4 lectures on Class Field Theory

I. Introduction

CFT has its origin in 'reciprocity laws'.

Problem Let $f \in \mathbb{Z}[X]$. How does factorisation of $f \bmod p$ depend on p?

Clearly essential case is f irreducible, & (after ch. of var.) monic. Then for almost all p, $f \bmod p$ is separable, ($\Leftrightarrow p \nmid \mathrm{Discr}(f)$) and the factorisation type of $f \bmod p$ is a partition $n = m_1 + \dots + m_r$ ($n = \deg f$).

Thm 1.: Suppose $\mathrm{Gal}(f/\mathbb{Q})$ is abelian. Then $\exists\, N = N(f) \geq 1$ s.t. factorisation of $f \bmod p$ depends only on $p \bmod N$.

Exs. $f = X^2 + 1$: $f \bmod p$ irreducible $\Leftrightarrow p \equiv 3 \pmod 4$

$(\text{linear}) \times (\text{linear})$ $\quad p \equiv 1 \pmod 4$

$(X+1)^2$ $\quad p \equiv 2 \pmod 4$

$f = X^2 - q$, q odd prime. Then for $p \notin \{2, q\}$,

$f \bmod p$ reducible $\Leftrightarrow \left(\frac{q}{p}\right) = 1$

$\Leftrightarrow \left(\frac{p}{q}\right) = (-1)^{(p-1)(q-1)/4}$ by quadratic reciprocity

which depends only on $p \bmod 4q$

Let $\bar{f} = f \bmod p$ (assumed separable).

$= g_1 \cdots g_r$, g_i irred $\in \mathbb{F}_p[X]$, degree m_i.

By Galois thy, Frobenius $\varphi_p \in \mathrm{Gal}(\bar{f}/\mathbb{F}_p) \subset S_m$ has cycle type $(m_1, \ldots, m_r)$.

More precisely, let L = splitting field of f

v = place of L over p; $f \bmod p$ separable $\Rightarrow$ v unramified

$\Rightarrow Fr_v \in \mathrm{Gal}(L_v/\mathbb{Q}_p) = G_v \subset \mathrm{Gal}(L/\mathbb{Q}) = G$

If $v'|p$ is another place, then $v' = \sigma v$ for some $\sigma \in G$.

and $G_{v'} = \sigma^{-1} G_v \sigma$, $Fr_{v'} = \sigma^{-1} Fr_v \sigma$.

So p determines a conjugacy class $Fr_p = \{Fr_v \mid v|p\} \subset G$.

(G abel. $\Rightarrow$ $Fr_p = \{Fr_v\}$ $\forall v|p$)

Refined problem: how does this vary with p? (Can we forget about f.)

Thm 1': $L/\mathbb{Q}$ abelian field, $G = \mathrm{Gal}(L/\mathbb{Q})$.
$\exists N \geq 1$ s.t. Fr_p depends only on $p \bmod N$.

Proof: is a consequence of

Kronecker-Weber Thm: if $L/\mathbb{Q}$ is finite abelian, then for some $N \geq 1$, $L \subset \mathbb{Q}(\zeta_N) = \mathbb{Q}(e^{2\pi i/N})$.

Now $\mathrm{Gal}(\mathbb{Q}(\zeta_N)) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^*$

$\sigma_a \longleftrightarrow a$, $\sigma_a(\zeta_N) = \zeta_N^a$.

So if $p \nmid N$, σ_p = the arithmetic Frobenius
(as $\sigma_p(x) \equiv x^p \bmod p \quad \forall x \in \mathbb{Z}[\zeta_N]$).

Hence trivially depends only on p and N.

More generally L/K extn of number fields,
$G = Gal(L/K)$ abelian. The $\forall v$ finite, unramified in L/K
place of K
have $Fr_v \in G$. Class field Theory then says:

$\exists$ modulus m, divisible by only the ramified and ∞ places of K, such that Fr_v depends only on the class of v in ray class group

$$Cl_m(K) = J_K / K^* U_m \cong \frac{I_m(K)}{P_m(K)}$$

(Recall from Ex Sheet 2.
$v \longleftrightarrow$ class of idele $(1, \dots, 1, \pi_v, 1, \dots) \in J_K/K^* U_m$
$\longleftrightarrow$ class of $P_v^{-1} \in I_m(K)/P_m(K)$.

Precisely:

Thm 1'' (Artin's reciprocity law) $\exists!$ cts. hom

$$Art_K : J_K \longrightarrow Gal(L/K)$$

such that (i) $Art_K(K^*) = 1$

(ii) $\forall$ unramified finite v,

$\forall x \in K_v^* \subset J_K$, $\quad Art_K(x) = Fr_v^{v(x)}$

Remarks

(1) v unramified $\Rightarrow$ $\mathrm{Art}_K(\mathcal{O}_v^*) = 1$

and $\mathrm{Art}_K(K_v^*) = \langle \mathrm{Fr}_v \rangle = G_v = \mathrm{Gal}(L_w/K_v)$ $\forall w|v$.

(2) From Ex. sheet 3, (i) & (ii) determine Art_K uniquely, if it exists.

(3) For <u>every</u> v (incl. ramified & infinite ones) get hom
$$K_v^* \longrightarrow G$$
whose image is in fact the local Galois gp. G_v

(4) Another thm. describes kernel:
$$\ker(\mathrm{Art}_K) = K^* N_{L/K}(J_L).$$

(5) In contrast to case of $\mathbb{Q}(\zeta_N)/\mathbb{Q}$, no <u>explicit</u> iso between G and $J_K/K^* N_{L/K}(J_L)$.

Modern approach to CFT: begin by studying local picture – ie. (3)

<u>Notation</u>: K field, $\bar{K}$ = a alg. closure (unique up to $\cong$)
$\mathrm{Gal}(\bar{K}/K)$ unique up to conjugacy.

$\bar{K} \supset K^{ab}$ = max^l abelian subfield
– again unique up to iso. In this case, $\mathrm{Gal}(K^{ab}/K)$ unique up to unique $\cong$

Also, if G a finite gp,

$G^{ab} := G/[G,G]$ max$^{\text{l}}$ ab. quotient

G profinite gp: $G^{ab} = G/\overline{[G,G]}$ max$^{\text{l}}$ cts ab. quotient

Infinite Galois theory: $G = Gal(\bar{K}/K)$

- closed sgps. of G $\longleftrightarrow$ subfields of $\bar{K}$
- open ——— $\longleftrightarrow$ ..... finite /K.

and $G^{ab} = Gal(K^{ab}/K)$!

Local CFT

- statements, exs.

Fix p, $\bar{\mathbb{Q}}_p \supset \mathbb{Q}_p$; consider finite exts $K/\mathbb{Q}_p$ inside $\bar{\mathbb{Q}}_p$, $q = \#k_K$.

$$K \subset K^{nr} \subset K^{ab} \subset \bar{K} = \bar{\mathbb{Q}}_p$$

K^{nr} = max$^{\text{l}}$ unram ext of K in $\bar{\mathbb{Q}}_p$

$$= \bigcup_{(n,p)=1} K(\zeta_n)$$

$$Gal(K^{nr}/K) \simeq Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q) \simeq \hat{\mathbb{Z}}$$

$$\text{Fr}_{K^{nr}/K} \longmapsto \varphi_q^{-1} \longmapsto 1$$

Thm. $\exists!$ family of abs hom's (**Artin map**)

$$\mathrm{Art}_K : K^\times \longrightarrow \mathrm{Gal}(K^{ab}/K)$$

satisfying the 2 properties:

i) $K^\times \xrightarrow[\mathrm{Art}_K]{} \mathrm{Gal}(K^{ab}/K) \to \mathrm{Gal}(K^{ur}/K)$

is the map $x \longmapsto \mathrm{Fr}_{K^{ur}/K}^{v(x)}$

ii) If L/K ($\leadsto L^{ab} \supset K^{ab}$), the diagram

$$\begin{array}{ccc} L^\times & \longrightarrow & \mathrm{Gal}(L^{ab}/L) \\ \downarrow N_{L/K} & & \downarrow \text{restriction} \\ K^\times & \longrightarrow & \mathrm{Gal}(K^{ab}/K) \end{array}$$

commutes.

Moreover: iii) Art_K is injective, with image the dense subgp.

$$W_{K^{ab}/K} = \left\{ \sigma \in \mathrm{Gal}(K^{ab}/K) \;\middle|\; \sigma|_{K^{ur}} = \mathrm{Fr}_{K^{ur}/K}^{n} \right\}$$

for some $n \in \mathbb{Z}$

iv) If L/K is finite Galois, Art_K induces a (surjection)

$$\mathrm{Art}_{L/K} : K^\times / N_{L/K}(L^\times) \xrightarrow{\sim} \mathrm{Gal}(L/K)^{ab}.$$

NB. Can't hope that $K^\times \simeq \mathrm{Gal}(K^{ab}/K)$ since Gal is profinite, but $K^\times$ isn't, since $v : K^\times \twoheadrightarrow \mathbb{Z}$.

Clarify iii):

$$\begin{array}{ccccccc} 1 \to I(K^{ab}/K) & \longrightarrow & Gal(K^{ab}/K) & \longrightarrow & Gal(K^{nr}/K) & \longrightarrow & 1 \\ \| & & \cup & & \cup & & \\ 1 \to I(K^{ab}/K) & \longrightarrow & W(K^{ab}/K) & \longrightarrow & \langle Fr_{K^{nr}/K} \rangle^{\mathbb{Z}} & \longrightarrow & 1 \end{array}$$

$\hat{\mathbb{Z}} \simeq \mathbb{Z} \times \prod_{p \text{ prime}} \mathbb{Z}_p$

II. The case of $\mathbb{Q}_p$ Completely explicit (roots of unity):

$$\mathbb{Q}_p^{cycl} := \bigcup_{N \geq 1} \mathbb{Q}_p(\zeta_N) = \mathbb{Q}_p^{nr} \cdot \mathbb{Q}_p(\mu_{p^\infty})$$

$$\mathbb{Q}_p(\mu_{p^\infty}) = \bigcup \mathbb{Q}_p(\zeta_{p^n})$$

totally ram.

$$\text{So } Gal(\mathbb{Q}_p^{cycl}/\mathbb{Q}_p) = Gal(\mathbb{Q}_p^{nr}/\mathbb{Q}_p) \times Gal(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)$$

$$Gal(\mathbb{Q}_p^{nr}/\mathbb{Q}_p) \ni Fr_p \qquad Gal(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) \ni \sigma_a : \zeta_{p^n} \mapsto \zeta_{p^n}^a \text{ mod } p^n, \; a \in \mathbb{Z}_p^*$$

$$\simeq \hat{\mathbb{Z}} \times \mathbb{Z}_p^* = \varprojlim (\mathbb{Z}/p^n\mathbb{Z})^* = Gal(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p)$$

Define $\mathbb{Q}_p^* \longrightarrow Gal(\mathbb{Q}_p^{cycl}/\mathbb{Q}_p)$

$$\cup$$

$$p^m a, \; a \in \mathbb{Z}_p^* \longmapsto Fr_p^m \times \sigma_a.$$

- image is $\mathbb{Z} \times \mathbb{Z}_p^* \subset \hat{\mathbb{Z}} \times \mathbb{Z}_p^*$

This is the map $Art_{\mathbb{Q}_p}$, since:

Local Kronecker Weber Thm: $\mathbb{Q}_p^{ab} = \mathbb{Q}_p^{cycl}$

Proof Let $K/\mathbb{Q}_p$ be fin. abel.; need to show $K \subset \mathbb{Q}_p^{cycl}$.

(1) **K unramified** Then $K \subset \mathbb{Q}_p^{ur} = \bigcup_{(n,p)=1} \mathbb{Q}_p(\zeta_n) \subset \mathbb{Q}_p^{cycl}$.

(2) **Enough to consider $K/\mathbb{Q}_p$ totally ramified**

Let m = exponent of $G = Gal(K/\mathbb{Q}_p)$ (i.e. $g^m = 1 \ \forall g \in G$)

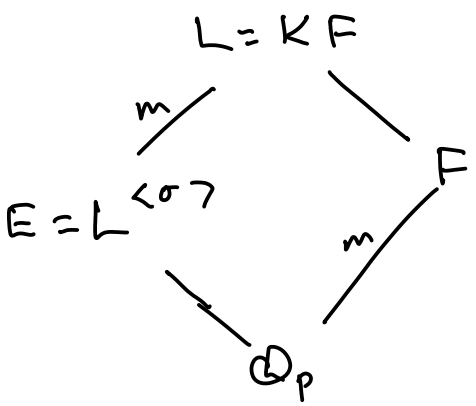
Let F = unram. ext of $\mathbb{Q}_p$ of degree m $\left(= \mathbb{Q}_p(\zeta_{p^m-1})\right)$

$L = KF$. Then

$$G' = Gal(L/\mathbb{Q}_p) \subset G_1 \times \underbrace{Gal(F/\mathbb{Q}_p)}_{\wr \ \mathbb{Z}/m\mathbb{Z}}$$

so G' has exponent m too.

$Gal(F/\mathbb{Q}_p) = \langle Fr_{F/\mathbb{Q}_p} \rangle$; let $\sigma \in G'$ be any elt. s.t. $\sigma|_F = Fr_{F/\mathbb{Q}_p}$. As G' has exponent m, σ has order m. Let $E = L^{\langle \sigma \rangle}$. Diagram:



Now F = max! unr. subfield of L,

And $F \cap E = F^{\langle \sigma \rangle} = \mathbb{Q}_p$ so

$E/\mathbb{Q}_p$ is tot. ram, and $EF = L$.

As F is cyclotomic, STP that E is.

(3) $K/\mathbb{Q}_p$ totally ram. abelian of degree n, $(n,p)=1$

$\Rightarrow$ K cyclotomic.

Proof: $G = Gal(K/\mathbb{Q}_p) = I(K/\mathbb{Q}_p)$. As $K/\mathbb{Q}_p$ is tamely ram,

(9)

the character $\Theta_0 : G \hookrightarrow k_K^* = \mathbb{F}_p^*$. So G is cyclic of order $n \mid p-1$. Now $\mu_{p-1} \subset \mathbb{Q}_p$, so by Kummer theory,

$$K = \mathbb{Q}_p(\sqrt[n]{x}) \quad \text{some } x \in \mathbb{Q}_p^* \qquad x = p^b \cdot u \text{ say } u \in \mathbb{Z}_p^*$$

$$\subset \underbrace{\mathbb{Q}_p(p^{-1}\sqrt{-p})}_{\| \; \mathbb{Q}_p(p\sqrt{-1})}\left(p^{-1}\sqrt{-1}, p^{-1}\sqrt{u}\right)$$

unramified so cyclotomic.

So if $K/\mathbb{Q}_p$ is abelian, $G = Gal(K/\mathbb{Q}_p) = G_1 \times G_2$ $(\#G_1, p) = 1$, $\#G_2 = p^m$. $K = K_1 K_2$ $K_1 = K^{G_2}$, $K_2 = K^{G_1}$ and $Gal(K_i/\mathbb{Q}_p) = G_i$. So K_1 is cyclotomic, and STP that K_2 is

From here on, $p \neq 2$!

(4) Enough to prove that $\nexists$ abelian $K/\mathbb{Q}_p$ with

$$Gal(K/\mathbb{Q}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^3$$

Proof. Let $\mathbb{Q}_p^{ab,p}$ = max! abelian p-extn of $\mathbb{Q}_p$

= $\cup$ of all abel. extns of p-power order.

$$\mathbb{Q}_p^{cyd,p} = \mathbb{Q}_p^{ab,p} \cap \mathbb{Q}_p^{cyd} = \mathbb{Q}_p^{nr,p} \cdot \mathbb{Q}_p^{ram,p}$$

$$\mathbb{Q}_p^{nr,p} = \bigcup_{n \geq 1} (\text{unram. extns of deg. } \nmid p^n) \; ; \; Gal(\mathbb{Q}_p^{nr,p}/\mathbb{Q}_p) = \mathbb{Z}_p.$$

$$\mathbb{Q}_p^{ram,p} = \mathbb{Q}_p^{ab,p} \cap \mathbb{Q}_p(\zeta_{p^\infty}) = \bigcup_n \mathbb{Q}_p(\zeta_{p^n})$$

$$Gal(\mathbb{Q}_p(\zeta_{p^n})/\mathbb{Q}_p) \supset \triangle$$

$$\| \qquad\qquad \|$$

$$(\mathbb{Z}/p^n\mathbb{Z})^* \cong \mathbb{Z}/p^{n-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}. \qquad \mathbb{Z}/(p-1)\mathbb{Z}$$

So $Gal(\mathbb{Q}_p^{cycl,p}/\mathbb{Q}_p) \simeq \mathbb{Z}_p \times \mathbb{Z}_p$

Inclusion $\mathbb{Q}_p^{cycl} \subset \mathbb{Q}_p^{ab}$ gives surjection

$$\Gamma = Gal(\mathbb{Q}_p^{ab,p}/\mathbb{Q}_p) \twoheadrightarrow \Gamma_{cycl} = Gal(\mathbb{Q}_p^{cycl,p}/\mathbb{Q}_p) \simeq \mathbb{Z}_p^2$$

which need to show is <u>isom</u>.

Both sides are abelian <u>pro-p groups</u> (inverse limit of finite abel. p-groups)
(in particular, they are $\mathbb{Z}_p$-modules).

Suppose $\Gamma/\Gamma^p \xrightarrow{\sim} \Gamma_{cycl}/\Gamma_{cycl}^p \simeq (\mathbb{Z}/p\mathbb{Z})^2$ (*)

The easy argument shows $\Gamma/\Gamma^{p^n} \xrightarrow{\sim} \Gamma_{cycl}/\Gamma_{cycl}^{p^n} = (\mathbb{Z}/p^n\mathbb{Z})^2$
$\forall n \Rightarrow \Gamma \xrightarrow{\sim} \Gamma_{cycl}$.

[Details: let $x, y \in \Gamma$ map to the generators of Γ_{cycl} (as $\mathbb{Z}_p$-module). Let $n > 1$, $M_n = \Gamma/\Gamma^{p^n}$, a $\mathbb{Z}/p^n\mathbb{Z}$-module. Then x, y generate M by Nakayama's lemma, and so for every n,

$$\Gamma/\Gamma^{p^n} \xrightarrow{\sim} \Gamma_{cycl}/\Gamma_{cycl}^{p^n}$$

and $\Gamma = \varprojlim \Gamma/\Gamma^{p^n}$, also Γ_{cycl}.]

So enough to show (*). But Γ/Γ^p = Galois gp. of maximal abel. ext^n of $\mathbb{Q}_p$ of exponent p, and to show this $\simeq (\mathbb{Z}/p\mathbb{Z})^2$, enough to show $\nexists$ a $(\mathbb{Z}/p\mathbb{Z})^3$-ext^n of $\mathbb{Q}_p$.

(5) Last (and deepest) step. There are 2 ways to do this:

(a) ramification theory (b) Kummer theory.

– of these, (a) is shorter, (b) generalises more easily. (and uses much less number theory.)

Method (a). As $\exists!$ unramified extension of $\mathbb{Q}_p$ of degree p, enough to show: $\nexists K/\mathbb{Q}_p$ totally ramified, Galois with group $\cong (\mathbb{Z}/p\mathbb{Z})^2$. We need these facts (from lectures & ex. sheet 2):-

L/K totally ram $\Rightarrow \mathcal{O}_L = \mathcal{O}_K[\pi_L]$, $g(\pi_L) = 0$ and then

- $\mathfrak{D}_{L/K} = (g'(\pi_L)) = (e\pi_L^{e-1} + \dots)$
- $e-1 \leq \delta_{L/K} = v_L(\mathfrak{D}_{L/K}) \leq e-1+v_L(e)$ (i)
  $\uparrow$ $<$ if $p \mid e$
- $\delta_{L/K} = \sum_{i \geq 0} (\#G_i - 1)$, $G_i = G_i(L/K)$ (ii)
  ramif. groups.
  if L/K Galois.

So if L/K cyclic of degree p, ramified, let k be the "gap" in the (G_i):-

$\mathbb{Z}/p\mathbb{Z} \simeq G = Gal(L/K) = G_0 = G_1 \dots = G_k$, $G_{k+1} = \{1\}$
$\uparrow$ (as L/K is wildly ramified)

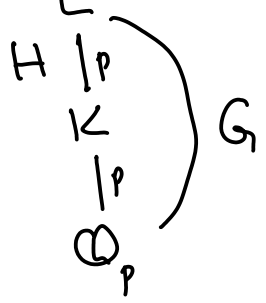
Then $\delta_{L/K} \overset{(ii)}{=} (p-1)(k+1) \leq p-1+v_L(p)$ by (i)
$= p-1+p.e(K/\mathbb{Q}_p)$

$\Rightarrow 1 \leq k \leq \frac{p}{p-1} e(K/\mathbb{Q}_p)$

(12)

Now suppose $L/\mathbb{Q}_p$ is Galois, totally ramified, degree p^2. RTP then $G = Gal(L/\mathbb{Q}_p)$ is cyclic.

Let $H \subset G$ be a subgp of order p, $K = L^H$.



By above, for $K/\mathbb{Q}_p$ we have $1 \le k \le \frac{p}{p-1}$

ie. $k=1$, so $\delta_{K/\mathbb{Q}_p} = 2(p-1)$

For L/K, $\delta_{L/K} = (p-1)(k+1)$ where

$1 \le k \le \frac{p^2}{p-1}$ ie. $1 \le k \le p+1$.

$\therefore \delta_{L/\mathbb{Q}_p} = \delta_{L/K} + e(L/K)\delta_{K/\mathbb{Q}_p} = (p-1)(k+1) + 2p(p-1)$

$= (p-1)(2p+k+1)$

Now each $G_i/G_{i+1} \xrightarrow[\theta_i]{} m_L^{i-1}/m_L^i \cong k_L \cong \mathbb{F}_p$

so $\exists\, i<j$ s.t.

$$G = G_0 = G_1 = G_i \supsetneq G_{i+1} = G_j \supsetneq G_{j+1} = \{1\}.$$

and so $\delta_{L/\mathbb{Q}_p} = (i+1)(p^2-i) + (j-i)(p-1)$ by (ii).

ie. $(i+1)(p+1) + (j-i) = 2p+k+1 \le 3p+2$

As $i \ge 1$ HD forces $i=1$, $j = k \ge 2$

So $H = H_2$ and G_2 both have order p.

But $H_2 = H \cap G_2$ so must have $H = G_2$

I.e. H is unique! so G must be cyclic. $\square$

(5) Kummer theory

F a field, $n>1$ prime to $\mathrm{char}(F)$, and $\mu_n \subset F$.
Then any abel. extn of F of exponent $|n$ is obtained by extracting n^{th} roots. Precisely: let $G_F = \mathrm{Gal}(\bar{F}/F)$.

Then $\exists$ canonical $\cong$ $F^\times/(F^\times)^n \xrightarrow{\sim} \mathrm{Hom}(G_F, \mu_n)$

(Hom = continuous homomorphisms)

$$\begin{array}{ccc} x & \overset{\psi}{\mapsto} & \psi_x \\ \bmod (F^\times)^n & & \left(\sigma \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}\right) \end{array}$$

If $F = E(\zeta_n)$ for some E then
$\gamma \in \Delta = \mathrm{Gal}(F/E)$ acts on both sides: on $F^\times$ by Galois action; and on $\varphi \in \mathrm{Hom}(G_F, \mu_n)$ by

$$\gamma\varphi : \sigma \longmapsto \gamma(\varphi(\tilde{\gamma}^{-1}\sigma\tilde{\gamma}))$$

where $\tilde{\gamma} \in \mathrm{Gal}(\bar{F}/E) \longmapsto \gamma \in \mathrm{Gal}(F/E)$.

Lemma Suppose n is prime (or more generally that $(n, \varphi(n)) = 1$).
Then

$$\mathrm{Hom}(G_E, \mathbb{Z}/n\mathbb{Z}) = \mathrm{Hom}_\Delta(\mu_n, F^\times/(F^\times)^n)$$
$$= \{f : \mu_n \to F^\times/(F^\times)^n \text{ commuting with } \Delta\}.$$

Pf. $\mathrm{Hom}(G_F, \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Hom}(\mu_n, F^\times/(F^\times)^n)$
by the above, so STP

$$\mathrm{Hom}(G_E, \mathbb{Z}/n\mathbb{Z}) \xrightarrow{\sim} \mathrm{Hom}_\Delta(G_F, \mathbb{Z}/n\mathbb{Z}).$$

More generally, if G is a gp, H a normal subgp of finite index, then $\forall n>1$, G acts on $\mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z})$ by conjugation:

$f: G \to \mathbb{Z}/n\mathbb{Z}$, $\gamma \in G$

$\rightsquigarrow {}^{\gamma}f: G \to \mathbb{Z}/n\mathbb{Z}$, $({}^{\gamma}f)(g) = f(\gamma^{-1}g\gamma)$

and H acts trivially since if $\gamma \in H$,

$f(\gamma^{-1}g\gamma) = f(\gamma^{-1}) + f(g) + f(\gamma) = f(g)$.

So $\exists$ natural map

$$\mathrm{Hom}(G, \mathbb{Z}/n\mathbb{Z}) \to \mathrm{Hom}(H, \mathbb{Z}/n\mathbb{Z})^{G/H}$$

which is an isom if n is coprime to $(G:H) = d$.

[Proof: If $f: G \to \mathbb{Z}/n\mathbb{Z}$ and $f(H) = 0$, let $g \in G$.
Then $g^d \in H$ so $0 = f(g^d) = d f(g) \Rightarrow f(g) = 0$ as $(n, d) = 1$.

So map is injective. Now let $f: H \to \mathbb{Z}/n\mathbb{Z}$ be invariant under conjugation by G. Let $e = d^{-1} \pmod n$ and extend f to $\tilde{f}: G \to \mathbb{Z}/n\mathbb{Z}$ by $\tilde{f}(g) = e \cdot f(g^d)$.
Easy to check $\tilde{f}$ is a hom, hence map is surjective.]

Now let $E = \mathbb{Q}_p$. Then

$\mathrm{Hom}(\Gamma/\Gamma^p, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G_{\mathbb{Q}_p}, \mathbb{Z}/p\mathbb{Z})$ in earlier notn

$= \mathrm{Hom}_{\Delta}(\mu_p, K^*/(K^*)^p)$ $\quad K = \mathbb{Q}_p(\zeta_p)$.

We have $1 \to \mathcal{O}_K^*/(\mathcal{O}_K^*)^p \to K^*/(K^*)^p \xrightarrow{v_K} \mathbb{Z}/p\mathbb{Z} \to 0$

$\wr$

$(1+\pi_K)^*/(1+\pi_K)^p$ as $\dfrac{\mathcal{O}_K^*}{1+\pi_K} = k_K^*$ has order prime to p.

and here are no nonzero Δ-hom $\mu_p \to \mathbb{Z}/p\mathbb{Z}$.

$\Rightarrow \mathrm{Hom}(\Gamma/\Gamma^p, \mathbb{Z}/p\mathbb{Z}) \cong (1+\mathfrak{m}_K)^\times / (1+\mathfrak{m}_K)^p$.

Lemma: $(1+\mathfrak{m}_K)^\times$ is the product of $(1+\mathfrak{m}_K)^\times_{\text{tors}} = \mu_p$ and a free $\mathbb{Z}_p[\Delta]$-module of rk 1.

Pf. (This works for any Galois ext K/F of degree prime to p in place of $K/\mathbb{Q}_p$).

Normal basis thm $\Rightarrow \exists x \in K$ with $K = \mathcal{O}_p[\Delta].x$

WLOG, $x \in p\mathcal{O}_K$. Let $\Lambda = \mathbb{Z}_p[\Delta]x$, a free rk 1 $\mathbb{Z}_p[\Delta]$-submodule of $p\mathcal{O}_K$.

Then $\exp(\Lambda) \subset 1+\mathfrak{m}_K$ is a free rk 1 $\mathbb{Z}_p[\Delta]$-submodule of $1+\mathfrak{m}_K$ of finite index.

But $\mathbb{Z}_p[\Delta] = \mathbb{Z}_p[T]/(T^p-1) \cong \dfrac{\mathbb{Z}_p[T]}{(T-1)} \times \dfrac{\mathbb{Z}_p[T]}{(\Phi_p(T))}$

as $(T-1, \Phi_p(T)) = \mathbb{Z}_p[T]$. $\quad \cong \mathbb{Z}_p \times \mathbb{Z}_p[\zeta_p]$.

and both $\mathbb{Z}_p$, $\mathbb{Z}_p[\zeta_p]$ are PIDs. It follows that

$(1+\mathfrak{m}_K)^\times = (1+\mathfrak{m}_K)^\times_{\text{tors}} \oplus$ (free module of rk 1). $\square$

We are now finished, since we have

$\mathrm{Hom}(\Gamma/\Gamma^p, \mathbb{Z}/p\mathbb{Z}) \cong \mathrm{Hom}_\Delta(\mu_p, \mu_p \oplus \mathbb{F}_p[\Delta])$

and $\dim_{\mathbb{F}_p} \mathrm{Hom}_\Delta(\mu_p, \mathbb{F}_p[\Delta]) = 1$ by character theory of finite ab. gps.

$\Rightarrow \dim_{\mathbb{F}_p}(\Gamma/\Gamma^p) = 2$ as required.

Case $p=2$. Now $\mathbb{Z}_2^* = \{\pm 1\} \times (1+4\mathbb{Z}_2)^*$, $(1+4\mathbb{Z}_2)^* \cong \mathbb{Z}_2$

So $\mathbb{Q}_2^* \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$, and so

- $\Gamma_2^{cycl} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2$

- $\Gamma_2/2\Gamma_2 \simeq \mathrm{Hom}(\mathbb{Q}_2^*/(\text{squares}), \mathbb{Z}/2\mathbb{Z})$ (by Kummer theory)
$\simeq (\mathbb{Z}/2\mathbb{Z})^3$.

So $\Gamma_2/2\Gamma_2 \simeq \Gamma_2^{cycl}/2\Gamma_2^{cycl}$. Same argument as for $p \neq 2$ then implies that as a $\mathbb{Z}_2$-module Γ_2 can be generated by 3 elements. So as

$\Gamma_2 \twoheadrightarrow \Gamma_2^{cycl}$, have $\Gamma_2 \simeq \begin{cases} \mathbb{Z}_2^3 & \text{or} \\ \mathbb{Z}/2^m\mathbb{Z} \times \mathbb{Z}_2^2, & \text{some } m \geq 1. \end{cases}$

We need to show $\Gamma_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2$, so it's enough to show:

Lemma $\exists\, K/\mathbb{Q}_2$ quadratic which is not contained in any cyclic quartic extension $L/\mathbb{Q}_2$.

Proof. Take $K = \mathbb{Q}_2(i)$, $i^2 = -1$. If $L \supset K$ is a cyclic quartic extension, then $L = K(\Theta)$, $\Theta^2 = x = a+bi \in K$.

$L/\mathbb{Q}_2$ Galois $\Rightarrow L = K(\sqrt{x'})$, $x' = a-bi$, hence $x'/x = y^2$, $y = c+di \in K$. Let $\mathrm{Gal}(L/\mathbb{Q}_2) = \langle \sigma \rangle$, $\sigma^4 = 1$. Then $\mathrm{Gal}(L/K) = \langle \sigma^2 \rangle$ so $\sigma^2(\Theta) = -\Theta$. The other conjugates of Θ are $\pm\sqrt{x'}$, so (replacing σ by σ^{-1} if nec.) $\sigma(\Theta) = \sqrt{x'}$ and $\sigma\Theta/\Theta = \pm y$. But then $-1 = \sigma^2(\Theta)/\Theta = \sigma(y).y = c^2+d^2$, and it's easy to see that $c^2+d^2 = -1$ has no solution in $\mathbb{Q}_2$. $\square$

(17) Now show $\mathrm{Art}_K(K^*) \subset \mathrm{Gal}(K^{ab}/K)$ is dense.

Rem. If $\mathrm{Art}_{L/K}$ is surjective $\forall$ cyclic L, then it is surjective for every abelian L/K.

(If $\mathrm{Art}_{L/K}(K^*) = H \subsetneq G = \mathrm{Gal}(L/K)$ then let $H \subset H' \subsetneq G$ with G/H' cyclic, $F = L^{H'}$. Then $\mathrm{Art}_{F/K}(K)^* = \{1\}$.)

So STP $\mathrm{Art}_{L/K}$ is surjective for L/K cyclic.

Consider now

$$\begin{array}{ccc} E^\times & \xrightarrow[\mathrm{Art}_{EL/E}]{} & \mathrm{Gal}(EL/E) \\ {\scriptstyle N_{E/K}}\downarrow & & \downarrow{\scriptstyle \text{restr.}} \\ K^\times & \xrightarrow[\mathrm{Art}_{L/K}]{} & \mathrm{Gal}(E/K) \end{array}$$

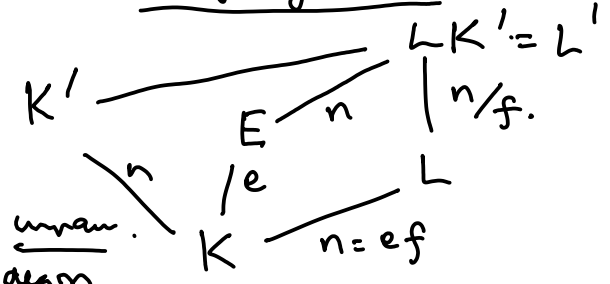
Claim $\exists E/K$ s.t. 1) $E \cap L = K$, so $\mathrm{Gal}(EL/E) \xrightarrow[\text{restr}]{\sim} \mathrm{Gal}(L/K)$

2) EL/E is unramified.

$\Rightarrow \mathrm{Art}_{EL/E}$ is surjective by property (i).

$\therefore \mathrm{Art}_{L/K}$ is surjective.

Proof of claim. As in step (2) above:



$L' \cap K^{ur} = K'$

& $\exists E \subset L'$ s.t.

- E/K is tot. ramified (i.e. $E \cap K' = K$)
- $E \cap L = K$
- $L' = E.L$

Let $L_0 = L \cap K' = L \cap K^{ur}$.

$$\mathrm{Gal}(L'/K) \xrightarrow{\sim} \left\{ (\sigma, \tau) \in \mathrm{Gal}(L/K) \times \mathrm{Gal}(K'/K) \;\middle|\; \sigma|_{L_0} = \tau|_{L_0} \right\}$$

Let $\gamma \in \mathrm{Gal}(F'/K)$ s.t. $\gamma \mapsto (\sigma, \mathrm{Fr}_{K'/K})$ where $\langle\sigma\rangle = \mathrm{Gal}(F/K)$.

Then $E = L'^{\langle\gamma\rangle}$ does the trick. (exists as $\mathrm{Gal}(L/K) \cong \mathbb{Z}/n \cong \mathrm{Gal}(F/K)$)

L.III

Lubin-Tate theory.

The ramified part of $\mathbb{Q}_p^{ab}$ is covered by the p-power cyclo. ext.

$$\mathbb{Q}_p(\mu_{p^\infty}) = \bigcup_n \mathbb{Q}_p(\zeta_{p^n}).$$

$$= \bigcup_n \mathbb{Q}_p(\pi_n) \quad \pi_n = \zeta_{p^n} - 1$$

Consider the polynomial

$$f(X) = (X+1)^p - 1 = X^p + \sum_{i=1}^{p-1} \binom{p}{i} X^i.$$

Then $f(\pi_{n+1}) = \pi_n$, $f(\pi_1) = 0$ so $\mathbb{Q}_p(\mu_{p^\infty})$ is generated by the roots of the iterates

$$f^{(n)} := \underbrace{f \circ \dots \circ f}_{n} = f(f(\dots(f(X))\dots)).$$

which form a group under the law

$$X \boxplus Y = (X+1)(Y+1) - 1 = X + Y + XY.$$

Amazingly, for any $K/\mathbb{Q}$, there is a group structure on the roots of the iterate $f_\pi^{(n)}$, where $f_\pi = X^q + \pi X$ (actually many other choices would do). The roots of $f_\pi^{(n)}$ all have $|\cdot|_p < 1$, and the group law is given by a power series

$$X \boxplus Y = F(X,Y) = X + Y + \dots \in \mathcal{O}_K[[X,Y]]$$

(converges for X, Y in $\overline{K}$ with $|\cdot| < 1$).

Def^n. A <u>formal gp law</u> over a ring R is a power series $F(X,Y) \in R[[X,Y]]$ s.t. :-

i) $F(X,Y) = X + Y +$ (terms of degree ≥ 2)

ii) $F(X,Y) = F(Y,X)$

iii) $F(X,0) = X$

iv) $F(X, F(Y,Z)) = F(F(X,Y),Z)$

v) $\exists\ I(X) \in R[[X]]$, $I(X) = -X + (\deg \geq 2)$ s.t. $F(X, I(X)) = X$.

Interested in case $R = \mathcal{O}_K$. Then if $x, y \in \mathfrak{m}_K$,

i) implies that $F(x,y)$ cvgs to an elt. of $\mathfrak{m}_K$ (since K is complete) and the other axioms

$\Rightarrow$ $\mathfrak{m}_K$ together with $x +_F y := F(x,y)$ defines an abelian gp.

Of course, we for every finite L/K, F defines a gp str. on $\mathfrak{m}_L$, hence on $\mathfrak{m}_{\bar{K}} = \bigcup_L \mathfrak{m}_L$ (NB $\bar{K}$ not complete!).

Ex. (1) $F(X,Y) = X + Y$. (<u>additive</u> formal gp. law)

$(\mathfrak{m}_{\bar{K}}, +_F) = (\mathfrak{m}_{\bar{K}}, +)$

(2) $F(X,Y) = X + Y + XY$ (<u>multiplicative</u> f.g.l.)

$(\mathfrak{m}_{\bar{K}}, +_F) \simeq (1 + \mathfrak{m}_{\bar{K}}, \times)$ $(x \mapsto 1+x)$

Rem: actually (iii), (v) are consequences of over 3 axioms.

Suppose F is a f.g.l.a.u/$\mathcal{O}_K$.

$\forall n \in \mathbb{Z}$ have power series $[n](X)$

defined inductively by $[n+1](X) = F(X, [n](X))$

$$[0](X) = 0.$$

and $[n](X) = \underbrace{X +_F \cdots +_F X}_{n}$ if $x \in \mathfrak{m}_K$.

See easily that $[n](X) = nX + (\deg \geq 2)$,

and $[n]$ is a formal gp homomorphism:

If F, G are formal gp. laws, a homomorphism $F \to G$ is a power series $\varphi \in R[[X]]$, $\varphi(0) = 0$ with

$$F(\varphi(X), \varphi(Y)) = \varphi(F(X, Y)).$$

First novel feature of formal gp laws:-

Lemma Let $a \in \mathbb{Z}_p$. Then $\exists!\ [a](X) \in \mathcal{O}_K[[X]]$

s.t. (1) $[a](X) = aX + (\deg \geq 2)$

(2) $F([a](X), [a](Y)) = [a](F(X, Y))$

(i.e. $[a]$ is an endomorphism of F).

Ex. $F = X + Y + XY$: $[a](X) = (1+X)^a - 1$.

Pf. is elementary: write $[a](X) = aX + \sum_{r \geq 2} c_r X^r$

and use (2) to determine c_r in terms of $a, c_2, \ldots c_{r-1}$

In particular, if φ is an endo. of f.g. law F (or more generally, any hom of f.g. laws /R, domain of dim. 0) and $\varphi \equiv 0 \bmod X^2$, then $\varphi = 0$

Lubin-Tate gp laws. Let $f \in \mathcal{O}_K[[X]]$ s.t.

$$\cdot\ f \equiv X^q \pmod{\pi} \qquad \cdot\ f \equiv \pi X \bmod (X^2) \qquad (*)$$

Exs: $\cdot\ K = \mathbb{Q}_p$, $f = (X+1)^p - 1$

$\cdot\ f = X^q + \pi X$

Thm. (i) $\exists!$ formal gp. law $F_f \in \mathcal{O}_K[[X, Y]]$

s.t. f is an endomorphism of F_f

(ii) $\exists!$ ring hom $\mathcal{O}_K \hookrightarrow \mathrm{End}(F_f)$, $a \mapsto [a]$

such that $[a]_f \equiv aX \bmod X^2$

(In particular, $[\pi]_f = f$.)

F_f is called the Lubin-Tate formal gp law assoc. to f.

It is indep. on f in the following sense: let g be another power series satisfying $(*)$ (for the same choice of π!). Then $\exists!$ isom.

$$\varphi : F_f \xrightarrow{\sim} F_g$$

such that $\varphi \circ f = g \circ \varphi$.

So we can assume f monic poly., or even $f = X^q + \pi X$.

The action of $\mathcal{O}_F$ makes $(\mathfrak{m}_{\bar{K}}, +_{F_f})$ an $\mathcal{O}_K$-module.

Torsion points of a Lubin-Tate group.

Let $f^{(n)} = \underbrace{f \circ \dots \circ f}_{n}$ be the n^{th} iterate of f.

Then $[\pi^n]_f = f^{(n)}$.

Def° $W_{n,f} = \{ x \in \mathfrak{m}_{\bar{K}} \mid f^{(n)}(x) = 0 \}$.

$\exists$ a subgroup of $(\mathfrak{m}_{\bar{K}}, +_{F_f})$, even an $\mathcal{O}_K$-submodule.

$K_{\pi,n} = K(\{x \in W_{n,f}\}) =$ splitting field of $f^{(n)}$.

$K_{\pi,\infty} = \bigcup_n K_{\pi,n}$.

Thm. i) $K_{\pi,n}$ is abelian, totally ramified.

ii) $\exists$ isomorphism $\mathcal{O}_K^* \xrightarrow{\sim} \mathrm{Gal}(K_{\pi,\infty}/K)$, $a \mapsto \sigma_a$

such that $\forall x \in W_{n,f}$, $\sigma_a(x) = [a]_f(x)$

iii) $K^{ab} = K^{ur} \cdot K_{\pi,\infty}$

Granted this thm, we obtain the Artin map

$$\mathrm{Art}_K : K^* \longrightarrow \mathrm{Gal}(K^{ab}/K)$$
$$\| $$
$$\mathrm{Gal}(K^{ur}/K) \times \mathrm{Gal}(K_{\pi,\infty}/K)$$

$$\pi^n \cdot a \longmapsto (\mathrm{Frob}_{K^{ur}/K}^n, \sigma_a)$$

$a \in \mathcal{O}_K^*$ just as for $\mathbb{Q}_p$.

Proof Let $W_{f,n}^* = W_{f,n} \setminus W_{f,n-1}$

$$\left(= W_{f,1} \setminus \{0\} \text{ if } n=1 \right).$$

As $[\pi]_f : W_{f,n} \to W_{f,n-1}$, $K_{\pi,n} = K(W_{f,n}^*)$.

Let $\Phi_{\pi,n} = f^{(n)} / f^{(n-1)} = \left(\frac{f}{x}\right) \circ f \circ \dots \circ f$

– has degree $q^{n-1}(q-1)$, and is Eisenstein, hence irreducible.

Let $\pi_n \in W_{f,n}^*$ be a root of $\Phi_{\pi,n}$. Then $\forall a \in \mathcal{O}_K^*$, $[a]_f(\pi_n) \in W_{f,n}^*$, and $[a]_f(\pi_n) = (\pi_n)$

$\Leftrightarrow [a-1]_f(\pi_n) = 0 \Leftrightarrow a-1 \in \pi^n \mathcal{O}_K$. So as

$\# W_{f,n}^* = q^{n-1}(q-1) = \left(\mathcal{O}_K^* : 1+\mathfrak{m}_K^n\right)$,

$$W_{\pi,n}^* = \left(\mathcal{O}_K^* / 1+\mathfrak{m}_K^n\right).\pi_n$$

The action of $G_n = \mathrm{Gal}(K_{\pi,n}/K)$ on $W_{\pi,n}^*$ commutes with action of $\mathcal{O}_K^*$, since $[a]_f \in K[[X]]$.

So have inj $G_n \hookrightarrow \mathcal{O}_K^* / (1+\mathfrak{m}_K^n)$

+ as $\# G_n = [K_{\pi,n} : K] \geq [K(\pi_n) : K] = q^{n-1}(q-1)$

this an isomorphism. So $K_{\pi,n} = K(\pi_n)$ and as $\Phi_{f,n}$ is Eisenstein, it is totally ramified.

This proves (i) – (ii), so have Artin map

$$\mathrm{Art}_K^\pi : K^* \longrightarrow \mathrm{Gal}(K^{LT}/K), \quad K^{LT} = K^{nr} K_{\pi,\infty}$$

(a priori depends on π)

To prove part (iii), we either ramification theory (Hasse-Arf theorem - hard!) or can give more elementary proof using Kummer theory.

Finally we want a pf. of existence of L-T gps - purely elementary construction of power series term by term. (See eg. Serre's article in Cassels-Fröhlich §3.5).

L IV. Although Lubin-Tate theory gives a single relatively explicit proof of the basic theorems of local CfT, there is another approach, using cohomology, which it's important to know about.

Recall that if G is a group & A is a G-module (an abelian gp. on which G acts by automorphisms) there are defined cohomology groups $H^n(G,A)$ $(n \geq 0)$ which are abelian groups

Among their many properties:

1) $H^0(G,A) = A^G = \{a \in A \mid \forall g \in G,\ g(a) = a\}$

2) $H^1(G,A) = \dfrac{\{\text{maps } G \to A,\ g \mapsto a_g \text{ such that } a_{gh} = a_g + g(a_h)\}}{\{\text{maps of form } g \mapsto g(b) - b, \text{ some } b \in A\}}$.

Especially, if G acts freely on A, $H^1(G,A) = \mathrm{Hom}_{\mathrm{groups}}(G,A)$.

3) If $A \to B$ is a G-module map, there is an induced map $H^n(G,A) \to H^n(G,B)$, compatible with composition (so $H^n(G,-)$ are functors).

4) If $0 \to A \to B \to C \to 0$ is an exact sequence of G-modules then $\forall n \geq 0$ $\exists$ connecting homomorphisms

$$\delta_n : H^n(G,C) \to H^{n+1}(G,A)$$

making the following a long exact sequence:

$$0 \to H^0(G,A) \to H^0(G,B) \to H^0(G,C) \xrightarrow{\delta_0}$$
$$H^1(G,A) \to H^1(G,B) \to \cdots\cdots$$

5) If $A \times B \to C$ is a bilinear G-map, there is, for every $m,n \geq 0$, a bilinear cup-product map

$$\cup : H^m(G,A) \times H^n(G,B) \to H^{m+n}(G,C).$$

6) If $G \twoheadrightarrow G' = G/H$ is a surjection, then there are maps

$$i_{G,G'} : H^n(G', A^H) \to H^n(G,A)$$

(note that if A is a G-module then A^H is a G'-module).

If now G is a profinite group (especially: $G = \mathrm{Gal}(\bar{K}/K)$ for some field K) say A is a discrete G-module if, $\forall a \in A$, the stabiliser of a in G is open. Equivalently,

$$A = \bigcup_{G \supset H \text{ open}} A^H.$$

We may define the (continuous) cohomology groups of G with coefficients in A as

$$H^n(G, A) = \varinjlim_{H \text{ open} \lhd G} H^n(G/H, A^H)$$

Now let K be a field, $G_K = \mathrm{Gal}(\bar{K}/K)$. The cohomology groups $H^n(G_K, A)$ are called Galois cohomology groups.

The groups $H^n(G_K, \bar{K}^*)$ are particularly interesting.

$H^0(G_K, \bar{K}^*) = K^*$ (by Galois theory).

For any field, $H^1(G_K, \bar{K}^*) = \{1\}$ "Hilbert's Thm. 90"

which is the heart of the proof that if $\zeta_n \in K$ then every cyclic extn of K of degree dividing n is of the form $K(\sqrt[n]{a})$: consider the sequence

$$1 \longrightarrow \mu_n = \langle \zeta_n \rangle \longrightarrow \bar{K}^* \xrightarrow{n} \bar{K}^* \longrightarrow 1$$

and take cohomology to get:

$$1 \to K^*/(K^*)^n \to H^1(G_K, \mu_n) \to H^1(G_K, \bar{K}^*)$$
$$\| \qquad\qquad\qquad\qquad\qquad\qquad \| \qquad\qquad\qquad\qquad\qquad\qquad \|$$
$$\mathrm{Hom}(G_K, \mu_n) \qquad\qquad\qquad\qquad\qquad\qquad \{1\}$$
$$\text{as } \mu_n \subset K.$$

The group $H^2(G_K, \bar{K}^*) =: \mathrm{Br}(K)$ is called the Brauer group — it is central to class field theory (local and global).

Thm If $K/\mathbb{Q}_p$ is finite, $\exists$ canonical iso $\mathrm{Br}(K) \simeq \mathbb{Q}/\mathbb{Z}$.

27

[The map δ is actually quite explicit: let $K \subset K^{ur} \subset \bar{K}$ be the max^{l} unramified extension. Then have

a diagram:

$$H^2(\mathrm{Gal}(K^{ur}/K), K^{ur\,*}) \to H^2(G_K, \bar{K}^*)$$

$$\downarrow \text{ induced by } v : K^{ur\,*} \to \mathbb{Z}$$

$$H^2(\mathrm{Gal}(K^{ur}/K), \mathbb{Z})$$

$$\delta \uparrow \text{ induced by exact sequence } (*)$$

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

$$H^1(\mathrm{Gal}(K^{ur}/K), \mathbb{Q}/\mathbb{Z})$$

$$\| $$

$$\mathrm{Hom}_{\text{cts}}(\hat{\mathbb{Z}}, \mathbb{Q}/\mathbb{Z}) \simeq \mathbb{Q}/\mathbb{Z})$$

and one shows all the maps are isomorphisms.]

Granted this, we can construct a pairing

$$K^* \times \mathrm{Hom}_{\text{cts}}(G_K, \mathbb{Q}/\mathbb{Z}) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

(which is equivalent to giving a map $K^* \longrightarrow G_K^{ab}$)

as follows:

$$\mathrm{Hom}(G_K, \mathbb{Q}/\mathbb{Z}) = H^1(G_K, \mathbb{Q}/\mathbb{Z}) \quad \text{(as in } (*) \text{ above)}$$

$$\simeq H^2(G_K, \mathbb{Z})$$

$$K^* = H^0(G_K, \bar{K}^*)$$

and take cup-product:

$$K^* \times \mathrm{Hom}(G_K, \mathbb{Q}/\mathbb{Z}) \longrightarrow H^2(G_K, K^*) \cong \mathbb{Q}/\mathbb{Z}.$$

See Serre's article in Cassels-Fröhlich for a lucid account of this!

One reason why we should care about the cohomological approach is that Galois cohomology groups occur everywhere in modern number theory (eg in Selmer groups of elliptic curves, in Iwasawa theory...) and class field theory gives a handle on them. For example:

$K/\mathbb{Q}_p$ finite, A a finite G_K-module.

Let $A^D = \mathrm{Hom}_{\text{groups}}(A, \bar{K}^\times) = \mathrm{Hom}(A, \mu_N)$ for $N \gg 0$

which is a G_K-module by:

$$f \in A^D : \quad (gf)(a) = g(f(g^{-1}(a)).$$

[so $(A^D)^{G_K} = \{ G_K\text{-homomorphisms } A \to \bar{K}^\times \}$].

Tate duality theorem: For $0 \le n \le 2$, cup-product

$$H^n(G_K, A) \times H^{2-n}(G_K, A^D) \to H^2(G_K, \bar{K}^\times) = \mathbb{Q}/\mathbb{Z}$$

is a perfect pairing of finite abelian groups.

[i.e. the maps $H^n(G_K, A) \to \mathrm{Hom}(H^{2-n}(G_K, A^D), \mathbb{Q}/\mathbb{Z})$

$H^{2-n}(G_K, A^D) \to \mathrm{Hom}(H^n(G_K, A), \mathbb{Q}/\mathbb{Z})$

are isomorphisms. In particular, the 2 groups have the same order, and the same elementary divisors].

Archimedean local fields. Although almost trivial, it is worth pointing out that if $K = \mathbb{R}$ or $\mathbb{C}$ we can define a cts. homomorphism $\mathrm{Art}_K : K^* \longrightarrow G_K^{ab}$: trivial if $K = \mathbb{C}$, and

$$\mathrm{Art}_{\mathbb{R}} : \mathbb{R}^* \longrightarrow G_{\mathbb{R}}^{ab} = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$$

$$x \longmapsto \begin{cases} 1 & \text{if } x > 0 \\ \tau & x < 0. \end{cases}$$

Note that unlike the non-archimedean case, Art_K is surjective and very far from being injective.

Some words about global CFT. K a number field.

The Artin map is a homomorphism

$$C_K = J_K / K^* \xrightarrow{\mathrm{Art}_K} G_K^{ab}.$$

Recall: if $K \subset L$ we $J_K \hookrightarrow J_L$, so can define

$$J_{\bar{K}} = \bigcup_{L/K \text{ finite}} J_L, \quad C_{\bar{K}} = J_{\bar{K}} / \bar{K}^*.$$

The G_K-module $C_{\bar{K}}$ is the global counterpart of the local module K^*. In particular, a lot of global CFT is contained in the fact that

$$\boxed{H^2(G_K, C_{\bar{K}}) \simeq \mathbb{Q}/\mathbb{Z}.}$$

Unlike in local CFT (where one proves $Br(K) \simeq \mathbb{Q}/\mathbb{Z}$ and uses it to construct the Artin map), in the global case one has to prove most of the theory first, and deduce this formula as a consequence.

This is also a global duality theorem (Tate-Poitou) - see Serre's "Cohomologie Galoisienne" or Milne's "Arithmetic Duality Theorems" (Ch. 1)

The kernel of the global Artin map is precisely the maximal connected subgroup C_K° of C_K. This is the closure in C_K of the subgroup

$$\prod_{v \text{ real}} (\mathbb{R}^*_{>0}) \times \prod_{v \text{ complex}} \mathbb{C}^*$$

- which is a closed subgp. of J_K, but not of C_K unless O_K^* is finite ie $K = \mathbb{Q}$ or $\mathbb{Q}(\sqrt{-D})$.

Of course $Art_K(C_K^\circ)$ must be zero, since G_K^{ab} is profinite, hence has no non-trivial connected subgroups. (Or because Art_K is the product of the local Artin maps Art_{K_v} and we know what happens if $K_v \simeq \mathbb{R}$ or $\mathbb{C}$).

It's natural to ask if there is a Galois-theoretic interpretation of all of C_K, not just C_K / C_K°. This seems unlikely at first (because C_K can't be a Galois group) but there is an elegant Galois-theoretic description, using Hecke characters (see Ex. sheet 3, last qn.).

A Hecke character is a cts. hom $C_K \xrightarrow{\psi} \mathbb{C}^*$.

Every cts. hom $G_K \xrightarrow{\chi} \mathbb{C}^*$ (necessarily with finite image) gives a Hecke character ψ by composition with Art_K. But there are lots of other ψ — for example ideles like

$$|-|_{\mathbb{A}} : C_K \longrightarrow \mathbb{R}^*.$$

Suppose $\psi : C_K \longrightarrow \mathbb{C}^*$ is an algebraic Hecke character (see ex. sheet 3 again). Then:

(1) $\exists$ finite $E/\mathbb{Q}$ such that $\forall$ finite v, $\psi_v(K_v^*) \subset E$.

(2) for every finite place λ of E, with $\lambda | \ell$ say, $\exists$ continuous hom

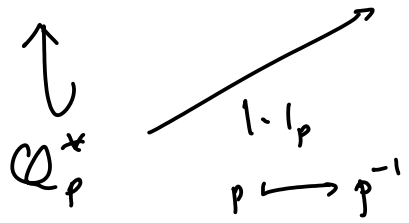
$$\Theta_\lambda : G_K \longrightarrow E_\lambda^* \qquad (E_\lambda = \text{completion, finite ext}^n \text{ of } \mathbb{Q}_\ell)$$

such that for every $v \nmid \ell$,

$$\Theta_\lambda|_{G_{K_v}} \circ \mathrm{Art}_{K_v} = \psi_v.$$

(One can also characterize exactly which Θ occur in this way)

Ex: $K = \mathbb{Q}$, $\psi = |\cdot|_{\mathbb{A}} : J_{\mathbb{Q}} / \mathbb{Q}^* \longrightarrow \mathbb{C}^*$



$l \neq p$: consider the isomorphisms

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{l^n})/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/l^n\mathbb{Z})^*$$

$$(\sigma_a : \zeta \mapsto \zeta^a) \longleftrightarrow a \bmod l^n$$

which fit together to give the <u>cyclotomic character</u>

$$\chi_{cycl} : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_l^* = \varprojlim (\mathbb{Z}/l^n\mathbb{Z})^*$$

The $\chi_{cycl} | G_{\mathbb{Q}_p}$ maps Frob_p to p^{-1}

(Frob_p = geometric Frob, so its image in $\mathrm{Gal}(\mathbb{Q}(\zeta_{l^n})/\mathbb{Q})$ is σ_p^{-1}).

So in this case, $\Theta = \chi_{cycl}$.