Today I want to discuss class field theory, but first we should understand the problem, and recall some infinite Galois theory.

Basic Q: determine all finite extensions of a number field K (e.g. $\mathbb{Q}$).

Certainly this is a fundamental question in number theory.

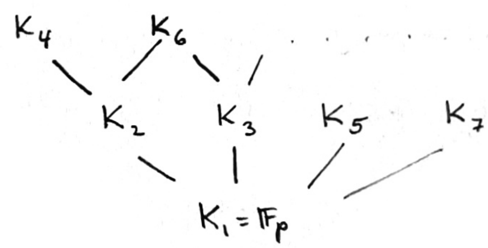
For most questions of the form: $\boxed{\text{How many number fields satisfy blah?}}$

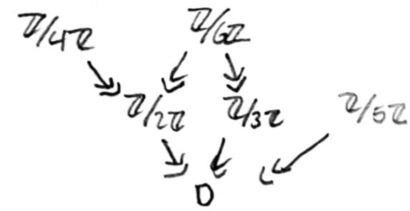
the answer is unknown.

Let us consider an example where we can say something.

<u>Example:</u> Let $K = \mathbb{F}_p$, fix $\overline{K}$ an algebraic closure.

For any $n \geq 1$ there is a unique subfield K_n with p^n-elements.





Let us calculate $\mathrm{Gal}(\overline{K}/K)$.

$$\overline{K} = \bigcup_{n\geq 1} K_n \implies \mathrm{Gal}(\overline{K}/K) \hookrightarrow \prod_n \underset{\substack{\mathbb{Z}/n\mathbb{Z} \ni 1 \\ \downarrow}}{\mathrm{Gal}(K_n/K)} \ni \mathrm{Frob}_{p^n}$$

$$\varphi \longmapsto (\varphi_n).$$

Sequence (γ_n) is in the image $\iff$ $\gamma_m = \gamma_n \bmod m$ whenever $m \mid n$.

Hence: $$\mathrm{Gal}(\overline{K}/K) = \varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}$$ "profinite completion of $\mathbb{Z}$"

<u>Exercise:</u> (a) $\hat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p$

(b) Show that $\hat{\mathbb{Z}}$ has uncountably many subgroups, hence naive Galois correspondence can't hold.

Infinite Galois theory

L/K Galois : algebraic, normal, seperable.

$$\mathrm{Gal}(L/K) \hookrightarrow \prod_{\substack{K \subset L' \subset L \\ \text{finite Galois}}} \mathrm{Gal}(L'/K)$$

$$\varphi \mapsto \varphi_{L'}$$

image determined by: $\forall$ $M \supset L'' \supset L' \supset L$

$$\begin{array}{ccc} \varphi_{L''} \in & \mathrm{Gal}(L''/L) \\ \downarrow & \downarrow \\ \varphi_{L'} \in & \mathrm{Gal}(L'/L) \end{array}$$

i.e.
$$\mathrm{Gal}(L/K) = \varprojlim_{\substack{K \subset L' \subset L \\ \text{finite Galois}}} \mathrm{Gal}(L'/K)$$

If we give the product topology then inherits the subspace topology.

Hence $\mathrm{Gal}(L/K)$ becomes a topological group.

Exercise (important, can be used as a definition):

Basis of open nbhds of $1 \in \mathrm{Gal}(L/K)$ given by kernels of

$$\mathrm{Gal}(L/K) \to \mathrm{Gal}(L'/K) \quad \text{for } L' \,|\, K \text{ finite Galois.}$$

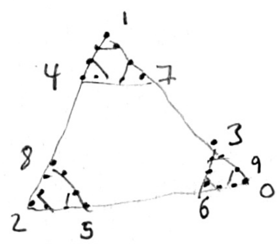
Exercise: $\prod \mathrm{Gal}(L'/K)$ is compact, $\mathrm{Gal}(L/K) \subset \prod$ is closed, hence compact.

(E.g. $\hat{\mathbb{Z}}$ is compact, which might look strange).

[G a group, $\hat{G} = \varprojlim G/H$ H finite index normal, G profinite if $G \xrightarrow{\sim} \hat{G}$.

Key example: $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n\mathbb{Z}$, what does it look like?

p=3:



"Galois groups are fractal like objects".
and profinite groups

L/K Galois.

Fundamental theorem of infinite Galois theory

$$\left\{ \begin{array}{c} L \\ | \\ L' \\ | \\ K \end{array} \right\} \xleftrightarrow{\sim} \begin{array}{l} \text{closed subgroups} \\ \text{of } Gal(L/K) \end{array}$$

$$L^H \longleftarrow\!\shortmid \; H$$

$$L' \longmapsto Gal(L/L')$$

Moreover:

finite ext^{ns} $\longleftrightarrow$ open and closed

Galois $\longleftrightarrow$ normal.

Exercise: Any closed subgroup of $\hat{\mathbb{Z}}$ is of the form $n\hat{\mathbb{Z}}$ for $n \in \mathbb{Z}$.

$n \geq 1 \leftrightarrow K_n$, $n = 0 \leftrightarrow \bar{K}$.

(only closed subgroup which isn't open).

Let us revisit our problem: describe the closed subgroups of $Gal(\bar{K}/K)$.

Note that this isn't really well-defined (from a philosophical point of view) because $\bar{K}$ involves a choice. Thus $Gal(\bar{K}/K)$ is only really a "group up to conjugacy". (or many many choices if you want)

Thought experiment: Show that the isomorphism classes of representations of a "group up to conjugacy" are canonical. This is one reason representations are so important in the Langlands program!

On the other hand the maximal abelian extension K^{ab} is canonical, and we can hope to describe it.

(K^{ab} is the extension corresponding to $\overline{[Gal(\bar{K}/K), Gal(\bar{K}/K)]}$).

Global class-field theory: first version

Key example: $\zeta_n = e^{2\pi i/n}$. $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ Galois w/ Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$.

$$\mathbb{Q}(\mu_\infty) := \bigcup_{n\geq 1} \mathbb{Q}(\zeta_n) \quad \text{abelian w/ Galois group}$$

$$\varprojlim_n (\mathbb{Z}/n\mathbb{Z})^\times = \prod_p \mathbb{Z}_p^\times .$$

Fact ("Kronecker Jugendtraum"): $\mathbb{Q}(\mu_\infty) = \mathbb{Q}^{ab}$. (not easy! will follow from global class-field theory)

How do we predict this starting from $\mathbb{Q}$?

Exercise: Use Jugendtraum to show that any continuous $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{C}^\times$ "is" a Dirichlet character.

Given a number field or function field it is useful to consider all norms at once. A place of K is an equivalence class of nontrivial multiplicative norms $\|\cdot\| : K \to \mathbb{R}_{>0}$ on K.

Thm: All places of a number field K are of the following form:

finite places: $|x|_v := (\# \mathcal{O}_K/\mathfrak{p})^{-\mathrm{val}_\mathfrak{p}(x)}$ for $\mathfrak{p} \subset \mathcal{O}_K$ prime.

real places: $|x|_v := |i(x)|$ for each real embedding $i : K \hookrightarrow \mathbb{R}$

complexes places: $|x|_v := \|i(x)\|^2$ for each pair of conjugate embeddings $i : K \hookrightarrow \mathbb{C}$.

The reason for the above normalisation is the beautiful:

Product formula: $\prod_{\text{places } v} |x|_v = 1.$

makes sense because finitely many are $\neq 1$.

Function field case:
"# zeroes and poles agree"

Global class field theory according to Artin:

Fix $\begin{array}{c} L \\ | \\ K \end{array}$ abelian. $\begin{array}{c} \mathcal{O}_L \\ | \\ \mathcal{O}_K \end{array}$ rings of integers. $S :=$ set of places including ramified primes $\subset \mathcal{O}_K$ and places at ∞.

We have seen: $\mathfrak{p} \subset \mathcal{O}_K$ prime, $\mathfrak{p} \notin S \rightsquigarrow \mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(L/K)$

conjugacy class in general, but is abelian, hence we get an elt.

Chebotarev

Hence get a map $A: J^S \xrightarrow[\text{map}]{\text{Artin}} \mathrm{Gal}(L/K)$.

$$J^S = \bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}\mathfrak{p} \qquad \mathfrak{p} \longmapsto \mathrm{Frob}_{\mathfrak{p}} \qquad A: \sum_{i=1}^m n_i \mathfrak{p}_i \longmapsto \prod_{i=1}^m \mathrm{Frob}_{\mathfrak{p}_i}^{n_i}$$

<u>Q:</u> How to determine the kernel of Artin map?

Given a finite set of places S a <u>modulus supported in S</u> is a formal linear combination $\mathfrak{m} = \sum n_i v_i$ s.t. $n_i \geq 0$ and $n_i \in \{0,1\}$ for real v_i and $n_i = 0$ for complex v_i.

$$\begin{tikzcd}
K^\times \arrow[r] \arrow[rr, bend left, "\mathrm{val}"] & J = \text{group of fractional ideals} & = \bigoplus_{\mathfrak{p}} \mathbb{Z}\mathfrak{p} \\
\cup & \cup & \cup \\
K^S \arrow[r] & J^S & = \bigoplus_{\mathfrak{p} \notin S} \mathbb{Z}\mathfrak{p} \\
\cup & & \\
K^{\mathfrak{m},1} \arrow[uur, "\mathrm{val}"] & &
\end{tikzcd}$$

image = principal ideals

unique factorisation

"α is $\mathfrak{m}$-close to 1" i.e.

$$K^{\mathfrak{m},1} = \left\{ \alpha \in K^S \;\middle|\; \begin{array}{ll} \mathrm{val}_{\mathfrak{p}_i}(\alpha - 1) \geq n_i & \text{finite places} \\ \alpha > 0 & n_i = 1 \text{ real places.} \end{array} \right\}$$

Ray class group: $Cl_K^m := J^S / \mathrm{val}(K^{m,1})$.

Example: If $m=0$, Cl_K is the class group of K.

Thm: For any modulus Cl_K^m is finite and surjects onto
(finiteness) the class group of K.

Thm: "Any $\begin{matrix} L \\ | \\ K \end{matrix}$ as above admits a modulus".

That is, there exists a modulus m with support in S such that $\mathrm{val}(K^{m,1})$ is contained in the kernel of the Artin map. I.e.

Artin: $Cl_K^m \twoheadrightarrow \mathrm{Gal}(L/K)$

Example: $\begin{matrix} \mathbb{Q}(i) \\ | \\ \mathbb{Q} \end{matrix}$, $S=\{2,\infty\}$. For any $p \neq 2$,

$\mathrm{Frob}_p(i) = i^p$, hence

$\mathrm{Frob}_p \longmapsto p \bmod 4 \in (\mathbb{Z}/4\mathbb{Z})^\times = \mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$.

$J^S = \{ \frac{a}{b} \in \mathbb{Q} \mid \begin{matrix} a \text{ and } b \text{ coprime to } 2 \\ a,b>0 \end{matrix} \} = \mathbb{Z}^\times_{(2),>0}$

Artin map is the natural map $\mathbb{Z}^\times_{(2),>0} \to (\mathbb{Z}/4\mathbb{Z})^\times$.

Kernel $= \{ \lambda \in \mathbb{Z}^\times_{(2),>0} \mid \mathrm{val}_2(\lambda - 1) \geq 2 \}$ ← "congruence condition at 2".

Exercise: If $m = m(\infty)$ then $Cl_{\mathbb{Q}}^m = (\mathbb{Z}/m\mathbb{Z})^\times$.

Hence, letting m become more and more divisible

gives $\mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) = \varprojlim (\mathbb{Z}/m\mathbb{Z})^\times = \prod_{p \text{ prime}} \mathbb{Z}_p^\times$

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

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

commutes.

Example: If $\mathfrak{m}=0$ then $Cl_K^{\mathfrak{m}} = Cl$. Hence there exists L/K 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 $\mathcal{O}_K = v^{-1}(\mathbb{Z}_{\geq 0} \cup \{\infty\})$ $\qquad k_K := \mathcal{O}_K / \mathfrak{m}_K$ residue field.

$\cup$

$\mathfrak{m}_K = v^{-1}(\mathbb{Z}_{>0} \cup \{\infty\}) \ni \pi$ a uniformiser.

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

② k_K is finite.

Exercise: ① and ② are equivalent to K being locally compact.

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

$$\begin{array}{c} L \\ | \\ K \end{array}$$ finite, Galois any elt $\sigma \in Gal(L/K)$ preserves $\begin{array}{c} \mathcal{O}_L \\ | \\ \mathcal{O}_K \end{array}$, $\begin{array}{c} m_L \\ | \\ m_K \end{array}$ and hence acts on $\begin{array}{c} k_L \\ | \\ k_K \end{array}$.

We get a map

$$I_{L/K} \longrightarrow Gal(L/K) \twoheadrightarrow Gal(k_L/k_K)$$

$$Gal(k_L/k_K) = \mathbb{Z}/d\mathbb{Z}$$, generated by Frobenius.

$I_{L/K}$: inertia subgroup

For $L = \overline{K}$ we get: $I_{\overline{K}/K} \to Gal(\overline{K}/K) \twoheadrightarrow Gal(\overline{k_K}/k_K)$. $Gal(\overline{k_K}/k_K) = \hat{\mathbb{Z}}$

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

<u>Local class field theory:</u> There exists a natural homomorphism

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

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

$\widehat{K}^\times$: completion wrt subgroups of finite index, profinite completion.

Moreover:

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

② $$\begin{array}{c} \overline{K} \\ | \\ L \\ | \\ K \end{array}$$ all Galois

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

commutes.

<u>Remark:</u> In fact, r_K is uniquely determined by these properties.