Overview of Class Field Theory

16/10/2020
Chris Williams

Starting point: Let K be a local or global field

e.g. finite extensions of $\mathbb{Q}_p$; number fields.

Aim: Describe the Galois extensions of K ...
... in terms of the arithmetic of K.

Class Field Theory (CFT): does this for abelian extensions of K.

§1: Splitting Behaviour of Primes

What does "arithmetic" mean?

- $K = \mathbb{Q}$; $\quad \text{primes}(\mathbb{Q}) = \{p \text{ prime}\}$.

- K number field, $\mathcal{O}_K \subset K$ ring of integers;
$$\text{primes}(K) = \{\mathfrak{p} \subset \mathcal{O}_K \text{ prime ideals}\}.$$

Let L/K extension of number fields. Interplay between arithmetic of K and L:

$$\begin{array}{ccccccccc}
\text{prime} & \mathfrak{P} & \subset & \mathcal{O}_L & \longrightarrow & \mathcal{O}_L/\mathfrak{P} & =: & \mathbb{F}_{\mathfrak{P}} & \\
 & | & & \uparrow & & \uparrow & & \uparrow & \text{extn. of finite fields.} \\
\mathfrak{P} \cap \mathcal{O}_K & =: \mathfrak{p} & \subset & \mathcal{O}_K & \longrightarrow & \mathcal{O}_K/\mathfrak{p} & =: & \mathbb{F}_{\mathfrak{p}} &
\end{array}$$

Theorem: Let $\mathfrak{p} \subset \text{primes}(K)$. Then
$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \qquad \mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p},$$
where:

- $e_i \geqslant 1$ "ramification degree",
- $f_i := [\mathbb{F}_{\mathfrak{P}_i} : \mathbb{F}_{\mathfrak{p}}] \geqslant 1$ "inertia degree",
- $e_1 f_1 + \cdots + e_r f_r = [L:K]$.

If L/K Galois, then $e_1 = \cdots = e_r =: e$, $f_1 = \cdots = f_r =: f$.

<u>Q</u>: Can we parametrise Galois extensions by the behaviour of the primes?

$\hookrightarrow$ 2 special classes of behaviours:

- Say $\mathfrak{p} \in \text{primes}(K)$ is $\begin{cases} \underline{\text{ramified}} \text{ in } L \text{ if } e > 1 \\ \underline{\text{unramified}} \text{ in } L \text{ if } e = 1. \end{cases}$

Let
$$\text{Ram}(L/K) = \{\mathfrak{p} : \mathfrak{p} \text{ ramified in } L\}.$$

<u>Fact</u>: $\text{Ram}(L/K)$ is a <u>finite</u> set.

- Say $\mathfrak{p}$ <u>splits completely in L</u> if $e = 1$ (unramified) and $f = 1$.
  $\iff \exists\, [L:K]$ primes $\mathfrak{P}$ above $\mathfrak{p}$ ("$\mathfrak{p}$ breaks apart maximally in L")

Let
$$\text{Spl}(L/K) = \{\mathfrak{p} : \mathfrak{p} \text{ splits completely in } L\}.$$

<u>Proposition</u>: If L/K, L'/K finite Galois extensions with $\text{Spl}(L/K) = \text{Spl}(L'/K)$. Then $L = L'$.

Pf: Theorem of Frobenius: the set $\text{Spl}(L/K) \subset \text{primes}(K)$ has density $\frac{1}{[L:K]}$.

General fact: $\mathfrak{p}$ splits completely in L and L'
$\iff$ it does in LL'.

$$\begin{tikzcd}[column sep=small] & LL' \arrow[dl, dash] \arrow[dr, dash] & \\ L & & L' \\ & K \arrow[ul, dash] \arrow[ur, dash] & \end{tikzcd}$$

$\hookrightarrow$ $\text{Spl}(L/K) = \text{Spl}(LL'/K) = \text{Spl}(L'/K)$,

so
$$[L:K] = [LL':K] = [L':K].$$
But $L \subset LL' \supset L'$, this forces $L = LL' = L'$. $\square$

<u>Upshot</u>: $\exists$ bijection
$$\left\{\begin{matrix}\text{finite Galois} \\ L/K\end{matrix}\right\} \longleftrightarrow \{\text{subsets } \text{Spl}(L/K) \subset \text{primes}(K)\}.$$

<u>Aim</u>: Make this explicit!
a) given L/K, describe $\text{Spl}(L/K)$;
b) given $\text{Spl}(L/K)$, describe L/K.

CFT: successful answer to a, b for L/K abelian.

§2: Quadratic Reciprocity

"Quadratic reciprocity is the first result in class field theory".

<u>Example</u>: $K = \mathbb{Q}$, q prime $\equiv 1 \pmod 4$, $L = \mathbb{Q}(\sqrt{q})$. Then:

- $\mathrm{Ram}(\mathbb{Q}(\sqrt{q})/\mathbb{Q}) = \{q\}$,

- $p \neq q$ splits in $L \iff X^2 - q = (X-\alpha)(X-\beta) \pmod p$

$$\iff q \text{ is a square mod } p$$
$$\overset{\text{quad.}}{\underset{\text{rec}}{\iff}} p \text{ is a square mod } q.$$

<u>Note</u>: There is a lot of extra structure here to give clues for generalisations!

↳ Let $J = \left[(\mathbb{Z}/q\mathbb{Z})^\times \right]^2 \subset (\mathbb{Z}/q\mathbb{Z})^\times$.

Then $\mathrm{Spl}(\mathbb{Q}(\sqrt{q})/\mathbb{Q}) = \{ p : p \pmod q \in J \}$.

<u>Picture</u>:

$$\begin{tikzcd}
\mathrm{Gal}(\mathbb{Q}(\sqrt{q})/\mathbb{Q}) \arrow[r, phantom, "\cong"] & C_2 \arrow[r, phantom, "\cong"] & (\mathbb{Z}/q\mathbb{Z})^\times / J \\
 & & \mathrm{Primes}(\mathbb{Q}) \setminus \{q\} \arrow[u] \arrow[ull, dashed] \\
 & & \mathrm{Spl}(\mathbb{Q}(\sqrt{q})/\mathbb{Q}) \arrow[u]
\end{tikzcd}$$

... this picture exists much more generally!

§3: The Reciprocity Map

<u>Fact</u>: L/K abelian. There is a canonical natural map ("Reciprocity")

$$\mathrm{rec} : \mathrm{Primes}(K) \setminus \mathrm{Ram}(L/K) \longrightarrow \mathrm{Gal}(L/K)$$
$$\mathfrak{p} \longmapsto \mathrm{Frob}_{\mathfrak{p}} = \text{"Frobenius"}$$

s.t.

$$\mathrm{Frob}_{\mathfrak{p}} = 1 \iff \mathfrak{p} \in \mathrm{Spl}(L/K).$$

Sketch: $L/\mathbb{Q}$, $\mathfrak{P} \in \text{primes}(L)$, $\mathfrak{P} \cap \mathbb{Z} = (p)$, e = ramification index, f = inertia degree.

Galois theory of finite fields: $\text{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_p)$ = cyclic of order f

$= \langle \text{Frob}_p \rangle$,

where $\text{Frob}_p : \mathbb{F}_{\mathfrak{P}} \longrightarrow \mathbb{F}_{\mathfrak{P}}$

$x \longmapsto x^p$.

If $L/\mathbb{Q}$ abelian, p is unramified: $\exists$ canonical "lift" of Frob_p to $\text{Gal}(L/\mathbb{Q})$.

Note: p splits completely $\Leftrightarrow$ $f = 1$ $\Leftrightarrow$ $\text{Frob}_p = 1$.

This is set-theoretic. There is a lot of extra structure here:

Definition: Let I_K := group of fractional ideals of K

= free abelian group on primes(K).

Let S := finite subset of primes(K).

Let I_K^S := free abelian group on primes$(K) \setminus S$

= group of fractional ideals "coprime to S".

$\rightsquigarrow$ have a group homomorphism $\text{rec} : I_K^{\text{Ram}(L/K)} \longrightarrow \text{Gal}(L/K)$,

with kernel generated by $\text{Spl}(L/K)$.

Can we describe the kernel intrinsically to K?

§4: CLASS FIELDS / GROUPS

Def'n: Let Σ_∞ := {set of real embeddings $K \hookrightarrow \mathbb{R}$}.

A modulus is a (formal) product $\mathfrak{m} = \mathfrak{m}_\infty \cdot \mathfrak{m}_0$, where:

- $\mathfrak{m}_\infty \subset \Sigma_\infty$ subset,
- $\mathfrak{m}_0 \subset \mathcal{O}_K$ ideal.

e.g. Every modulus for $K=\mathbb{Q}$ has form $\infty\cdot(N)$ or (N).
(as all ideals are principal, and there is only one embedding $\mathbb{Q}\hookrightarrow\mathbb{R}$).

<u>Definition</u>: Let $\mathfrak{m}$ modulus, and

$$P_{\mathfrak{m}} := \left\{ \begin{array}{l} \text{group of } \underline{\text{principal}} \text{ frac. ideals } (a) \text{ which have} \\ \text{a generator } a\in K \text{ s.t.:} \\ \quad - \ a\equiv 1 \pmod{\mathfrak{m}_0}, \\ \quad - \ i(a)>0 \quad \forall i\in \mathfrak{m}_\infty \end{array} \right\}.$$

Let $S_{\mathfrak{m}_0} := \{\mathfrak{p} : \mathfrak{p}\mid \mathfrak{m}_0\}$. Then $P_{\mathfrak{m}} \leq I_K^{S_{\mathfrak{m}_0}}$. Let

$$C_{\mathfrak{m}} := I_K^{S_{\mathfrak{m}_0}}/P_{\mathfrak{m}},$$

the <u>ray class group of K of conductor $\mathfrak{m}$</u>.

<u>Theorem</u>: (Global class field theory). For every modulus $\mathfrak{m}$, there is a unique <u>class field</u> $H_{\mathfrak{m}}$ such that:
- $H_{\mathfrak{m}}/K$ is abelian,
- Reciprocity induces an isomorphism $C_{\mathfrak{m}} \xrightarrow{\sim} \mathrm{Gal}(H_{\mathfrak{m}}/K)$,
- $\mathfrak{p}\in \mathrm{Ram}(H_{\mathfrak{m}}/K) \Rightarrow \mathfrak{p}\mid\mathfrak{m}_0$ ("$H_{\mathfrak{m}}$ unramified outside $\mathfrak{m}_0$.").

<u>Every</u> finite abelian extension L of K arises as a subfield of some $H_{\mathfrak{m}}$
$\longleftrightarrow$ subgroup of $C_{\mathfrak{m}}$ $\longleftrightarrow$ $P_{\mathfrak{m}} \subset \mathrm{Ker}(\mathrm{rec})$.

e.g. $K=\mathbb{Q}$, $\mathfrak{m}=\infty\cdot(N)$.

(Roughly!)
$$I_K^{S_N} \sim \{n\in\mathbb{Z} : (n,N)=1\},$$
$$P_{\infty\cdot N} \sim \{n\in\mathbb{Z} : n\geq 0,\ n\equiv 1 \pmod N\}.$$

$$\rightsquigarrow C_{\infty\cdot N} \cong (\mathbb{Z}/N\mathbb{Z})^\times, \qquad H_{\infty\cdot N} = \mathbb{Q}(\zeta_N).$$

Thm (GCFT) $\Rightarrow$ every abelian extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_N)$
$\rightsquigarrow$ recover Kronecker-Weber theorem.

§6: Local Class Field Theory

If L/K abelian extension of number fields, $\mathfrak{P} \in \text{primes}(L)$, $\mathfrak{p} \in \text{primes}(K)$, then $L_{\mathfrak{P}}, K_{\mathfrak{p}} / \mathbb{Q}_p$ finite extensions and

$$L_{\mathfrak{P}} / K_{\mathfrak{p}} \text{ is abelian.}$$

$\rightsquigarrow$ Classification of abelian extensions of number fields
$\Rightarrow$ classification of abelian extensions $L_{\mathfrak{P}} / K_{\mathfrak{p}}$ $(/\mathbb{Q}_p)$.

<u>Theorem</u>: (Local Class field theory). Let $K/\mathbb{Q}_p$ finite. If L/K finite abelian, then

$$\text{Norm}(L^\times) \subset K^\times \text{ has finite index.}$$

The norm map defines an inclusion-reversing bijection

$$\begin{aligned} \{\text{finite abelian } L/K\} &\longleftrightarrow \{\text{finite index subgroups of } K^\times\} \\ L &\longmapsto \text{Norm}(L^\times). \end{aligned}$$