{K|L}(\prod_{\mathfrak{P}} \mathcal{O}^*_{L_{\mathfrak{P}}}) = \prod_{\mathfrak{p}} \underbrace{N_{L_{\mathfrak{p}}|K_{\mathfrak{p}}}(\mathcal{O}^*_{L_{\mathfrak{p}}})}_{\text{this is open in } K^*_{\mathfrak{p}} \text{ and } = \mathcal{O}^*_{K_{\mathfrak{p}}} \text{ for } \mathfrak{p} \text{ unram. (see chapter on local CFT)}}$)

$\Rightarrow K^* \cdot N_{L|K}(\mathbb{I}_L) \subset \mathbb{I}_K$

union of translates of open subgp,

hence itself an open subgp,

hence in particular closed.

Thus $K^* \cdot N_{L|K}(\mathbb{I}_L) \subset \mathbb{I}_K$ is dense & closed,

hence equal to $\mathbb{I}_K$

$$\Rightarrow \underbrace{[\mathbb{I}_K : K^* \cdot N_{L|K}(\mathbb{I}_L)]}_{= [C_K : N_{L|K}(C_L)] \geq [L:K] \text{ by first inequality}} = 1$$

$\Rightarrow L = K$ $\square$

This gives a first result about splitting of primes and allows to control $\mathrm{Gal}(L/K)$ by Frobenii:

Prop Let L/K be solvable.

a) If $L \neq K$, then $\exists$ infinitely many primes in K that do not split completely in L/K.

b) Let T be any finite set of primes of L containing all those that ramify in L/K. Then $G := \mathrm{Gal}(L/K)$ is generated by the Frobenii

$$\mathrm{Frob}_{\mathfrak{P}} \in G_{\mathfrak{P}} \subset G \quad \text{for } \mathfrak{P} \nmid T.$$

Pf. a) Argue by contradiction:

Suppose $\exists$ finite set $S \supset S_\infty$ of places sth every prime $\mathfrak{p} \notin S$ splits completely in L/K.

Consider the subgp

$$\mathcal{D} := \{ a \in \mathbb{I}_K \mid \forall \mathfrak{p} \in S : a_{\mathfrak{p}} = 1 \} \subset \mathbb{I}_K.$$

For all $\mathfrak{p} \notin S$ and any $\mathfrak{P} \mid \mathfrak{p}$,

we have $L_{\mathfrak{P}} = K_{\mathfrak{p}}$ (since $\mathfrak{p}$ splits completely)

$$\Rightarrow \mathcal{D} \subset N_{L/K}(\mathbb{I}_L)$$

We claim $K^* \cdot \mathcal{D}$ is dense in $\mathbb{I}_K$

(hence $L = K$ by the previous corollary ↯):

Take any $c \in \mathbb{I}_K$.

Weak approximation: For any $\varepsilon > 0$ $\exists b \in K^*$ w/

$$|b - c_{\mathfrak{p}}|_{\mathfrak{p}} < \varepsilon \quad \text{for all } \mathfrak{p} \in S$$

Define $a \in \mathbb{I}_K$ by

$$a_{\mathfrak{p}} := \begin{cases} c_{\mathfrak{p}}/b, & \mathfrak{p} \notin S \\ 1, & \mathfrak{p} \in S \end{cases}$$

$$\Rightarrow a \in \mathcal{D} \text{ and } b \cdot a \in K^* \cdot \mathcal{D} \text{ has } |ba - c|_{\mathfrak{p}} < \varepsilon \text{ for } \underline{\text{all}} \ \mathfrak{p}$$

$$\Rightarrow K^* \cdot \mathcal{D} \subset \mathbb{I}_K \text{ dense}$$

b) Enlarge T

$\Rightarrow$ wlog T stable under the action of G

$\Rightarrow$ $H := \langle \mathrm{Frob}_\mathfrak{p} \mid \mathfrak{p} \notin T \rangle \trianglelefteq G$ normal subgp

Consider $M := L^H$

For $\mathfrak{p} \notin T$ we have

$$\mathrm{Frob}_{\mathfrak{p}\cap M} = (\mathrm{Frob}_\mathfrak{p})|_M = \mathrm{id}$$

$\mathfrak{p}$ unramified in L/K

$G_\mathfrak{p} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$

$(-)|_M \downarrow$ $\downarrow$

$G_{\mathfrak{p}\cap M} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}\cap M}/\mathbb{F}_p)$

$\mathrm{Frob}_\mathfrak{p} \in H$ and $M = L^H$

$\Rightarrow$ $\mathfrak{p} := \mathfrak{P} \cap K$ splits completely in M/K, $\forall\, \mathfrak{P} \notin T$

Upshot: Every prime $\mathfrak{p} \notin S := \{\mathfrak{P} \cap K : \mathfrak{P} \in T\}$ splits completely in M/K.

S finite $\Rightarrow$ $M = K$ by part (a) $\Rightarrow$ $H = G$ $\square$

5. The second inequality: Reduction to the basic case

Let L/K be Galois w/ gp $G = \mathrm{Gal}(L/K)$.

For L/K cyclic, $h^2(G, C_L) \geq [L:K]$ (1^{st} inequality)

Goal: For any L/K, $h^2(G, C_L)$ divides $[L:K]$.

In particular $h^2(G, C_L) \leq [L:K]$ (2^{nd} inequality)

Rem For L/K cyclic we have:

a) $h^2(G, C_L) = h^0_T(G, C_L) = [\text{Ш}_K : K^* \cdot N_{L/K}(\mathbb{I}_L^*)]$.

b) This number divides $[L:K]$ iff $h^1(G, C_L) = 1$.

Pf. a) $H^2(G, C_L) \simeq H^0_T(G, C_L) \simeq C_K / N(C_L) \simeq \text{Ш}_K / K^* \cdot N(\mathbb{I}_L)$

b) $h(G, C_L) = [L:K]$ by the previous section, so

$h^2(G, C_L) \mid [L:K] \iff h^2(G, L) = [L:K] \iff h^1(G, L) = 1$

$\square$

Our main goal is:

Thm ("second inequality")

For any finite Galois extension L/K w/ gp G, we have:

a) $h^2(G, C_K)$ divides $[L:K]$.

b) $h^1(G, C_K) = 1$. ← much harder than H90!

c) $h_T^0(G, C_K) = [\text{Ш}_K : K^* \cdot N_{L/K}(\text{Ш}_L)]$ divides $[L:K]$.

Rem CFT will ultimately show:

- $H_T^0(G, C_L) \simeq G^{ab}$
- $H^2(G, C_K)$ cyclic of order $[L:K]$

These two gps have the same order iff L/K is abelian.

They are isomorphic iff L/K is cyclic.

To prove the thm we reduce it to a "basic case" to be discussed in the next section.

Step 1. It suffices to prove the thm for G a p-gp. (p prime)

Pf. Let $H \subset G$ be a p-Sylow subgp.

$\Rightarrow$ $\text{res}^G_H : H_T^*(G, -)_{(p)} \xrightarrow{C} H_T^*(H, -)$

injective on p-parts

(as coresres = multiplicat^n by $[G:H]$)

So if the thm is true for L/L^H (instead of L/K), then

- $h^2(H, C_L) \mid [L:L^H]$ & $h_T^0(H, C_L) \mid [L:L^H]$

  $\Rightarrow$ $h^2(G, C_L)$ & $h_T^0(G, C_L)$ not divisible by a higher p-power than $[L:K]$
- $h^1(H, C_L) = 1$

  $\Rightarrow$ $h^1(G, C_L)$ not divisible by p

Since this works for all p, the claim follows. □

Step 2 It suffices to prove the thm for $G \simeq \mathbb{Z}/p\mathbb{Z}$. ($p$ prime)

Pf. Wlog G is a p-group (step 1)

$\Rightarrow \exists$ normal subgp $H \trianglelefteq G$ of index p

Assume the thm holds for $G/H \circlearrowright C_M$ w/ $M = L^H$

and also for $H \circlearrowright C_L$ by induction on $|G|$.

- $H^1(G, C_L) = 1$:

$$0 \to \underbrace{H^1(G/H, C_M)}_{=0 \text{ by assumption}} \xrightarrow{\inf} H^1(G, C_L) \xrightarrow{\text{res}} \underbrace{H^1(H, C_L)}_{=0 \text{ by induct}^n}$$

- $H^2(G, C_L)$ divides $[L:K]$:

From $H^1(G, C_L) = 0$ we have exactness of

$$0 \to \underbrace{H^2(G/H, C_M)}_{\#\text{ divides } [M:K] \text{ by assumption}} \xrightarrow{\inf} H^2(G, C_L) \xrightarrow{\text{res}} \underbrace{H^2(H, C_L)}_{\#\text{ divides } [L:M] \text{ by induction}}$$

- $h_T^0(G, C_L)$ divides $[L:K]$:

$\exists$ epi $N_{M/K} : C_M / N_{L/M}(C_L) \twoheadrightarrow N_{M/K}(C_M) / N_{L/K}(C_L)$

$\Rightarrow h_T^0(G, C_L) = [C_K : N_{L/K}(C_L)]$

$$= \underbrace{[C_K : N_{M/K}(C_M)]}_{\text{divides } [M:K] \text{ by assumption}} \cdot \underbrace{[N_{M/K}(C_M) : N_{L/K}(C_L)]}_{\text{divides } [C_M : N_{L/M}(C_L)] \text{ hence } [L:M] \text{ by ind}^n}$$

□

Step 3 It suffices to show that if

- L/K is cyclic of degree p (prime) and
- K contains $\zeta_p :=$ a primitive p^{th} root of 1, (will allow to apply Kummer theory...)

then

$$h_T^0(G, C_L) \text{ divides } [L:K] = p.$$

Pf. By step 2, it is enough to prove the theorem for L/K cyclic of degree p.

For L/K cyclic we have seen at the beginning of this section that a), b), c) in the thm are equivalent, so we only need to check property c):

$$h_T^0(G, L/K) \text{ divides } [L:K] = p.$$

Assume this holds whenever $\zeta_p \in K$.

To deduce it in general, pass to $\tilde{K} := K(\zeta_p)$, $\tilde{L} := L(\zeta_p)$

$\Rightarrow \tilde{L} = \tilde{K} \cdot L$ & $\tilde{K} \cap L = K$

($[L:K] = p$ coprime to $[\tilde{K}:K]$)

$\Rightarrow \tilde{G} := \mathrm{Gal}(\tilde{L}/\tilde{K}) \simeq G := \mathrm{Gal}(L/K)$,

ie $\tilde{L}/\tilde{K}$ is again cyclic of degree p

$\Rightarrow h_T^0(\tilde{G}, C_{\tilde{L}})$ divides p by assumption since $\zeta_p \in \tilde{K}$

So it suffices to show $h_T^0(G, C_L)$ divides $h_T^0(\tilde{G}, C_{\tilde{L}})$

In fact we claim the inclusion $C_L \xhookrightarrow{i} C_{\tilde{L}}$ induces an embedding $i_*: H_T^0(G, C_L) \hookrightarrow H_T^0(\tilde{G}, C_{\tilde{L}})$:

Both gps are p-torsion since $|G| = |\tilde{G}| = p$.

$\Rightarrow$ multiplicat^n by $p-1$ invertible on them

$\Rightarrow$ multiplicat^n by $d := [K':K]$ — as $d \mid (p-1)$

$\Rightarrow \forall\, x \in C_K\ \exists\, y \in C_K: [x] = [y^d]$ in $H_T^0(G, C_L)$.

If $[x] \in \ker(i_*)$, then

$[i(y)]^d = 1$ in $H_T^0(\tilde{G}, C_{\tilde{L}})$

$\Rightarrow [i(y)] = 1$ since d is invertible

$\Rightarrow \exists\, \tilde{z} \in C_{\tilde{L}}: i(y) = N_{\tilde{L}/\tilde{K}}(\tilde{z})$ $\quad z := N_{\tilde{L}/L}(\tilde{z})$

$\Rightarrow y^d = N_{\tilde{K}/K}(y) = N_{\tilde{L}/K}(\tilde{z}) = N_{L/K}(z)$

$\Rightarrow [x] = 1$ in $H_T^0(G, C_L)$. $\square$

6. The second inequality: Pf in the basic case

Setup: L/K cyclic of order p

& $K \ni \zeta_p :=$ a primitive p-th root of 1

By Kummer theory (using $\zeta_p \in K$),

$\exists\, a \in K: \quad L = K(\sqrt[p]{a})$

[Pick a generator σ of $G = Gal(L/K)$

$\Rightarrow H^\bullet(G, L^*) = H^\bullet\left(L^* \xrightarrow{\sigma-1} L^* \xrightarrow{N} L^* \xrightarrow{\sigma-1} \dots\right)$

w/ $N: L^* \to L^*,\ a \mapsto \prod_{i=0}^{p-1} \sigma^i(a)$.

$\Rightarrow \ker(N) = \mathrm{im}(\sigma-1)$ by Hilbert 90

But $N(\zeta_p) \underset{\zeta_p \in K}{=} \zeta_p^p = 1 \Rightarrow \exists\, b \in L^*: \zeta_p = \frac{\sigma(b)}{b}$

$\Rightarrow a := b^p \in (L^*)^G = K^*$ but $b \notin K^*$

$\Rightarrow L = K(b) = K(\sqrt[p]{a})$ for degree reasons.]

Now fix a finite set $S \supset S_\infty$ of places of K sth

a) $a \in \mathcal{O}_{K,S}^*$

b) $S \supset \{$primes above $p\}$

c) $\mathbb{I}_K = \mathbb{I}_{K,S} \cdot K^*$

Rem Conditions a), b) imply

$S \supset \{$primes ramified in $L/K\}$

since $\mathrm{discr}(L/K) = \pm p^p \cdot a^{p-1}$ (exercise).

We have $L \subset M := K(\sqrt[p]{x} \mid x \in \mathcal{O}_{K,S}^*)$.
This subfield can be described by giving the subgp $Gal(M/L) \subset Gal(M/K)$:

Lemma $\exists$ finite set T of places of K w/ $S \cap T = \emptyset$ sth $Gal(M/L)$ is an $\mathbb{F}_p$-vector space with basis given by the Frobenii $Frob_\varphi$ $(\varphi \in T)$.

Pf. By Kummer theory

$$\mathrm{Gal}(M/K) \xrightarrow{\sim} \mathrm{Hom}\left(\mathcal{O}_{K,S}^* / (\mathcal{O}_{K,S}^*)^p,\ \mathbb{Z}/p\mathbb{Z}\right)$$

$$\tau \longmapsto \left([a] \longmapsto i \bmod p \text{ w/ } \frac{\tau(\sqrt[n]{a})}{\sqrt[n]{a}} = \zeta_p^i\right)$$

$\Rightarrow$ $\mathrm{Gal}(M/K)$ is an $\mathbb{F}_p$-vector space,

so $\mathrm{Gal}(M/L)$ is an $\mathbb{F}_p$-vector subspace.

Any place $\mathcal{Q}$ of M with $\wp := \mathcal{Q} \cap K \notin S$

is unramified by the previous remark about S,

hence $G_{\mathcal{Q}} = \mathrm{Gal}(M_{\mathcal{Q}}/K_\wp)$ is cyclic

(being $\simeq \mathrm{Gal}(\mathbb{F}_{\mathcal{Q}}/\mathbb{F}_\wp)$ by unramifiedness).

But it is also killed by p (being $\subset \mathrm{Gal}(M/K)$)

$\Rightarrow$ For $\mathfrak{P} := \mathcal{Q} \cap L$

- either $K_\wp = L_\mathfrak{P} \xhookrightarrow{\mathbb{Z}/p} M_{\mathcal{Q}}$
- or $K_\wp \xhookrightarrow{\mathbb{Z}/p} L_\mathfrak{P} = M_{\mathcal{Q}}$

(*)

As we saw as an application of the 1st inequality,

$\exists$ finite set T_L of places of L sth the Frobenii

$\mathrm{Frob}_\mathfrak{P}$ w/ $\mathfrak{P} \in T_L$ generate $\mathrm{Gal}(M/L)$.

Shrinking T_L we may assume they form a basis

as an $\mathbb{F}_p$-vector space.

Let $T := \{ \mathfrak{P} \cap K \mid \mathfrak{P} \in T_L \}$.

For $\mathfrak{P} \in T_L$ above $\wp := \mathfrak{P} \cap K \in T$

we have:

$\mathrm{Frob}_\mathfrak{P} \neq \mathrm{id}$ in $\mathrm{Gal}(M/L)$ by def of a basis

$\Rightarrow M_{\mathcal{Q}} \neq L_\mathfrak{P}$ for $\mathcal{Q} \mid \mathfrak{P}$

$\Rightarrow L_\mathfrak{P} = K_\wp$ by (*)

$\Rightarrow$ $\mathrm{Frob}_\mathfrak{P} = \mathrm{Frob}_\wp$

$\in \mathrm{Gal}(M/L) \subset \mathrm{Gal}(M/K)$

□

Cor $L = K(\sqrt[p]{\Delta})$ for

$$\Delta := \ker\left(\mathcal{O}_{K,S}^* \xrightarrow{\varphi} \prod_{\mathfrak{p}\in T} \mathcal{O}_{K_\mathfrak{p}}^* / (\mathcal{O}_{K_\mathfrak{p}}^*)^p\right).$$

Pf. We need to show $\mathcal{O}_{K,S}^* \cap (L^*)^p = \Delta$.

"$\subset$" If $a \in \mathcal{O}_{K,S}^* \cap (L^*)^p$

then $a \in (L_\mathfrak{P}^*)^p$ for all $\mathfrak{P} \mid \mathfrak{p} \in T$

But $L_\mathfrak{P} = K_\mathfrak{p}$ $\forall\, \mathfrak{P} \mid \mathfrak{p} \in T \Rightarrow a \in (\mathcal{O}_{K_\mathfrak{p}}^*)^p$

"$\supset$" If $a \in \Delta = \ker(\varphi)$,

then $\sqrt[p]{a} \in K_\mathfrak{p}^*$ for all $\mathfrak{P} \mid \mathfrak{p} \in T$

$\Rightarrow \sqrt[p]{a}$ is fixed by $\mathrm{Frob}_\mathfrak{p}$ for all $\mathfrak{p} \in T$

$\Rightarrow \sqrt[p]{a}$ is fixed by $\mathrm{Gal}(M/L)$

$\Rightarrow \sqrt[p]{a} \in L$, ie $a \in (L^*)^p$ $\square$

Upshot An element of $\mathcal{O}_{K,S}^*$ is a p-th power in L

iff it is a p-th power in $K_\mathfrak{p}$ for all $\mathfrak{p} \in T$

Rem The above map φ is surjective:

$$\varphi : \mathcal{O}_{K,S}^* \twoheadrightarrow \prod_{\mathfrak{p}\in T} \mathcal{O}_{K_\mathfrak{p}}^* / (\mathcal{O}_{K_\mathfrak{p}}^*)^p$$

Pf. It suffices to show

$$[\mathcal{O}_{K,S}^* : \Delta] = \prod_{\mathfrak{p}\in T} [\mathcal{O}_{K_\mathfrak{p}}^* : (\mathcal{O}_{K_\mathfrak{p}}^*)^p].$$

RHS: $\mathcal{O}_{K_\mathfrak{p}}^* \simeq \mu(K_\mathfrak{p}) \times \mathbb{Z}_\ell^r$ w/ $\ell = \mathrm{char}(\mathbb{F}_\mathfrak{p})$, $r = [K_\mathfrak{p} : \mathbb{Q}_\ell]$

For $\mathfrak{p} \in T$ we have $\ell \neq p$ since $T \cap S = \emptyset$

$\Rightarrow p : \mathbb{Z}_\ell \xrightarrow{\simeq} \mathbb{Z}_\ell$ iso

$\Rightarrow [\mathcal{O}_{K_\mathfrak{p}}^* : (\mathcal{O}_{K_\mathfrak{p}}^*)^p] = [\mu(K_\mathfrak{p}) : (\mu(K_\mathfrak{p}))^p] = p$ ($\zeta_p \in K$)

LHS: Kummer theory:

$$\begin{array}{ccc} \mathrm{Hom}(\mathcal{O}_{K,S}^*/\Delta, \mathbb{Z}/p) & \xrightarrow{\simeq} & \mathrm{Gal}(M/L) \\ \cap & & \cap \\ \mathrm{Hom}(\mathcal{O}_{K,S}^*/(\mathcal{O}_{K,S}^*)^p, \mathbb{Z}/p) & \xrightarrow{\simeq} & \mathrm{Gal}(M/K) \end{array}$$

$\Rightarrow [\mathcal{O}_{K,S}^* : \Delta] = \#\,\mathrm{Gal}(M/L) = p^{\#T}$ $\square$

Having L/K understood well enough, we want to show the 2nd inequality: $[C_K : N_{L/K}(C_L)]$ divides p.

For this we'll construct a subgp $W = W_{S,T} \subset \mathbb{I}_K$ whose image $\bar{W} := K^* W / K^* \subset C_K$ satisfies

a) $\bar{W} \subset N_{L/K}(C_L)$, ← ie W not too large

b) $[C_K : \bar{W}]$ divides p ← ie W not too small

For any finite $\Sigma \supset S$:

$$\mathbb{I}_K = K^* \cdot \mathbb{I}_{K,\Sigma} \quad \text{and} \quad C_K = \mathbb{I}_{K,\Sigma} / \mathcal{O}^*_{K,\Sigma}$$

w/ $$\mathbb{I}_{K,\Sigma} := \prod_{\mathfrak{p} \in \Sigma} K^*_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin \Sigma} \mathcal{O}^*_{K_{\mathfrak{p}}}.$$

Take $\Sigma := S \cup T$ for T as above and

$$W_{S,T} := \prod_{\mathfrak{p} \in S} (K^*_{\mathfrak{p}})^p \times \prod_{\mathfrak{p} \in T} K^*_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin \Sigma} \mathcal{O}^*_{K_{\mathfrak{p}}} \subset \mathbb{I}_{K, S \cup T}.$$

Lemma a) $W_{S,T} \subset N_{L/K}(\mathbb{I}_L)$,

b) $K^* \cap W_{S,T} = (\mathcal{O}^*_{K,S \cup T})^p$.

Pf. a) Let $\mathfrak{P}$ be a place of L and $\mathfrak{p} = \mathfrak{P} \cap K$.

- For $\mathfrak{p} \in S$ we have $(K^*_{\mathfrak{p}})^p \subset N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(L^*_{\mathfrak{P}})$ since by local CFT

$$K^*_{\mathfrak{p}} / N(L^*_{\mathfrak{P}}) \xrightarrow{\sim} \underbrace{\mathrm{Gal}(L^*_{\mathfrak{P}}/K^*_{\mathfrak{p}})}_{\text{killed by } p}$$

- For $\mathfrak{p} \in T$ we have $L_{\mathfrak{P}} = K_{\mathfrak{p}}$ (see the pf of the Lemma introducing the set T).

- For $\mathfrak{p} \notin S \cup T$ we have $N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(\mathcal{O}^*_{L_{\mathfrak{P}}}) = \mathcal{O}^*_{K_{\mathfrak{p}}}$ by local CFT since here $\mathfrak{P}/\mathfrak{p}$ is unramified.

$\Rightarrow W_{S,T} \subset N_{L/K}(\mathbb{I}_L)$.

b) $(\mathcal{O}^*_{K,SUT})^p \subset K^* \cap W_{S,T}$ trivially.

For "$\supset$" pick any $a \in K^* \cap W_{S,T}$

Let $M := K(\sqrt[p]{a})$. We must show $M = K$.

($\Rightarrow$ a is a p-th power in K

hence $a \in (\mathcal{O}^*_{K,SUT})^p$)

To show $M = K$, it suffices to find a subgp

$D \subset \mathbb{I}_K$ sth

b1) $D \subset N_{M/K}(\mathbb{I}_M)$, and

b2) $K^* \cdot D = \mathbb{I}_K$

(dense subgp would suffice, see 1st inequality)

We'll show these properties for

$$D := \prod_{p \in S} K_p^* \times \prod_{p \in T} (\mathcal{O}^*_{K_p})^p \times \prod_{p \notin SUT} \mathcal{O}^*_{K_p} :$$

b1) is similar to a):

- Over $p \in S$: $M_p = K_p$

  since $a \in (K_p^*)^p$ by def of $W_{S,T}$

- Over $p \in T$: $(\mathcal{O}^*_{K_p})^p \subset N(\mathcal{O}^*_{L_p})$

  since local CFT says

  $K_p^* / N(L_p^*) \simeq \underbrace{Gal(L_p | K_p)}_{\text{killed by } p}$

  (Kummer theory)

- Over $p \notin SUT$: $\mathcal{O}^*_{K_p} = N(\mathcal{O}^*_{L_p})$ by unramified local CFT

b2) We know surjectivity of

$$\varphi: \mathcal{O}^*_{K,S} \twoheadrightarrow \prod_{p \in T} \mathcal{O}^*_{K_p} / (\mathcal{O}^*_{K_p})^p = \mathbb{I}_{K,S} / D$$

$\Rightarrow \mathbb{I}_{K,S} = \mathcal{O}^*_{K,S} \cdot D$

$\Rightarrow \mathbb{I}_K = K^* \cdot \mathbb{I}_{K,S} = K^* \cdot D$ $\square$

Recall the exact sequence

$$1 \to \mathcal{O}^*_{K,S\cup T} \to \mathbb{I}_{K,S\cup T} \to C_K \to 1.$$

For $\bar{W}_{S,T} := K^* W_{S,T} / K^* \subset C_K$ this gives an exact sequence

$$1 \to \frac{\mathcal{O}^*_{K,S\cup T}}{K^* \cap W_{S,T}} \to \frac{\mathbb{I}_{K,S\cup T}}{W_{S,T}} \to \frac{C_K}{\bar{W}_{S,T}} \to 1$$

Prop Put $s := \#S$. Then

a) $[\mathcal{O}^*_{K,S\cup T} : K^* \cap W_{S,T}] = p^{2s-1}$

b) $[\mathbb{I}_{K,S\cup T} : W_{S,T}] = p^{2s}$

Hence $[C_K : \bar{W}_{S,T}] = p$,

and thus the 2nd inequality holds.

Pf. a) The previous lemma, part b), shows

$$[\mathcal{O}^*_{K,S\cup T} : K^* \cap W_{S,T}] = [\mathcal{O}^*_{K,S\cup T} : (\mathcal{O}^*_{K,S\cup T})^p].$$

The RHS can be computed via Dirichlet's unit thm:

For any finite set $\Sigma \supset S_\infty$ of places,

$$\mathcal{O}^*_{K,\Sigma} \simeq \mu(K) \times \mathbb{Z}^{n-1} \quad \text{with } n = \#\Sigma.$$

If $\zeta_p \in K$, then $[\mu(K) : (\mu(K))^p] = p$

$$\Rightarrow [\mathcal{O}^*_{K,\Sigma} : (\mathcal{O}^*_{K,\Sigma})^p] = p \cdot p^{n-1} = p^n.$$

In our case take $\Sigma = S \cup T$

$$\Rightarrow n = s + t \quad \text{w/} \quad \begin{matrix} s := \#S \\ t := \#T \end{matrix}$$

$\Rightarrow$ Only need to show $t = s - 1$

This follows from Kummer theory:

For $M := K(\sqrt[p]{O_{K,S}^*})$, we had

$$\left.\begin{aligned} [M:L] &= p^t \quad \text{by choice of } T \\ [M:K] &= [O_{K,S}^* : (O_{K,S}^*)^p] = p^s \end{aligned}\right\} \Rightarrow t = s-1$$

since $[L:K] = p$

$[M:K] = [O_{K,S}^* : (O_{K,S}^*)^p]$: Kummer theory

$= p^s$: Dirichlet's unit thm

b) $[\mathbb{I}_{K,S\cup T} : W_{S,T}] = \prod_{\mathfrak{p}\in S} [K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^p]$

by def of $W_{S,T}$

Exercise: For any $n \in \mathbb{N}$,

$$[K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^n] = \frac{n}{|n|_\mathfrak{p}} \cdot \#\mu_n(K_\mathfrak{p}).$$

Take $n = p$ & $\zeta_p \in K$: $[K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^p] = \frac{p^2}{|p|_\mathfrak{p}}$.

$$\Rightarrow \prod_{\mathfrak{p}\in S} [K_\mathfrak{p}^* : (K_\mathfrak{p}^*)^p] = p^{2s}$$

by the product formula. □

Upshot For any Galois extension $L|K$ of number fields & $G = \mathrm{Gal}(L|K)$,

a) $h^2(G, C_L)$, $h_T^0(G, C_L)$ both divide $[L:K]$,

b) $h^1(G, C_L) = 1$.

From part b we recover two famous results:

Cor 1 (Hasse norm thm) For $L|K$ a cyclic extension of # fields and $a \in K^*$ TFAE:

a) $a \in N_{L|K}(L^*)$

b) $a \in N_{L_\mathfrak{P}|K_\mathfrak{p}}(L_\mathfrak{P}^*)$

for all places $\mathfrak{p}$ of K and all $\mathfrak{P}|\mathfrak{p}$ (including the ∞ places)

Pf. By the 2nd inequality $H^1(G, C_L) = 1$.

G cyclic $\Rightarrow$ $H^{-1}(G, C_L) \simeq H^1(G, C_L) = 1$

From $1 \to L^* \to \mathbb{I}_L \to C_L \to 1$ we get

$$\cdots \to \underset{\parallel}{H_T^{-1}(G, C_L)} \to \underset{\parallel}{H_T^0(G, L^*)} \to \underset{\parallel}{H_T^0(G, \mathbb{I}_L)} \to \cdots$$

$$1 \qquad K^*/N(L^*) \qquad \mathbb{I}_K/N(\mathbb{I}_L)$$

$$\cap$$

$$\prod_{\wp} K_{\mathfrak{p}}^*/N(L_{\mathfrak{P}}^*)$$

($\mathfrak{P}$ any above $\wp$) $\square$

Rem • Any $a \in K^*$ is $\in N(L_{\mathfrak{P}}^*)$ for all but finitely many places $\wp$

• The Hasse norm thm usually fails for L/K not cyclic: For $L = \mathbb{Q}[\sqrt{13}, \sqrt{17}]$ / $K = \mathbb{Q}$, $a = 25$ is a local norm at every place but not a global norm (Serre-Tate).

Cor 2 (Albert–Brauer–Hasse–Noether thm)

For any number field K the map

$$Br(K) \hookrightarrow \bigoplus_{\wp} Br(K_\wp)$$

is injective.

Pf. For L/K finite have $1 \to L^* \to \mathbb{I}_L \to C_L \to 1$

For $G := Gal(L/K)$ then

$$\underbrace{H^1(G, C_L)}_{=1 \text{ (by 2nd ineq)}} \to \underbrace{H^2(G, L^*)}_{= Br(L/K)} \longrightarrow \underbrace{H^2(G, \mathbb{I}_L)}_{= \bigoplus_{\wp} H^2(G_\wp, \mathbb{I}_{L_\wp}) = \bigoplus_{\wp} Br(L_\wp/K_\wp)}$$

(any $\wp | \wp$)

Now use

$$Br(K) = \bigcup_{\substack{L/K \\ \text{finite}}} Br(L/K) \quad \& \text{ ditto for } Br(K_\wp).$$

□

7. The main thm of global CFT

L/K abelian extension of # fields

$G = Gal(L/K)$

Goal $\exists$ epi $(-, L/K): C_K \twoheadrightarrow G$

inducing an iso

$$Art_{L/K}: C_K / N_{L/K}(C_L) \xrightarrow{\sim} G$$

By the previous section we know

a) $h^1(G, C_L) = 1$,

b) $h^2(G, C_L)$ divides $[L:K]$.

The axioms of abstract CFT would need more in b):

$\exists$ inv: $H^2(G, C_L) \xrightarrow{\sim} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$

compatible w/ restriction in towers $M \supset L \supset K$?

We instead take a shortcut, putting together the local norm residue symbols from local CFT to define a global norm residue symbol directly:

Def For any place $\wp$ of K consider the local norm residue symbol

$$(-, L_\wp / K_\wp) : K_\wp^* \longrightarrow G_\wp \subset G$$

This only depends on $\wp$, not on $\mathfrak{P} | \wp$, since L/K is abelian. For infinite places we here put

$$(-, \mathbb{C}/\mathbb{R}) : \mathbb{R}^* \longrightarrow \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\pm 1\}$$
$$a \longmapsto \mathrm{sgn}(a)$$

(and $(-, L_\wp / K_\wp) := 1$ for $L_\wp = K_\wp$)

Def For $a = (a_\wp)_\wp \in \mathbb{I}_K$ define

$$(a, L/K) := \prod_\wp \underbrace{(a_\wp, L_\wp / K_\wp)}_{\in G_\wp \subset G} \in G$$

Note that this is well-defined:

$a_\wp \in \mathcal{O}_{K_\wp}^*$ for all but fin. many $\wp$,

$\Rightarrow (a_\wp, L_\wp / K_\wp) = 1$ ⟂

since $\mathcal{O}_{K_\wp}^* = N(\mathcal{O}_{L_\wp}^*)$ for $\mathfrak{P} | \wp$ unram.

We get a gp hom.

$$(-, L/K) : \mathbb{I}_K \longrightarrow G.$$

We'll show it factors over $C_K = \mathbb{I}_K / K^*$.

This will prove the main thm:

- $(-, L/K) : \mathbb{I}_K \twoheadrightarrow G$ surjective:

  Indeed G is generated by Frobenii Frob_φ at unramified primes $\mathfrak{P}|\varphi$ as we have seen as a corollary of the 1st inequality, and $\mathrm{Frob}_\varphi = (\pi_\varphi, L_\mathfrak{P}/K_\varphi) = (a, L/K)$

  w/ $a := (\ldots 1, 1, \underset{\text{at } \varphi}{\pi_\varphi}, 1, 1, \ldots) \in \mathbb{I}_K$

- $N_{L/K}(L^*) \subset \ker(-, L/K)$

  since this holds locally at every φ

- IF $K^* \subset \ker(-, L/K)$, then we get an induced epi

  $$(-, L/K) : C_K / N_{L/K}(C_L) \twoheadrightarrow G,$$

  which must be an iso by the 2nd inequality.

Why should $K^* \subset \ker(-, L/K)$ hold?

Ex Let $L = \mathbb{Q}(\zeta_m) \,/\, K = \mathbb{Q}$.

Since $\mathrm{Gal}(L/K) \simeq \prod_{\substack{\ell^\nu \| m \\ \ell \text{ prime}}} \mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^\nu})/\mathbb{Q})$

and

$$(a, L/K)\big|_{\mathbb{Q}(\zeta_{\ell^\nu})} = (a, \mathbb{Q}(\zeta_{\ell^\nu})/\mathbb{Q})$$

for any $a \in \mathbb{Q}^*$, it suffices to show

$(a, \mathbb{Q}(\zeta_{\ell^\nu})/\mathbb{Q}) = 1$ for all primes ℓ

$\Rightarrow$ Wlog $m = \ell^\nu > 2$ a prime power

Compute $(a, L/K)_\varphi$ for each place φ:

- At $\varphi = \infty$ we have $L_\varphi = \mathbb{C} \,/\, K_\varphi = \mathbb{R}$, giving $(a, \mathbb{C}/\mathbb{R}) = \mathrm{sgn}(a)$

  $\in \{\pm 1\} \subset (\mathbb{Z}/\ell^\nu\mathbb{Z})^* \simeq \mathrm{Gal}(L/K)$

- At a prime $p \neq \ell$ the extension L/K is unramified. For $a = v \cdot p^s$ w/ $p \nmid v$ then

$$(a, L_{\mathfrak{P}}/\mathbb{Q}_p) = [p^s] \in (\mathbb{Z}/\ell^v\mathbb{Z})^*$$

$$\downarrow \qquad \downarrow \wr$$

$$(\mathrm{Frob}_p)^r = (\zeta \mapsto \zeta^{p^s}) \in \mathrm{Gal}(L/K)$$

w/ $\zeta := \zeta_{\ell^v}$ a primitive ℓ^v-th root of 1.

- At the prime $p = \ell$ the extension L/K is totally ramified. For $a = u \cdot \ell^r$ w/ $\ell \nmid u$ then by Lubin-Tate theory

$$(a, L_{\mathfrak{P}}/\mathbb{Q}_p) = [u^{-1}] \in (\mathbb{Z}/\ell^v\mathbb{Z})^*$$

$$\downarrow \qquad \downarrow \wr$$

$$\sigma_u = (\zeta \mapsto \zeta^{u^{-1}}) \in \mathrm{Gal}(L/K)$$

for the inverse $u^{-1} \in (\mathbb{Z}/\ell^v\mathbb{Z})^*$.

Putting everything together we obtain for $a = \ell^r \cdot u$ w/ $\ell \nmid u$ the values:

- $(a, \mathbb{C}/\mathbb{R}) = \mathrm{sgn}(u)$,
- $(a, L_{\mathfrak{P}}/\mathbb{Q}_p) = p^{v_p(u)}$ at all $p \neq \ell$,
- $(a, L_{\mathfrak{P}}/\mathbb{Q}_p) = u^{-1}$ at $p = \ell$.

Thus

$$\begin{aligned}(a, L/\mathbb{Q}) &:= \prod_{\mathfrak{P}} (a, L_{\mathfrak{P}}/\mathbb{Q}_p) \\ &= \mathrm{sgn}(u) \cdot \prod_{p \neq \ell} p^{v_p(u)} \cdot u^{-1} \\ &= \mathrm{sgn}(u) \cdot |u| \cdot u^{-1} \\ &= 1 \quad \text{as claimed.}\end{aligned}$$

For arbitrary $L|K$ we'll show $K^* \subset \ker(-, L/K)$ together w/ a similar claim for $H^2(G, L^*)$ in place of $H^0(G, L^*) = K^*$:

Thm a) For any $a \in K^*$ we have

$$(a, L/K) := \prod_{\mathfrak{p}} (a, L_{\mathfrak{P}}/K_{\mathfrak{p}}) = 1.$$

b) For any $b \in H^2(G, L^*)$ we have

$$\sum_{\mathfrak{p}} \mathrm{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(b) = 0 \quad \text{in } \mathbb{Q}/\mathbb{Z}.$$

Here we use the invariant map from local CFT:

$$\mathrm{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} : H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*) \to \mathbb{Q}/\mathbb{Z}$$

$$H^2(G, L^*)$$

For $\mathfrak{p} \mid \infty$ we put $\mathrm{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} : H^2(G_{\mathfrak{P}}, L_{\mathfrak{P}}^*) \hookrightarrow \frac{1}{2}\mathbb{Z}/\mathbb{Z}$.

the unique embedding

Rem • Part a) says that $\prod_{\mathfrak{p}} (-, L_{\mathfrak{P}}/K_{\mathfrak{p}})$ factors over $C_K = \mathbb{I}_K / K^*$.

• In contrast, part b) only shows that $\sum_{\mathfrak{p}} \mathrm{inv}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ factors over the image of $H^2(G, \mathbb{I}_L) \xrightarrow{\alpha} H^2(G, C_L)$.

The map α is not necessary surjective since $H^3(G, L^*)$ may be $\neq 0$, so to define $\mathrm{inv} : H^2(G, C_L) \to \mathbb{Q}/\mathbb{Z}$ we would need more work. This is why we don't use axiomatic CFT in the global setup (though one could).

Pf of the thm.

① If a) holds for $L|K$, then also for

- $M|K$ any subextension of $L|K$,
- $L' = LK'/K'$ composite w/ any K'/K.

Indeed:

- The diagram

$$\begin{array}{ccc} \mathbb{I}_K & \xrightarrow{(-,L|K)} & \mathrm{Gal}(L|K) \\ & \searrow^{(-,M|K)} & \downarrow \mathrm{res} \\ & & \mathrm{Gal}(M|K) \end{array}$$

commutes, since the local norm residue symbols are compatible in towers.

- For any place $\mathfrak{p}'$ of K' and any $\mathfrak{P}'|\mathfrak{p}'$ we have a commutative diagram

$$\begin{array}{ccc} K'^*_{\mathfrak{p}'} & \xrightarrow{(-,L'_{\mathfrak{P}'}|K'_{\mathfrak{p}'})} & \mathrm{Gal}(L'_{\mathfrak{P}'}|K'_{\mathfrak{p}'}) \\ \downarrow N & & \downarrow \\ K^*_{\mathfrak{p}} & \xrightarrow{(-,L_{\mathfrak{p}}|K_{\mathfrak{p}})} & \mathrm{Gal}(L_{\mathfrak{p}}|K_{\mathfrak{p}}) \end{array}$$

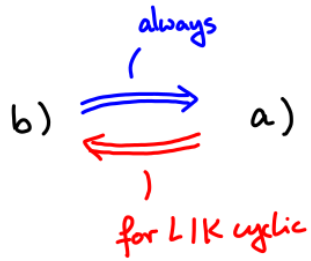
where $\mathfrak{P} := \mathfrak{P}' \cap L$, $\mathfrak{p} := \mathfrak{p}' \cap K$.

Hence we get

$$\begin{array}{ccccc} K'^* & \subset & \mathbb{I}_{K'} & \xrightarrow{(-,L'|K')} & \mathrm{Gal}(L'|K') \\ \downarrow & & \downarrow N & & \downarrow \\ K^* & \subset & \mathbb{I}_K & \xrightarrow{(-,L|K)} & \mathrm{Gal}(L|K) \end{array}$$

and the claim follows.

② We have



Indeed: Put $G = \mathrm{Gal}(L|K)$.

For any $\chi \in \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ we have a comm. diagram

$$\begin{array}{ccccc} K^* & \longrightarrow & \mathbb{I}_K & \xrightarrow{(-,L|K)} & G \\ \downarrow \cup \delta\chi & & \downarrow \cup \delta\chi & & \downarrow \chi \\ H^2(G, L^*) & \longrightarrow & H^2(G, \mathbb{I}_L) & \longrightarrow & \mathbb{Q}/\mathbb{Z} \\ & & & \nwarrow^{\sum_{\mathfrak{p}} \mathrm{inv}_{L_{\mathfrak{p}}|K_{\mathfrak{p}}}} & \end{array}$$

where

$$\begin{array}{ccc} \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) & \xrightarrow{\delta} & H^2(G, \mathbb{Z}) \\ \cup & & \cup \\ \chi & \longmapsto & \delta\chi \end{array}$$

Here the second square commutes since it does so locally at each place by construction of the local norm residue symbol via abstract CFT (see the lemma in section II.5).

By the diagram clearly b) $\Rightarrow$ a), since χ can be chosen arbitrarily (recall for $g \in G$ that $g = 1 \Leftrightarrow \forall \chi : \chi(g) = 0$)

If $L|K$ is cyclic, then we can pick χ sth $H^2(G, \mathbb{Z}) \simeq \mathbb{Z}/_{|G|\mathbb{Z}}$ is generated by $\delta\chi$, and then (iso (exercise))

$$(-) \cup \delta\chi : H^0_T(G, L^*) \xrightarrow{\sim} H^2(G, L^*)$$

Then $K^* \xrightarrow{\cup \delta\chi} H^2(G, L^*)$ is surjective, so the diagram shows also a) $\Rightarrow$ b).

③ We can now prove the thm as follows:

a) holds for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ by earlier example

$\Rightarrow$ a) for any cyclotomic L/K by ①

(we call L/K cyclotomic if $\exists n: L \subset K(\zeta_n)$)

$\Rightarrow$ b) for any cyclic cyclotomic L/K by ②

(because for cyclic extensions a) $\Rightarrow$ b))

We'll see below that

$$H^2(\mathrm{Gal}(\bar{K}/K), \bar{K}^*) = \bigcup_{L/K} H^2(G(L/K), L^*)$$

$$= \bigcup_{\substack{L/K \\ \text{cyclic cyclotomic}}} H^2(G(L/K), L^*)$$

Since

$$\begin{array}{ccc} H^2(\mathrm{Gal}(L/K), L^*) & \xrightarrow{\sum_{\mathfrak{p}} \mathrm{inv}_{L_{\mathfrak{p}}/K_{\mathfrak{p}}}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow & \nearrow_{\exists} & \\ H^2(\mathrm{Gal}(\bar{K}/K), \bar{K}^*) & & \end{array}$$

by the compatibility of the local invariant map in towers, we get:

b) for all cyclic cyclotomic L/K

$\Rightarrow$ b) for all finite L/K

$\Rightarrow$ a) for all finite L/K

(since always b) $\Rightarrow$ a) by ②). $\square$

8. More about Brauer gps & the invariant map

Let K be a number field.

Put $G_K := \mathrm{Gal}(\bar{K}/K)$,

$G_{L/K} := \mathrm{Gal}(L/K)$ for L/K Galois.

We are interested in

$\mathrm{Br}(L/K) = H^2(G_{L/K}, L^*)$ inside

$$\mathrm{Br}(K) = \varinjlim_{L/K \text{ finite}} \mathrm{Br}(L/K)$$

$$= \bigcup_{L/K \text{ finite}} \mathrm{Br}(L/K) \quad \text{(using H90)}$$

$$\overset{?}{=} \bigcup_{L/K \text{ cyclic cyclotomic}} \mathrm{Br}(L/K)$$

We'll prove a stronger statement also for

$$\mathbb{B}\mathrm{r}(L/K) := H^2(G_{L/K}, \mathbb{I}_L)$$

$$= \bigoplus_{\mathfrak{p}} \mathrm{Br}(L_{\mathfrak{P}}/K_{\mathfrak{p}})$$

($\mathfrak{P}$ any $\mathfrak{P}|\mathfrak{p}$)

inside $\mathbb{B}\mathrm{r}(K) := \bigcup_{L/K \text{ finite}} \mathbb{B}\mathrm{r}(L/K)$:

Thm a) $\mathbb{B}\mathrm{r}(K) = \bigcup_{L/K \text{ cyc cyc}} \mathbb{B}\mathrm{r}(L/K)$

b) $\mathbb{B}\mathrm{r}(K) = \bigcup_{L/K \text{ cyc cyc}} \mathbb{B}\mathrm{r}(L/K)$

w/ union only over cyclic cyclotomic L/K.

Slogan. Cyclic cyclotomic extensions are to global CFT what unramified extensions are to local CFT.

Pf. $\mathbb{B}r(K) \hookrightarrow \mathbb{B}r(K)$

& $\mathbb{B}r(L|K) \hookrightarrow \mathbb{B}r(L|K)$ injective

(Albert-Brauer-Hasse-Noether, § IV.6)

$\Rightarrow$ only need to prove part b).

For this let $c \in \mathbb{B}r(K)$.

Pick $L'|K$ finite with $c \in \mathbb{B}r(L'|K)$.

Let $m \in \mathbb{N}$ w/ $c^m = 1$ (e.g. $m = \#G_{L'|K}$)

Consider the finite set

$S := \{$ places φ of $K \mid c_\varphi \neq 1$ in $\mathbb{B}r(L_\varphi|K_\varphi)\}$

Claim $\exists$ cyclic cyclotomic $L|K$ sth

- $[L_\varphi : K_\varphi] \in m\mathbb{Z}$ for all $\varphi \in S \setminus S_\infty$,
- $[L_\varphi : K_\varphi] = 2$ for all real $\varphi \in S \cap S_\infty$.

Assuming this, we show $c \in \mathbb{B}r(L|K)$

as follows: For $N := L \cdot L'$ take the

inflation-restriction sequence (using $H^1 = 0$):

$$1 \longrightarrow \mathbb{B}r(L|K) \longrightarrow \mathbb{B}r(N|K) \xrightarrow{\text{res}_L} \mathbb{B}r(N|L)$$

$$\uparrow \qquad \nearrow$$

$$\mathbb{B}r(L'|K)$$

$\Rightarrow$ enough to show $\text{res}_L(c) = 1$.

But we have:

$$\text{res}_L(c) = 1 \iff \forall\, \mathfrak{P}|\varphi : \underbrace{\text{res}_{L_\mathfrak{P}}(c_\varphi) = 1}$$

$$\iff \forall\, \mathfrak{Q}|\mathfrak{P} : \text{inv}_{N_\mathfrak{Q}|L_\mathfrak{P}}(\cdots) = 1$$

using $\text{inv}_{N_\mathfrak{Q}|L_\mathfrak{P}} : \mathbb{B}r(N_\mathfrak{Q}|L_\mathfrak{P}) \hookrightarrow \mathbb{Q}/\mathbb{Z}$

and $\mathbb{B}r(N|L) = \bigoplus_{\mathfrak{P}} \mathbb{B}r(N_\mathfrak{Q}|L_\mathfrak{P})$ ($\mathfrak{Q}$ any $\mathfrak{Q}|\mathfrak{P}$)

Using the comm. diagram

$$\begin{array}{ccc} \mathrm{Br}(N_{\mathbb{Q}}|L_{\mathfrak{p}}) & \xrightarrow{\mathrm{inv}_{N_{\mathbb{Q}}|L_{\mathfrak{p}}}} & \mathbb{Q}/\mathbb{Z} \\ \uparrow{\scriptstyle \mathrm{res}_{L_{\mathfrak{p}}}} & & \uparrow{\scriptstyle d_{\mathfrak{p}}} \\ \mathrm{Br}(N_{\mathbb{Q}}|K_{\mathfrak{p}}) & \xrightarrow{\mathrm{inv}_{N_{\mathbb{Q}}|K_{\mathfrak{p}}}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

for $d_{\mathfrak{p}} := [L_{\mathfrak{p}} : K_{\mathfrak{p}}]$, we have

$$\mathrm{inv}_{N_{\mathbb{Q}}|L_{\mathfrak{p}}}(\mathrm{res}_{L_{\mathfrak{p}}}(c_{\mathfrak{p}})) = (\mathrm{inv}_{N_{\mathbb{Q}}|K_{\mathfrak{p}}}(c_{\mathfrak{p}}^{d_{\mathfrak{p}}}))$$

Therefore

$$\mathrm{res}_L(c) = 1 \iff \forall \mathfrak{p}: \; c_{\mathfrak{p}}^{d_{\mathfrak{p}}} = 1$$

and the last property holds since for $\mathfrak{p} \in S$:

- $\mathfrak{p} \nmid \infty \Rightarrow m \mid d_{\mathfrak{p}} \Rightarrow c_{\mathfrak{p}}^{d_{\mathfrak{p}}} = (c_{\mathfrak{p}}^{m})^{\cdots} = 1$
- $\mathfrak{p} \mid \infty$ real $\Rightarrow d_{\mathfrak{p}} = 2 \Rightarrow c_{\mathfrak{p}}^{d_{\mathfrak{p}}} = (\pm 1)^2 = 1.$

It remains to prove the claim. We show:

For any finite set S of places of K & any $m \in \mathbb{N}$,
$\exists$ cyclic cyclotomic $L|K$ sth

- $m \mid [L_{\mathfrak{p}} : K_{\mathfrak{p}}]$ for all $\mathfrak{p} \in S \setminus S_\infty$
- L is totally imaginary, i.e.
  $[L_{\mathfrak{p}} : K_{\mathfrak{p}}] = 2$ for all real $\mathfrak{p} \in S \cap S_\infty$.

We proceed in several steps:

① Replacing m by $m \cdot [K : \mathbb{Q}]$,
we may assume that $K = \mathbb{Q}$.

(for $\ell = 2$ let $n > 2$)

② Let ℓ be prime & ζ a primitive ℓ^n-th root of 1.
Then

$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/\ell^n)^* \simeq \begin{cases} H \times \mathbb{Z}/\ell^{n-1}, & \ell \neq 2 \\ H \times \mathbb{Z}/\ell^{n-2}, & \ell = 2 \end{cases}$$

with $|H| = \max\{\ell - 1, 2\}$.

$\Rightarrow$ $L_{\ell^n} := \mathbb{Q}(\zeta)^H$ cyclic cyclotomic / $\mathbb{Q}$

of degree

$$[L_{\ell^n} : \mathbb{Q}] = \begin{cases} \ell^{n-1} & \text{for } \ell \neq 2 \\ \ell^{n-2} & \text{for } \ell = 2 \end{cases}$$

Note that for $\ell = 2$, $L_{2^n} = \mathbb{Q}(\zeta - \zeta^{-1})$.

In particular, this is a totally imaginary field.

For any fixed ℓ and any p, we have

$$[L_{\ell^n, \mathfrak{p}} : \mathbb{Q}_p] \longrightarrow \infty \quad \text{as} \quad n \to \infty$$

($\mathfrak{p}$: any prime above p)

because

$$[\mathbb{Q}_p(\zeta) : \mathbb{Q}_p] \to \infty$$

$$[\mathbb{Q}_p(\zeta) : L_{\ell^n, \mathfrak{p}}] = |H| \leq \max\{\ell - 1, 2\}.$$

③ Let $m = \ell_1^{n_1} \cdots \ell_s^{n_s}$ w/ distinct primes $\ell_1, \ldots, \ell_s$.

Enlarging m we may assume $\ell_s = 2$, $n_s > 2$.

$\Rightarrow$ $L := L_{\ell_1^{n_1}} \cdots L_{\ell_s^{n_s}}$ totally imaginary & cyclic cyclotomic w/ the desired properties (by construction) $\square$

Cor ("fundamental sequence of Brauer gps")

We have a short exact sequence

$$1 \to Br(K) \xrightarrow{i} \bigoplus_{\mathfrak{p}} Br(K_{\mathfrak{p}}) \xrightarrow{inv} \mathbb{Q}/\mathbb{Z} \to 0$$

Pf.
- i injective by Albert-Brauer-Hasse-Noether
- inv surjective by local CFT
- $\operatorname{im}(i) \subset \ker(inv)$ by the previous section

- $\ker(\mathrm{inv}) \subset \mathrm{im}(i)$:

Let $c \in \mathbb{B}r(K) = \bigoplus_{\wp} \mathbb{B}r(K_\wp)$

$\downarrow$ $\qquad$ $\downarrow \mathrm{inv}$

$0 \in \mathbb{Q}/\mathbb{Z}$

By the above thm $\exists$ cyclic L/K

w/ $c \in \mathbb{B}r(L/K) = \bigoplus_{\wp} \mathbb{B}r(L_\mathfrak{P}/K_\wp)$

$\uparrow$ any $\mathfrak{P} \mid \wp$

Since $\mathrm{inv}_{L_\mathfrak{P}/K_\wp} : \mathbb{B}r(L_\mathfrak{P}/K_\wp) \twoheadrightarrow \frac{1}{n_\wp}\mathbb{Z}/\mathbb{Z}$

for $n_\wp := [L_\mathfrak{P} : K_\wp]$, we have

$\mathrm{inv}_{L/K} : \mathbb{B}r(L/K) \twoheadrightarrow \frac{1}{n}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$

w/ $n := \gcd(n_\wp \mid \text{all places } \wp)$

For L/K cyclic we have $n = [L:K]$:

Indeed $\mathrm{Gal}(L/K)$ is cyclic of order $[L:K]$, but also generated by Frobenii $\mathrm{Frob}_\wp$ for primes $\wp$ unramified in L/K. For such $\wp$, $\mathrm{ord}(\mathrm{Frob}_\wp) = f_{\mathfrak{P}/\wp} = [L_\mathfrak{P} : K_\wp] = n_\wp$.

$\Rightarrow$ For L/K cyclic we get an epi

$$\mathbb{B}r(L/K)/\mathbb{B}r(K) \xrightarrow{\mathrm{inv}} \tfrac{1}{[L:K]}\mathbb{Z}/\mathbb{Z}$$

$$\| \text{ (Tate)}$$

$$H^2(G_{L/K}, \mathbb{I}_L)/H^2(G_{L/K}, L^*)$$

$$\| \qquad \leftarrow \quad G_{L/K} \text{ cyclic} \Rightarrow H^i_T \simeq H^{i+2}_T$$

$$H^0_T(G_{L/K}, \mathbb{I}_L)/H^0_T(G_{L/K}, L^*)$$

$$\|$$

$$C_K/N_{L/K}(C_L)$$

$\Rightarrow$ iso by counting (use 2nd inequality) $\square$

The above shows that for L/K cyclic we have an exact sequence

$$1 \to Br(L/K) \to Br(L/K) \xrightarrow{\text{inv}} \frac{1}{[L:K]}\mathbb{Z}/\mathbb{Z} \to 0$$

$$\| \qquad\qquad \|$$

$$H^2(G_{L/K}, L^*) \qquad H^2(G_{L/K}, \mathbb{I}_L)$$

Comparing w/ the long exact sequence induced by $1 \to L^* \to \mathbb{I}_L \to C_L \to 1$ we also get

surjectivity of the map

$$H^2(G_{L/K}, \mathbb{I}_L) \longrightarrow H^2(G_{L/K}, C_L)$$

by periodicity:

$$\# H^2(G_{L/K}, C_L) = \# H^0_T(G_{L/K}, C_L) = [L:K]$$

($\uparrow$ 2nd inequality)

This usually fails for L/K non-cyclic!

For L/K non-cyclic we only have

$$1 \to H^2(G_{L/K}, L^*) \to H^2(G_{L/K}, \mathbb{I}_L) \to H^2(G_{L/K}, C_L) \to \underbrace{H^3(G_{L/K}, L^*)}_{\text{usually } \neq 0} \to 0$$

But similar arguments as above show:

$$H^2(G_K, C_{\bar{K}}) = \bigcup_{L/K \text{ cyclic}} H^2(G_{L/K}, C_L).$$

Using this one can still define

$$\text{inv}: H^2(G_K, C_{\bar{K}}) \to \mathbb{Q}/\mathbb{Z}$$

& verify the class field axioms, which gives another proof of Artin reciprocity (see Neukirch's Bonn lectures).

9. Norm subgps & the existence thm

For any number field K we have constructed an epi

$$(-, K): C_K \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(K^{ab}/K)$$

that induces for every finite abelian L/K an iso

$$\mathrm{Art}_{L/K}: C_K/N_{L/K}(C_L) \xrightarrow{\sim} \mathrm{Gal}(L/K).$$

Def A subgp $U \subset C_K$ is a norm subgp

if $\exists$ finite abelian L/K: $U = N_{L/K}(C_L)$.

Galois theory for K^{ab}/K then gives a bijection:

$$\left\{\begin{array}{c}\text{norm subgps}\\ \text{of } C_K\end{array}\right\} \xleftrightarrow{\sim} \left\{\begin{array}{c}\text{finite abelian}\\ \text{extensions } L/K\end{array}\right\}$$

To characterize norm subgps we need topology:

Lemma The norm residue symbol

$$(-, K): C_K \longrightarrow\!\!\!\!\!\rightarrow \mathrm{Gal}(K^{ab}/K)$$

is a continuous homomorphism.

Pf. By definition of the Krull topology, any open subgp $U \subset \mathrm{Gal}(K^{ab}/K)$ has the form $U = \mathrm{Gal}(K^{ab}/L)$ for L/K a finite abelian extension. By the main thm then $(-, K)^{-1}(U) = N_{L/K}(C_L)$, which is open in C_K because the subgp $N_{L/K}(\mathbb{I}_L) \subset \mathbb{I}_K$ is open: It contains the basic open subset $\prod_{\wp} \underbrace{N_{L_\wp/K_\wp}(\mathcal{O}_{L_\wp}^*)}_{= \mathcal{O}_{K_\wp}^* \text{ for all unramified } \wp/p}$. □

Intrinsic characterization of norm subgps:

Thm ("existence thm of global CFT")

A subgp $U \subset C_K$ is a norm subgp

if and only if it is open of finite index

Pf. Norm subgps are open of finite index by the above. We show the converse in several steps.

① If $U \subset C_K$ is a norm subgp, then so is also any larger subgp $V \supset U$.

Indeed, let $U = N_{L|K}(C_L)$ w/ $L|K$ finite abelian.

$$\Rightarrow \quad \begin{array}{ccc} C_K/U & \xrightarrow[\mathrm{Art}_{L|K}]{\sim} & \mathrm{Gal}(L|K) \\ {\scriptstyle pr}\downarrow & & \downarrow \\ C_K/V & \xrightarrow{\sim} & \mathrm{Gal}(M|K) \end{array}$$

for $M := L^H$, $H := \mathrm{Art}_{L|K}(V/U)$.

② If $K \ni \zeta_p :=$ a primitive p-th (prime) root of 1, any open subgp $V \subset C_K$ of finite index w/ $p \cdot C_K/V = 0$ is a norm subgp.

Indeed, let

$U :=$ (preimage of V) $\subset \mathbb{I}_K$

$\Rightarrow U \subset \mathbb{I}_K$ open

$\Rightarrow \exists$ finite set $S \supset S_\infty$ of places w/

$$U \supset \prod_{\mathfrak{p} \in S} \{1\} \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{K_\mathfrak{p}}^*$$

We also have $U \supset \mathbb{I}_K^p$ since $p \cdot C_K/V = 0$

$$\Rightarrow U \supset \mathcal{E} := \prod_{\mathfrak{p} \in S} (K_\mathfrak{p}^*)^p \times \prod_{\mathfrak{p} \notin S} \mathcal{O}_{K_\mathfrak{p}}^*$$

Wlog $S \supset \{\text{primes above } p\}$

and $\mathbb{I}_K = K^* \cdot \mathbb{I}_{K,S}$.

For $L := K(\sqrt[p]{a} \mid a \in O_{K,S}^*)$ then

$$K^* \cdot N_{L|K}(\mathbb{I}_L) = K^* \cdot \epsilon \qquad (*)$$

by similar arguments as in section IV.6:

Show $\epsilon \in N_{L|K}(\mathbb{I}_L)$ and

$[\mathbb{I}_K : K^* \epsilon] = p^{\#S} = [\mathbb{I}_K : K^* \cdot N_{L|K}(\mathbb{I}_L)]$

(see Milne, proof of lemma 9.3)

$\Rightarrow K^* \cdot N_{L|K}(\mathbb{I}_L) = K^* \cdot \epsilon \subset U$

$\Rightarrow N_{L|K}(C_L) \subset V$

$\Rightarrow V \subset C_K$ is a norm subgp by ①

③ Let $U \subset C_K$ be any subgp of finite index.

If $\exists$ finite K'/K sth $N_{K'/K}^{-1}(U) \subset C_{K'}$

is a norm subgp, then so is $U \subset C_K$.

Indeed, if $U' := N_{K'/K}^{-1}(U) \subset C_{K'}$ is a

norm subgp, take L/K' finite abelian

w/ $U' = N_{L/K'}(C_L)$.

Here L/K needn't be abelian or Galois,

but by the norm limitation thm (see below)

$\exists$ $M \subset L$ with M/K abelian sth

$$N_{M/K}(C_M) = N_{L|K}(C_L)$$

$$= N_{K'|K}(U') = U.$$

④ For arbitrary open $U \subset C_K$ of finite index, show U is a norm subgp by induct^n on $[C_K : U]$:

Pick a prime $p \mid [C_K : U]$.

By ③ we may assume $\zeta_p \in K$.

Pick $U_1 \subset C_K$ of index p w/ $U \subset U_1$
(in particular $U_1 \subset C_K$ is open)

$\Rightarrow$ By ② $\exists$ finite abelian K'/K sth $U_1 = N_{K'/K}(C_{K'})$.

In particular K'/K is cyclic w/ $\mathrm{Gal}(K'/K) \simeq \mathbb{Z}/p\mathbb{Z}$.

Put $U' := N_{K'/K}^{-1}(U_1)$.

$\Rightarrow$ exact sequence

$$1 \to U' \to C_{K'} \xrightarrow{N_{K'/K}} U_1/U \to 1$$

$\Rightarrow [C_{K'} : U'] = [U_1 : U] = \frac{1}{p} \cdot [C_K : U]$

$\Rightarrow$ By induction $U' \subset C_{K'}$ is a norm subgp

$\Rightarrow$ By ③ $U \subset C_K$ is a norm subgp. □

Upshot: $\exists$ inclusion-reversing bijection

$$\left\{ \begin{array}{l} \text{open subgps of} \\ \text{finite index in } C_K \end{array} \right\} \overset{1:1}{\longleftrightarrow} \left\{ \begin{array}{l} \text{finite abelian} \\ \text{extensions of } K \end{array} \right\}$$

Ex Take $K = \mathbb{Q}$.

For $m = \prod_p p^{m_p} \in \mathbb{Z}$ take the open subgp

$$U(m) := \prod_{p \mid m} U_p^{m_p} \times \mathbb{R}^*_{>0} \subset \mathbb{I}_{\mathbb{Q}}$$

attached to the modulus $\mathfrak{m} = m \cdot \infty$ (see §0.3),

where

$$U_p^{m_p} := \begin{cases} \mathbb{Z}_p^* & \text{if } m_p = 0 \\ 1 + p^{m_p}\mathbb{Z}_p & \text{if } m_p > 0 \end{cases}$$

By the exercises

$$C_{\mathbb{Q}} = \mathbb{I}_{\mathbb{Q}} / \mathbb{Q}^* \xrightarrow{\sim} \left(\mathbb{R}^* \times \prod_p \mathbb{Z}_p^* \right) / _{\{\pm 1\}}$$

$$\left((x_\infty, (x_p)_p \bmod \mathbb{Q}^* \right) \longmapsto \pm \left(x_\infty, (x_p \cdot p^{-v_p(x_p)}) \right)$$

"diagonally embedded"

$\Rightarrow$ The open subgp

$U_m := (\text{image of } U(m)) \subset C_{\mathbb{Q}}$

is of finite index with

$$C_{\mathbb{Q}} / U_m \simeq \prod_{p \mid m} \underbrace{\mathbb{Z}_p^* / (1 + p^{m_p}\mathbb{Z}_p)}_{\simeq \left(\mathbb{Z}/p^{m_p}\mathbb{Z}\right)^*} \simeq \left(\mathbb{Z}/m\mathbb{Z}\right)^*$$

Via CFT it corresponds to $L = \mathbb{Q}(\zeta_m)$.

(replacing $\mathfrak{m} = m \cdot \infty$ by $\mathfrak{n} = m$,

we would get $C_{\mathbb{Q}} / U_m \simeq \left(\mathbb{Z}/m\mathbb{Z}\right)^* / (\pm 1)$

corresponding to the extension $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$).

!! Unlike in local CFT, in global CFT

•• the word "open" cannot be dropped:

Rem $\exists$ non-open subgps $U \subset C_{\mathbb{Q}}$ that are of finite index:

We know $C_{\mathbb{Q}} \simeq \mathbb{R}_{>0} \times \prod_p \mathbb{Z}_p^*$ (see above).

For each $p > 2$, $\exists$ epi $\mathbb{Z}_p^* \twoheadrightarrow \mathbb{F}_2$

$\mathbb{F}_p^* \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

$\Rightarrow$ epi $\varphi : C_K \twoheadrightarrow \prod_{p>2} \mathbb{F}_2 =: V$ which is continuous for the product top.

Now we have $W := \bigoplus_{p>2} \mathbb{F}_2 \subsetneq V$ as a dense proper subspace. By linear algebra & axiom of choice $\exists$ proper subspace $W' \subsetneq V$ sth $\dim_{\mathbb{F}_2} V/W' < \infty$ and $W \subset W'$.

$\Rightarrow U := \varphi^{-1}(W') \subset C_K$ is a proper subgp of finite index but dense (since $U \supset \varphi^{-1}(W)$), hence not closed, so not open!

For completeness we also recall the norm limitation thm, since in abstract CFT we did it only for Galois extensions:

Thm ("norm limitation thm") For any finite L/K (not necessarily Galois), let $M \subset L$ be the maximal subfield with M/K abelian Galois. Then

$$N_{L/K}(C_L) = N_{M/K}(C_M).$$

Pf. Let $\tilde{L}/K$ be the Galois hull of L/K.

Put $H := \mathrm{Gal}(\tilde{L}/L) \subset G := \mathrm{Gal}(\tilde{L}/K)$.

$$\begin{array}{ccc}
H^{ab} & & C_L/N_{\tilde{L}/L}(C_{\tilde{L}}) \\
\| & & \| \\
H_T^{-2}(H,\mathbb{Z}) & \xrightarrow{\sim} & H_T^0(H, C_{\tilde{L}}) \\
\downarrow \text{cores} & & \downarrow \text{cores} \\
H_T^{-2}(G,\mathbb{Z}) & \xrightarrow{\sim} & H_T^0(G, C_{\tilde{L}}) \\
\| & & \| \\
G^{ab} & & C_K/N_{\tilde{L}/K}(C_{\tilde{L}})
\end{array}$$

$$\Rightarrow \underbrace{\mathrm{cok}(H^{ab} \to G^{ab})}_{\simeq (G/H)^{ab}} \simeq \underbrace{\mathrm{cok}(C_L/\ldots \to C_K/\ldots)}_{\simeq C_K/N_{L/K}(C_L)}$$

$$\simeq \mathrm{Gal}(M/K)$$

$$\simeq C_K/N_{M/K}(C_M) \text{ by the main thm} \qquad \square$$

V. Analytic tools

1. Dirichlet series

Def A Dirichlet series is a formal series

$$f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

w/ coefficients $a_1, a_2, \ldots \in \mathbb{C}$.

Ex a) The Riemann zeta fct^n $\zeta(s) := \sum_{n \geq 1} \frac{1}{n^s}$.

b) More generally, for any number field K we define its Dedekind zeta fct^n

$$\zeta_K(s) := \sum_{0 \neq \alpha \trianglelefteq \mathcal{O}_K} \frac{1}{N(\alpha)^s}$$

(take $a_n := \#\{0 \neq \alpha \trianglelefteq \mathcal{O}_K \mid N(\alpha) = n\}$)

Convergence criterion

a) If a Dirichlet series $f(s) = \sum_{n \geq 1} \frac{a_n}{n^s}$ converges at some $s_0 \in \mathbb{C}$, then it converges locally uniformly to a holomorphic fct^n on the half-plane $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \mathrm{Re}(s_0)\}$. We define its abscissa of convergence by

$$\sigma(f) := \inf \{ c \in \mathbb{R} \mid f(s) \text{ converges for } \mathrm{Re}(s) > c \}$$

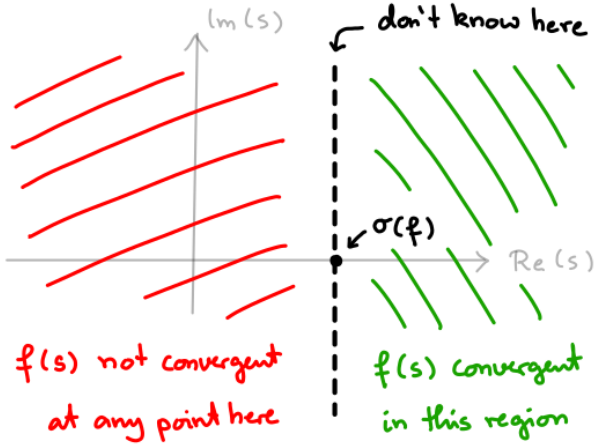
b) If $\exists\, c, \sigma_0 > 0$ sth $\forall n$:

$$|a_1 + \cdots + a_n| \leq c \cdot n^{\sigma_0}$$

then we have $\sigma(f) \leq \sigma_0$.

Pf. Elementary estimates, see e.g. Neukirch, CFT, V.1. □

Thus we have the following picture:



Ex The Dirichlet series $\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$

has abscissa of convergence $\sigma(\zeta_K) = 1$

(use the above criterion & divergence at $s=1$).

Like for the Riemann zeta fct^n we also have an expression as an infinite product:

Prop ("Euler product")

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \subsetneq \mathcal{O}_K \\ \text{max. ideal}}} \frac{1}{1 - N(\mathfrak{p})^{-s}} \quad \text{for } \mathrm{Re}(s) > 1.$$

Pf. Consider the geometric series

$$\frac{1}{1 - N(\mathfrak{p})^{-s}} = \sum_{i \geq 1} \frac{1}{(N(\mathfrak{p})^n)^s} = \sum_{i \geq 1} \frac{1}{N(\mathfrak{p}^n)^s}$$

$\Rightarrow$ Unique ideal factorization in $\mathcal{O}_K$ gives

$$\prod_{N(\mathfrak{p}) \leq n_0} \frac{1}{1 - N(\mathfrak{p})^{-s}} = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} \xrightarrow{n_0 \to \infty} \zeta_K(s)$$

$\uparrow$

sum over $\mathfrak{a} \subsetneq \mathcal{O}_K$ that are divisible at most by primes $\mathfrak{p}$ with $N(\mathfrak{p}) \leq n_0$

□

Like for the Riemann $\zeta(s)$ we find a pole at $s = 1$:

Thm ("class number formula") Let $N = [K:\mathbb{Q}]$.

Then the fct^n $\zeta_K(s)$ has an analytic continuation to $\{ z \in \mathbb{C} \mid \mathrm{Re}(z) > 1 - \frac{1}{N} \}$, holomorphic except for a simple pole at $s = 1$ with residue

$$\lim_{s \to 1+} (s-1)\,\zeta_K(s) = \underbrace{\frac{2^{r_1} \cdot (2\pi)^{r_2} \cdot R}{m \cdot \sqrt{|D|}}}_{=:\gamma} \cdot h$$

where

- $h = \# Cl_K$ class number
- $D = \mathrm{discr}(K)$ discriminant
- $m = \# \mu(K)$ roots of 1
- $r_1 = \#$ real places, $r_2 = \#$ cplex places
- $R =$ regulator
  $:=$ volume of fundamental parallelopiped of the lattice $\mathcal{O}_K^* / \mu(K) \hookrightarrow \mathbb{R}^{r_1+r_2}$

Pf. For every ideal class $c \in Cl_K$ put

$$\zeta_{K,c}(s) := \sum_{\substack{\mathfrak{a} \in c \\ \uparrow}} \frac{1}{N(\mathfrak{a})^s} = \sum_{n \geq 1} \frac{a_n}{n^s}$$

sum over all integral ideals $\mathfrak{a} \subseteq \mathcal{O}_K$ with $[\mathfrak{a}] = c$

w/ $a_n = \# \{ \mathfrak{a} \subseteq \mathcal{O}_K \mid [\mathfrak{a}] = c \ \& \ N(\mathfrak{a}) = n \}$.

Minkowski theory:

$$A_n := \# \{ \mathfrak{a} \subseteq \mathcal{O}_K \mid [\mathfrak{a}] = c \ \& \ N(\mathfrak{a}) \leq n \} = \gamma + O(n^{1-1/N})$$

$\Rightarrow$ The Dirichlet series

$$f(s) := \zeta_{K,c}(s) - \gamma \cdot \zeta(s) =: \sum_{n \geq 1} \frac{b_n}{n^s}$$

has $b_1 + \cdots + b_n = A_n - \gamma \cdot n = O(n^{1-1/N})$

hence converges on $\mathrm{Re}(s) > 1 - 1/N$

$\Rightarrow$ $\zeta_{K,c}(s)$ extends to $\mathrm{Re}(s) > 1 - 1/N$
w/ only simple pole at $s = 1$ & residue γ

$\Rightarrow$ $\zeta_K(s) = \sum_c \zeta_{K,c}(s)$ has w/ residue $\gamma \cdot h$. $\square$

Let's count ideals in a more sophisticated way, weighting ideal classes with a character. We do this more generally for class gps replaced by ray class gps $Cl(\mathfrak{m}) := I(\mathfrak{m})/R(\mathfrak{m})$

↑ $\mathfrak{m} = \mathfrak{m}_f \cdot \mathfrak{m}_\infty$ a modulus

where

$I(\mathfrak{m}) := \langle \mathfrak{p} \mid \mathfrak{p} \nmid \mathfrak{m}_f \rangle$ fractional ideals coprime to $\mathfrak{m}_f$

∪|

$R(\mathfrak{m}) := \{(a) \mid a \equiv 1 \bmod^* \mathfrak{m}\}$

↳ • $v_\mathfrak{p}(a-1) \geq v_\mathfrak{p}(\mathfrak{m}_f) \quad \forall \mathfrak{p} \mid \mathfrak{m}_f$

• $\sigma(a) > 0 \quad \forall \sigma \mid \mathfrak{m}_\infty$

Def For any character $\chi : Cl(\mathfrak{m}) \to \mathbb{C}^*$ the associated Dirichlet L-function is

$$L(s,\chi) := \sum_{\substack{\mathfrak{a} \in I(\mathfrak{m}) \\ \mathfrak{a} \subseteq \mathcal{O}_K}} \frac{\chi(\mathfrak{a})}{N(\mathfrak{a})^s}$$

Ex a) For $\mathfrak{m} = (1)$ and $\chi = 1$ we recover the zeta fct^n $L(s,1) = \zeta_K(s)$.

b) For $K = \mathbb{Q}$ and $\mathfrak{m} = (m) \cdot \infty$ we have $Cl(\mathfrak{m}) = (\mathbb{Z}/m\mathbb{Z})^*$ and get classical Dirichlet series $L(s,\chi) = \sum_{\substack{n \geq 1, \\ \gcd(m,n)=1}} \frac{\chi(n)}{n^s}$

In general $L(s,\chi)$ is still a Dirichlet series.

As before one shows that for $Re(s) > 1$ it converges and satisfies

$$L(s,\chi) = \prod_{\mathfrak{p} \nmid \mathfrak{m}} \left(1 - \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}\right)^{-1}$$

But for $\chi \neq 1$ it's even better:

Prop If $\chi \neq 1$, then $L(s,\chi)$ converges on the entire half-plane

$$\{ z \in \mathbb{C} \mid \mathrm{Re}(z) > 1 - \tfrac{1}{N} \} \quad \text{(no pole at } s=1\text{)}.$$

Pf. For $c \in Cl(m)$ put $\zeta_{K,c}(s) := \sum_{a \in c} \frac{1}{N(a)^s} =: \sum_{n \geq 1} \frac{a_n}{n^s}$

Minkowski theory gives a constant κ_m with

$$a_1 + \cdots + a_n = \kappa_m \cdot n + O(n^{1-1/N})$$

$$\Rightarrow \quad L(s,\chi) = \sum_c \chi(c) \cdot \zeta_{K,c}(s) =: \sum_{n \geq 1} \frac{b_n}{n^s}$$

has

$$b_1 + \cdots + b_n = \underbrace{\sum_c \chi(c)}_{= 0 \text{ for } \chi \neq 1 !} \cdot \kappa_m \cdot n + O(n^{1-1/N})$$

$\Rightarrow$ claim follows from the convergence criterion. $\square$

2. Dirichlet density

What's the probability of a random prime to be in a given set?

Def The Dirichlet density of a set T of prime ideals is the limit (if it exists)

$$\delta(T) := \lim_{s \to 1+} \frac{\sum_{\varphi \in T} N(\varphi)^{-s}}{\sum_{\text{all } \varphi} N(\varphi)^{-s}}$$

Rem If $d(T) := \lim_{n \to \infty} \frac{\#\{\varphi \in T \mid N(\varphi) \le n\}}{\#\{\text{all } \varphi \mid N(\varphi) \le n\}}$

exists, then so does $\delta(T)$ & they are equal.

But $\exists$ sets T sth • $\delta(T)$ exists &
• $d(T)$ doesn't.

A sufficient criterion for existence uses

$$\zeta_{K,T}(s) := \prod_{\varphi \in T} \frac{1}{1 - N(\varphi)^{-s}} :$$

Lemma ("polar criterion") If $\exists n \in \mathbb{N}$ sth $(\zeta_{K,T}(s))^n$ extends meromorphically w/ a pole of order m at $s = 1$, then T has Dirichlet density

$$\delta(T) = \frac{m}{n}.$$

Pf.

$$\log \zeta_{K,T}(s)^n \sim n \cdot \sum_{\varphi \in T} N(\varphi)^{-s}$$

(ie difference is bounded near $s = 1$)

by our assumpt^n $\longrightarrow \zeta$

$$m \cdot \log \frac{1}{s-1} \sim m \cdot \sum_{\text{all } \varphi} N(\varphi)^{-s}$$

□

Ex $T := \{ \mathfrak{p} \mid N(\mathfrak{p}) \text{ is not a prime} \}$

has $\zeta_{K,T}(s)$ holomorphic at $s = 1$,

hence Dirichlet density $\delta(T) = 0$:

For $\mathfrak{p} \in T$ we have $N(\mathfrak{p}) = p^f$ w/ $f \geq 2$

For any p $\exists$ at most $d := [K : \mathbb{Q}]$ primes $\mathfrak{p} \mid p$

$$\Rightarrow \zeta_{K,T}(s) = \prod_{i=1}^{d} g_i(s)$$

w/ $g_i(s) = \prod_p g_{i,p}(s)$,

$$g_{i,p}(s) = 1 \text{ or } = \frac{1}{1 - p^{-fs}} \quad (f \geq 2)$$

$$\Rightarrow g_i(1) \leq \prod_p \frac{1}{1 - p^{-2}} = \zeta(2) < \infty$$

$\Rightarrow g_i$ holom. at $s = 1$

$\Rightarrow \zeta_{K,T}(s)$ holom. at $s = 1$ □

Prop For L/K finite w/ Galois hull $\tilde{L}/K$,

$T := \{ \mathfrak{p} \trianglelefteq \mathcal{O}_K \mid \mathfrak{p} \text{ splits completely in } L \}$

has Dirichlet density $\delta(T) = \frac{1}{[\tilde{L} : K]}$.

Pf. $\mathfrak{p}$ splits completely in L/K iff it does in $\tilde{L}/K$

(for $\Rightarrow$ use that if $\mathfrak{p}$ splits completely in two extensions L, L' then it does in the composite $L \cdot L'$)

So wlog $L = \tilde{L}$ Galois over K

Let $\tilde{T} := \{ \text{primes } \mathfrak{P} \trianglelefteq \mathcal{O}_L \text{ w/ } \mathfrak{P} \cap K \in T \}$

Above each $\mathfrak{p} \in T$ $\exists$ precisely $[L : K]$ primes $\mathfrak{P} \in \tilde{T}$

and each has $N_{L/K}(\mathfrak{P}) = \mathfrak{p}$, so $N(\mathfrak{P}) = N(\mathfrak{p})$.

$$\Rightarrow \zeta_{L,\tilde{T}}(s) = (\zeta_{K,T}(s))^{[L:K]} \qquad (*)$$

Since $\tilde{T} \supset \{ \mathfrak{P} \text{ unramified in } L/\mathbb{Q} \text{ w/ } N(\mathfrak{P}) \text{ prime} \}$

we have $\zeta_{L,\tilde{T}}(s) \sim \zeta_L(s)$ by previous example

$\Rightarrow \delta(T) = \frac{1}{[L:K]}$ by polar criterion & $(*)$ □

3. Density theorems

m modulus

$\bar{H} \subset Cl(m)$ any subgp

$H \subset I(m)$ its preimage ("congruence subgp")

Q How are the prime ideals $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ distributed among the finitely many cosets of $H \subset I(m)$?

Let's start w/ the trivial coset:

Prop The set $T := \{\mathfrak{p} \trianglelefteq \mathcal{O}_K \mid \mathfrak{p} \in H\}$ has Dirichlet density

$$\delta(T) = \frac{1}{h} \quad \text{for } h := [I(m) : H].$$

↑ expected number if each coset has the same density!

Pf. By CFT $\exists$ finite abelian L/K (a subextension of the ray class field K_m) w/

$$Art_{L/K} : Cl(m)/H \xrightarrow{\sim} Gal(L/K).$$

For $\mathfrak{p} \nmid m$ unramified in L/K,

$$\mathfrak{p} \in H \iff [\mathfrak{p}] = 1 \in Cl(m)/H$$

$$\iff Frob_{\mathfrak{p}} = 1 \in Gal(L/K)$$

$$\iff \mathfrak{p} \text{ completely split in } L/K$$

Thus

$$\delta(\{\mathfrak{p} \in H\}) = \delta(\{\mathfrak{p} \trianglelefteq \mathcal{O}_K \text{ completely split in } L\})$$

$$= \frac{1}{[L:K]} \quad \text{by previous proposition}$$

$$= \frac{1}{h}.$$

□

Recall that $L(s,\chi) := \sum_{\alpha \in I(m)} \frac{\chi(\alpha)}{N(\alpha)^s}$

is holomorphic at $s=1$ for all $\chi \neq 1$. We get:

<u>Cor</u> $L(1,\chi) \neq 0$ for all $\chi \neq 1$.

Pf. For any $\chi \in \mathrm{Hom}(Cl(m), \mathbb{C}^*)$,

$$L(s,\chi) = \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{N(p)^s}\right)^{-1}$$

$$\Rightarrow \log L(s,\chi) \sim \sum_{p \nmid m} \frac{\chi(p)}{N(p)^s} \quad \text{as } s \to 1+$$

Sum over all $\chi \in \mathrm{Hom}(Cl(m), \mathbb{C}^*)$ and use the the relation

$$\sum_{\chi} \chi(p) = \begin{cases} |Cl(m)| & \text{if } p \in H \\ 0 & \text{if } p \notin H \end{cases}$$

↳ $= h$ for $H := R(m)$

$$\Rightarrow \sum_{\chi} \log L(s,\chi) \sim h \cdot \sum_{p \in H} \frac{1}{N(p)^s}$$

Here

$$\log L(s,1) \sim \begin{cases} \log \frac{1}{s-1} & (\chi = 1) \\ -m(\chi) \cdot \log \frac{1}{s-1} & (\chi \neq 1) \end{cases}$$

w/ $m(\chi) := \mathrm{ord}_{s=1} L(s,\chi) \geq 0$ for $\chi \neq 1$

$$\Rightarrow \left(1 - \sum_{\chi \neq 1} m(\chi)\right) \cdot \log \frac{1}{s-1} \sim h \cdot \sum_{p \in H} N(p)^{-s}$$

$$\Rightarrow \delta(\{p \in H\}) = \frac{1 - \sum_{\chi \neq 1} m(\chi)}{h}$$

$\Rightarrow m(\chi) = 0$ for all $\chi \neq 1$

by comparison w/ the proposition. $\square$

Cor ("Dirichlet density thm")

Let $\bar{H} \subset Cl(m)$ & $H \subset I(m)$ its preimage.

Then for any coset $c \in C_H := I(m)/H$,

$$\delta(\{\mathfrak{p} \in c\}) = \frac{1}{h} \quad \text{w/ } h := [I(m) : H].$$

Pf. Again $\log L(s,\chi) \sim \sum_{\mathfrak{p} \nmid m} \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s}$ as $s \to 1+$

$$= \sum_{b \in C_H} \chi(b) \cdot \sum_{\mathfrak{p} \in b} \frac{1}{N(\mathfrak{p})^s}$$

Multiply by $\chi(c^{-1})$ and sum over all χ:

$$\Rightarrow \log \zeta_K(s) + \sum_{\chi \neq 1} \chi(c^{-1}) \cdot \log L(s,\chi)$$

$$\sim \sum_{b \in C_H} \sum_{\chi} \chi(c^{-1}b) \cdot \sum_{\mathfrak{p} \in c} \frac{1}{N(\mathfrak{p})^s}$$

For $\chi \neq 1$ we have $L(1,\chi) \neq 0$ (previous cor.),

hence $\log L(s,\chi) \sim 0$ as $s \to 1+$.

Moreover

$$\sum_{\chi} \chi(c^{-1}b) = \begin{cases} h & \text{if } b = c \\ 0 & \text{else} \end{cases}$$

$$\Rightarrow \log \zeta_K(s) \sim h \cdot \sum_{\mathfrak{p} \in c} \frac{1}{N(\mathfrak{p})^s}$$

$$\Rightarrow \delta(\{\mathfrak{p} \in c\}) = \frac{1}{h}. \qquad \square$$

Ex (Dirichlet thm on primes in arithmetic progressions)

For $K = \mathbb{Q}$ & $\mathfrak{m} = (m) \cdot \infty$,

$Cl(m) \simeq (\mathbb{Z}/m\mathbb{Z})^*$.

Taking $\bar{H} = \{1\}$ we get for $c \in (\mathbb{Z}/m\mathbb{Z})^*$:

$$\delta(\{\text{primes } p \equiv c \bmod m\}) = \frac{1}{\varphi(m)}.$$

Now pick any finite Galois extension L/K

w/ gp $G = \mathrm{Gal}(L/K)$ (not necessarily abelian).

For $\sigma \in G$ let

$$P_{L/K}(\sigma) := \{ \mathfrak{p} \in \mathcal{O}_K \mid \exists \mathfrak{P} | \mathfrak{p} \text{ unramified w/ } \mathrm{Frob}_{\mathfrak{P}} = \sigma \}$$

↓ only depends on conjugacy class

$$cc(\sigma) := \{ g\sigma g^{-1} \mid g \in G \} \subset G.$$

Thm (Cebotarev) We have

$$\delta(P_{L/K}(\sigma)) = \frac{\#\, cc(\sigma)}{\#\, G}.$$

Pf. ① If $G = \langle \sigma \rangle$:

Pick m with $L \subset K_m$, ie $\exists\, R(m) \subset H \subset I(m)$

sth $\mathrm{Art}_{L/K} : I(m)/H \xrightarrow{\sim} G.$

ψ ψ

$\exists\, c \longmapsto \sigma$

$\Rightarrow P_{L/K}(\sigma) = \{ \mathfrak{p} \in c \}$

$\Rightarrow \delta(\dots) = \frac{1}{n} = \frac{1}{\#G} = \frac{\#\, cc(\sigma)}{\#G}$ by Dirichlet's density thm

$cc(\sigma) = \{\sigma\}$ for G abelian

② General case:

Let $M := (\text{fixed field of } \sigma) \subset L$

For $f := \mathrm{ord}(\sigma)$ then $\delta(P_{L/M}(\sigma)) = \frac{1}{f}$ by ①

Now consider

$P_{L/M}(\sigma)$ ← differ only by primes ramified or of degree > 1 over $\mathbb{Q}$

$\cup$

$P'_{L/M}(\sigma) := \{ \mathfrak{q} \in P_{L/M}(\sigma) \mid M_{\mathfrak{q}} = K_{\mathfrak{p}} \text{ for } \mathfrak{p} = \mathfrak{q} \cap K \}$

$\downarrow \varphi$

$P_{L/K}(\sigma)$ w/ $\varphi(\mathfrak{q}) := K \cap \mathfrak{q}$.

$$\varphi^{-1}(\mathfrak{p}) \simeq \{ \mathfrak{P} \trianglelefteq \mathcal{O}_L \text{ prime} \mid \mathfrak{P} | \mathfrak{p} \text{ unram}, \operatorname{Frob}_{\mathfrak{P}} = \sigma \}$$

$$\simeq Z_G(\sigma) / G_{\mathfrak{p}}$$

$$\left(\begin{array}{l} Z_G(\sigma) := \{ g \in G \mid g \sigma g^{-1} = \sigma \} \\ G_{\mathfrak{p}} := \{ g \in G \mid \sigma(\mathfrak{p}) = \mathfrak{p} \} \end{array} \right)$$

$$\Rightarrow \# \varphi^{-1}(\mathfrak{p}) = \# Z_G(\sigma) / f$$

$$\Rightarrow \delta(P_{L|K}(\sigma)) = \frac{1}{\# \varphi^{-1}(\mathfrak{p})} \cdot \delta(P'_{L|M}(\sigma))$$

$$= \frac{f}{\# Z_G(\sigma)} \cdot \delta(P_{L|M}(\sigma))$$

$$= \frac{f}{\# Z_G(\sigma)} \cdot \frac{1}{f}$$

$$= \frac{1}{\# Z_G(\sigma)}$$

$$= \frac{\# cc(\sigma)}{\# G} .$$

□