Some History:

Kronecker, Weber (1850–1880): explicit class field theory for $\mathbb{Q}$, $\mathbb{Q}(i)$, relevance of complex multiplication.

$$\begin{tikzcd} \mathbb{Q}(\mu_\infty) \arrow[d, dash] \\ \mathbb{Q} \end{tikzcd}$$ ⇝ calculate Gal.

Frobenius, Dedekind (1880): Frobenius element / conjugacy class associated to a prime $\mathfrak{p}$.

Hilbert (1897): first correct proof of Jugendtraum for $\mathbb{Q}$, emphasis on places at ∞, existence of Hilbert class field.

Hensel (1897): introduction of p-adic numbers, took time to catch on.

Takagi (1898–1901 in Göttingen, thesis 1903, proofs of existence theorem during WWI), presented at ICM in 1920

Hasse (1922): local-global theorem.

Chebotarev (~1927): density theorem

E. Artin (1927): Artin map, reciprocity theorem.

Schmidt (1930): local class field theory.

E. Noether (1930s): local proof should exist.

Chevalley (1940): local proof, of local CFT.

Hilbert 1900: Problem 12: extend Kronecker-Weber to any base field.

Still unsolved in explicit form! $\mathbb{Q}(\sqrt{d})$ $d \geq 0$ squarefree remains a mystery.

The bridge: some motivation for local class field theory

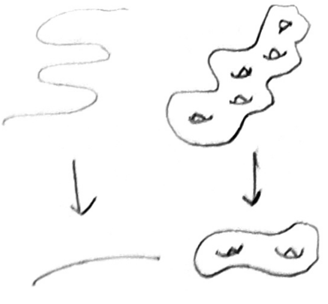
L
$|$
K

want to understand this extension

$\overset{\text{bridge}}{\leftsquigarrow}$

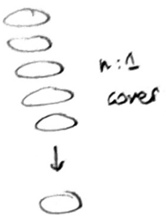
$$\begin{tikzcd} X \arrow[d, "f"] \\ Y \end{tikzcd}$$

dominant map of Riemann surfaces of degree n



Locally in the target, f is very simple

f is smooth at $y \in Y \Rightarrow$ étale $\Rightarrow$



f not smooth at $y \in Y \Rightarrow$

$n = \sum n_i$

f Galois $\Rightarrow$ all n_i are equal.

Moral: f is determined by relatively simple data ("local monodromies") at "ramified points of Y".

Remark:

$\mathbb{C}$
$\cup$

small disc $\leftrightsquigarrow$ $\operatorname{Spec} \mathbb{C}[[t]]$

$\cup$ $\qquad$ $\cup$

puncture disc $\leftrightsquigarrow$ $\operatorname{Spec} \mathbb{C}((t))$

Fact: $\mathbb{C}((t^{\mathbb{Q}})) = \bigcup_{n \geq 1} \mathbb{C}((t^{1/n}))$ is the algebraic closure of $\operatorname{Spec} \mathbb{C}((t))$.

Hence

$$\operatorname{Gal}(\overline{\mathbb{C}((t))}/\mathbb{C}((t))) = \operatorname{Gal}(\mathbb{C}((t^{\mathbb{Q}}))/\mathbb{C}((t))) = \hat{\mathbb{Z}}.$$

This is "why" local monodromy information is so simple.

In language to come: every extension of $\mathbb{Q}((t))$ is "tamely ramified."

Back to number fields:

$$\begin{tikzcd} L \arrow[d, dash, "\text{finite Galois}"] \\ K \end{tikzcd}$$

Fix a place v of K. If v is finite (corr. to $\mathfrak{p} \subset \mathcal{O}_K$) we know what it means for $\mathfrak{q}$ to lie over $\mathfrak{p}$.

(i.e. $\mathfrak{p} \mid \mathfrak{q}$, i.e. $\mathfrak{p}\mathcal{O}_L \subset \mathfrak{q}$).

If v is a real or complex place, corresponding to $K \overset{i}{\hookrightarrow} \mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$.

v' <u>lies over</u> v if corr. i' fits into a diagram

$$\begin{tikzcd} L \arrow[r, hook, "i'"] \arrow[d, dash] & \mathbb{K}' \arrow[d, dash] \\ K \arrow[r, hook, "i"] & \mathbb{K} \end{tikzcd}$$

A real place is <u>ramified</u> if it becomes complex in L.

Fix a place v and a place v' over v. Let K_v (resp. $L_{v'}$) denote the completion of K (resp. L) wrt v, v'.

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

Set $G_v := \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma \text{ acts continuously on } L_{v'}\}$

$$= \{\sigma \mid \sigma \text{ preserves } v'\} = \begin{cases} G_{\mathfrak{q}} & \text{decomposition group if } v \text{ is a finite place} \\ \{1\} & \text{if } v \text{ is infinite unramified} \\ \mathbb{Z}/2\mathbb{Z} & \text{if } v \text{ is infinite, ramified.} \end{cases}$$

(<u>Rmk:</u> in the last case, get $c \in G_v$, "complex conjugation assoc. to ∞ place")

The point: $\begin{tikzcd} L_{v'} \arrow[d, dash] \\ K_v \end{tikzcd}$ is an extension of local fields.

Try to understand these, and then piece them together to understand $\begin{tikzcd} L \arrow[d, dash] \\ K \end{tikzcd}$.

Existence theorem: For any modulus m and any quotient $Cl_K^m \overset{q}{\twoheadrightarrow} Q$ there exists an extension L of K ramified only at primes in the support of m and such that

$$\begin{tikzcd} Cl_K^m \arrow[r, "\text{Artin}"] \arrow[dr, "q"'] & \mathrm{Gal}(L/K) \arrow[d, equal] \\ & Q \end{tikzcd}$$

commutes.

Example: If $m = 0$ then $Cl_K^m = Cl$. Hence there exists $\begin{matrix} L \\ | \\ K \end{matrix}$ unramified everywhere w/ $\mathrm{Gal}(L/K) = Cl_K$. This extension is the Hilbert class field.

Rmk: Back to our counting problems: the finitely many weird primes (ramified) are precisely the primes determining our congruences.

Local class field theory: Between the "easy" case of finite fields and the complicated world of global fields lies the world of local fields.

K: field equipped w/ a discrete valuation $v_K : K \to \mathbb{Z} \cup \{\infty\}$.

ring of integers $\mathcal{O}_K = v^{-1}(\mathbb{Z}_{\geq 0} \cup \{\infty\})$ $\quad k_K := \mathcal{O}_K / m_K$ residue field.

$$\begin{matrix} \mathcal{O}_K = v^{-1}(\mathbb{Z}_{\geq 0} \cup \{\infty\}) \\ \cup \\ m_K = v^{-1}(\mathbb{Z}_{>0} \cup \{\infty\}) \ni \pi \end{matrix}$$ a uniformiser.

For us local field will mean ① K is complete wrt v_K, in other words, K has the topology coming from $\mathcal{O}_K = \varprojlim \mathcal{O}_K / m_K^n$.

② k_K is finite.

Exercise: ① and ② are equivalent to K being locally compact, unless $K = \mathbb{R}$ or $\mathbb{C}$.

E.g.: $\mathbb{Q}_p$ is locally compact, covered by dilates of $\mathbb{Z}_p$.

$$\begin{tikzcd} L \arrow[d, dash] \\ K \end{tikzcd}$$ finite, Galois any elt $\sigma \in \mathrm{Gal}(L/K)$ preserves $\begin{tikzcd} \mathcal{O}_L \arrow[d, dash] \\ \mathcal{O}_K \end{tikzcd}$; $\begin{tikzcd} m_L \arrow[d, dash] \\ m_K \end{tikzcd}$ and hence acts on $\begin{tikzcd} k_L \arrow[d, dash] \\ k_K \end{tikzcd}$.

We get a map

$$\begin{tikzcd} I_{L/K} \arrow[r] & \mathrm{Gal}(L/K) \arrow[r, two heads] & \mathrm{Gal}(k_L/k_K) \arrow[d, phantom, "\parallel"] \\ & & \mathbb{Z}/d\mathbb{Z} \end{tikzcd}$$

inertia subgroup

$\mathbb{Z}/d\mathbb{Z}$, generated by Frobenius.

For $L = \bar{K}$ we get: $$\begin{tikzcd} I_{\bar{K}/K} \arrow[r] & \mathrm{Gal}(\bar{K}/K) \arrow[r, two heads] & \mathrm{Gal}(\bar{k}_K/k_K) \arrow[d, phantom, "\parallel"] \\ & & \hat{\mathbb{Z}} \end{tikzcd}$$.

$$\mathrm{Gal}(\bar{K}/K)^{ab} \twoheadrightarrow \hat{\mathbb{Z}}$$

Local class field theory: There exists a natural homomorphism

$$r_K : K^\times \longrightarrow \mathrm{Gal}(\bar{K}/K)^{ab}$$

with dense image such that r_K induces an isomorphism $\widehat{K^\times} \xrightarrow{\sim} \mathrm{Gal}(\bar{K}/K)^{ab}$

$\uparrow$

completion wrt subgroups of finite index, profinite completion.

Moreover:

① $$\begin{tikzcd} I^{ab}_{\bar{K}/K} \arrow[r, hook] & \mathrm{Gal}(\bar{K}/K)^{ab} \arrow[r, two heads] & \mathrm{Gal}(\bar{k}_K/k_K) \\ \mathcal{O}_K^\times \arrow[u] \arrow[r, hook] & K^\times \arrow[u] \arrow[r, "val"] & \mathbb{Z} \arrow[u] \end{tikzcd}$$ commutes.

② $$\begin{tikzcd} \bar{K} \arrow[d, dash] \\ L \arrow[d, dash] \\ K \end{tikzcd}$$ all Galois

$$\begin{tikzcd} \mathrm{Gal}(\bar{K}/L)^{ab} \arrow[d, "res"] & L^\times \arrow[l] \arrow[d, "\mathrm{Norm}_{L/K}"] \\ \mathrm{Gal}(\bar{K}/K)^{ab} & K^\times \arrow[l] \end{tikzcd}$$

commutes.

Remark: In fact, v_K is uniquely determined by these properties

Analogue for $K = \mathbb{R}$: ① $$\begin{tikzcd} \mathbb{C}^\times \arrow[r] \arrow[d] & \mathrm{Gal}(\mathbb{C}/\mathbb{C})^{ab} \arrow[d] \\ \mathbb{R}^\times \arrow[r] & \mathrm{Gal}(\mathbb{C}/\mathbb{R})^{ab} \end{tikzcd}$$ cts. surjective. Kernel, norms from $\mathbb{C}^\times$.

$K = \mathbb{C}((t))$ ② $\mathbb{C}((t))^\times \xrightarrow{val} \mathrm{Gal}(\overline{\mathbb{C}((t))}/\mathbb{C}((t)))$ dense image.

Example: Let us see this explicitly for $\mathbb{Q}_p$:

$$\mathbb{Q}_p^{ab} = \mathbb{Q}_p(\mu_\infty) = \bigcup \mathbb{Q}_p(\zeta_n)$$ where ζ_n is an n^{th} root of unity.

(local version of Jugendtraum).

$$\mathbb{Q}_p^{ab} = \overset{\underset{p\nmid n}{\bigcup}\mathbb{Q}_p(\zeta_n)}{\overset{\|}{\mathbb{Q}_p(\mu_{p'})}} \cdot \overset{\underset{n\geq 0}{\bigcup}\mathbb{Q}_p(\zeta_{p^n})}{\overset{\|}{\mathbb{Q}_p(\mu_{p^\infty})}}$$

As before: $\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p) = \mathbb{Z}_p^\times$.

Note that $\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p$ is unramified for $p\nmid n$.

$$\left(\overline{\mathbb{F}}_p = \bigcup_{p\nmid n}\mathbb{F}_p(\mu_n)\right).$$

Hence $\mathrm{Gal}(\mathbb{Q}_p(\mu_n)/\mathbb{Q}_p) = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \hat{\mathbb{Z}}$.

$$\Rightarrow \mathrm{Gal}(\mathbb{Q}_p^{ab}/\mathbb{Q}_p) = \underset{\hat{\mathbb{Z}}}{\underset{\|}{\mathrm{Gal}(\mathbb{Q}_p(\mu_{p'})/\mathbb{Q}_p)}} \times \underset{\mathbb{Z}_p^\times}{\underset{\|}{\mathrm{Gal}(\mathbb{Q}_p(\mu_{p^\infty})/\mathbb{Q}_p)}}$$

$$\cup$$

$$\mathbb{Z} \times \mathbb{Z}_p^\times \cong \mathbb{Q}_p^\times.$$

This is the reciprocity map in this case.

Local Langlands for GL_1:

$$\begin{tikzcd}
1 \arrow[r] & I_{\overline{K}/K} \arrow[r] \arrow[d, phantom, "\|"] & W_K \arrow[r] \arrow[d, phantom, "\cap"] & \mathbb{Z} \arrow[r] \arrow[d, phantom, "\cap"] & \{0\} \\
1 \arrow[r] & I_{\overline{K}/K} \arrow[r] & \mathrm{Gal}(\overline{K}/K) \arrow[r] & \hat{\mathbb{Z}} \arrow[r] & \{0\}
\end{tikzcd}$$

Weil group

$$\mathrm{Hom}(W_{K_p}, \mathbb{C}^\times) = \mathrm{Hom}(W_{K_p}, \mathbb{C}^\times)$$

$$\overset{CFT}{=} \mathrm{Hom}(K_p^*, \mathbb{C}^\times)$$

$$= \text{irreducible } \overset{\text{cts.}}{\text{reps}} \text{ of } GL_1(K_p).$$

Structure of Galois groups of local fields

Rmk: This is hands on and rather explicit. Morally it should come long before class field theory!

$$\mathfrak{m}_L^e = \mathfrak{m}_K \mathcal{O}_L$$

$$\begin{array}{llcccccc} L & \text{finite Galois} & \mathcal{O}_L & \supset & \mathfrak{m}_L & \supset & (\pi_L) & \\ | & & \cup & & \cup & & \cup & \\ K & \text{local field} & \mathcal{O}_K & \supset & \mathfrak{m}_K & \supset & (\pi_K), & v_K \end{array}$$

$$\begin{tikzcd} k_L \arrow[d, dash, "f"] \\ k_K \end{tikzcd}$$

$$\begin{tikzcd} \{1\} \arrow[r] & I_{L/K} \arrow[r] \arrow[d, equal] & \mathrm{Gal}(L/K) \arrow[r] & \mathrm{Gal}(k_L/k_K) \arrow[r] \arrow[d, equal] & \{1\} \\ & \{\sigma \mid \sigma \text{ acts trivially on } k_L\}. & & \langle \mathrm{Frob} \rangle & \end{tikzcd}$$

↖ canonical generator.

Note: Gal preserves $\mathcal{O}_K$, hence $\mathfrak{m}$, hence v_K, hence acts on $\mathcal{O}_K/\mathfrak{m}^i$, hence acts continuously on L.

Key lemma: If $\sigma \in I_{L/K}$ fixes π_L, then it is the identity.

Pf: (sketch) Hensel's lemma: $k_L^\times \xhookrightarrow{i} \mathcal{O}_L^\times$ "Teichmüller lifts" "Witt vectors"

We can regard any elt of L as a Laurent series in π_L with coefficients in $\mathcal{O}_L^\times$. If σ fixes $k_L^\times$ then it fixes $i(k_L^\times)$ and hence (by continuity) its action on L is determined by its action on π_L. □

Set $I := I_{L/K}$ and define

$$I_0 = I$$

$$I_j := \{ \sigma \in I \mid \sigma(\pi_L)\pi_L^{-1} \in 1 + m_L^j \}, \qquad j \geq 1.$$

Proposition: This gives a filtration

$$I = I_0 \supset I_1 \supset \dots \supset I_m \supset \dots$$

such that

① each I_j is normal;

② $I_m = \{1\}$ for large m;

③ we have natural injections

$$I_0 / I_1 \hookrightarrow k_L^\times$$

$$I_j / I_{j+1} \hookrightarrow (1 + m_L^j)/(1 + m_L^{j+1}) \cong k_L$$

in particular I is solvable, I_0/I_1 has order prime to p,

and I_1 is the Sylow p-subgroup of I.

This filtration is called the <u>ramification filtration</u> of I.