LECTURE 2

Noether's method: let $G \subseteq S_d$, so $G \curvearrowright \mathbb{Q}(\alpha_1, \dots, \alpha_d)$ ← again indeterminants

$$K = \mathbb{Q}(\alpha_1, \dots, \alpha_d) \supseteq G$$
$$|$$
$$k = \mathbb{Q}(\alpha_1, \dots, \alpha_d)^G$$

Question: Is this a purely transcendental extension of $\mathbb{Q}$?

If yes, G is a Galois group / $\mathbb{Q}$ by Hilbert, as for S_n.

- Yes for $G < S_4$ (Noether)

But No in general:

- No for $G = C_{47}$ (Swan 1969)
- No for $G = C_8$ (Lenstra 1974).

From a computational perspective, invariant fields can be hard to compute.

Rmk $K = \mathbb{Q}(\alpha_1, \dots, \alpha_n)$ = field of rational functions of $\mathbb{A}^n_{\mathbb{Q}}$

$k = \mathbb{Q}(\alpha_1 \dots, \alpha_n)^G$ = field of rational functions of $V = \mathbb{A}^n_{\mathbb{Q}}/G$

↑ some n-dimensional affine variety.

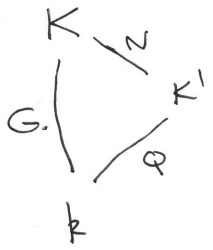
Noether's question: Is V a rational variety (birational to $\mathbb{A}^n_{\mathbb{Q}}$)?

Even if not, if $V(\mathbb{Q}) \neq \phi$ and $P \in V(\mathbb{Q})$ is such that

$\pi : \mathbb{A}^n_{\mathbb{Q}} \longrightarrow \mathbb{A}^n_{\mathbb{Q}}/G$ is unramified over P, then G is a Galois group $/\mathbb{Q}$.

§5 Quotients & Extension problem.

Clearly, if G is a Galois group $/k$, then so is any quotient $Q = G/N$



← when $k = \mathbb{Q}(t_1, \dots, t_n)$
K regular $\Rightarrow K'$ regular $(K' \cap \bar{\mathbb{Q}} \subseteq K \cap \bar{\mathbb{Q}} = \mathbb{Q})$

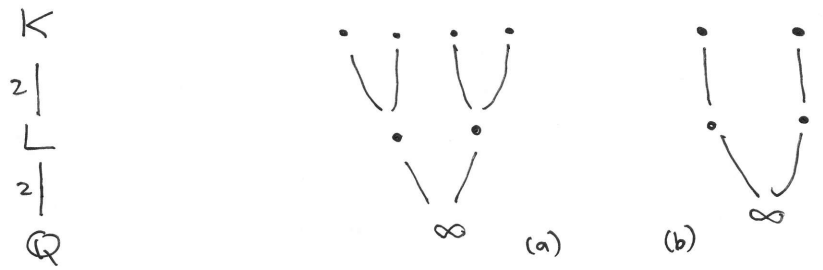
Thus, $\mathcal{I}_{G/\mathbb{Q}} \Rightarrow \mathcal{I}_{Q/\mathbb{Q}}$

$\mathcal{I}_{G/\mathbb{Q}(t)} \Rightarrow \mathcal{I}_{Q/\mathbb{Q}(t)}$

What about the converse? Can we always embed a Q-extension into a G-extension, and use this to construct, for example, 2-groups by repeated quadratic extensions, inductively?

This is known as the Extension Problem, and it is not always soluble.
(or Embedding Problem)

Ex Let $K/\mathbb{Q}$ be a Galois extension with $Gal(K/\mathbb{Q}) = C_4$



The decomposition group $D_\infty < C_4$ is of order ≤ 2, so either

(a) $D_\infty = C_1$ — 4 places $|\infty$ in K — 2 places $|\infty$ in L

(b) $D_\infty = C_2$ — 2 places $|\infty$ in K — 2 places $|\infty$ in L

↖ cosets C_4/D_∞ ↖ double cosets $C_2 \backslash C_4 / D_\infty$

In either case L has two places $|\infty$, so it is real quadratic.

Thus, for example, $\mathbb{Q}(i)$ cannot be embedded in a C_4-extension of $\mathbb{Q}$.

Witt has initiated a study of obstructions to the embedding problem:

Thm (Witt) k field, $\mathrm{char}\, k \neq 2$. A quadratic extension $k(\sqrt{e})$ can be embedded in a C_4-extension of k $\iff$ e is a sum of two squares in k.

See Exercise Q1.

Ex $\mathbb{Q}(\sqrt{5})$ ✓ ($\leftarrow$ in fact $\mathbb{Q}(\sqrt{5}) \subseteq \mathbb{Q}(\zeta_5)$)

$\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{3})$ ×

Thm (Witt, 1936) k field, $\mathrm{char}\, k \neq 2$. A biquadratic extension $k(\sqrt{a}, \sqrt{b})$ can be embedded in a Q_8-extension of k $\iff$ $aX^2 + bY^2 + abZ^2 \sim X^2 + Y^2 + Z^2$

↖ equivalence of quad. forms $/k$.

If $P = (P_{ij}) \in GL_3(k)$, $\det P = \frac{1}{ab}$ is such that $P^t \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{pmatrix} P = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, then such quaternion extensions containing $k(\sqrt{a}, \sqrt{b})$ are

$k(\sqrt{a}, \sqrt{b}, \sqrt{r(1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{a}\sqrt{b})})$ for $r \in k^\times$.

- Obstructions to the embedding problem were studied by Serre, Sonn, Mestre, Vila, ..., especially when $1 \to C_2 \to G \to Q \to 1$ is a central extension ($C_2 \subseteq Z(G)$), e.g. $G = \tilde{A}_n$ see Problem P.1
- Scholz-Reichardt and Shafarevich construct soluble groups over $\mathbb{Q}$ inductively, and need to deal with obstructions (by ramifying enough primes, essentially).

§ 6 Cyclic groups.

Problem Construct regular C_n-extensions of $\mathbb{Q}(t)$ for $n \geq 2$.

Kronecker-Weber $\Rightarrow$ every abelian ext. of $\mathbb{Q}$ is $\subseteq \mathbb{Q}(\zeta_N)$ for some N, but it is not clear how to get a family over $\mathbb{Q}(t)$.

Solution (Swith, Dentzer, Schneps) Say $\mathrm{Gal}(K/\mathbb{Q}) = C_n$. Then $K(\zeta_n)/\mathbb{Q}(\zeta_n)$ is (usally) a C_n-extension and, by Kummer theory,

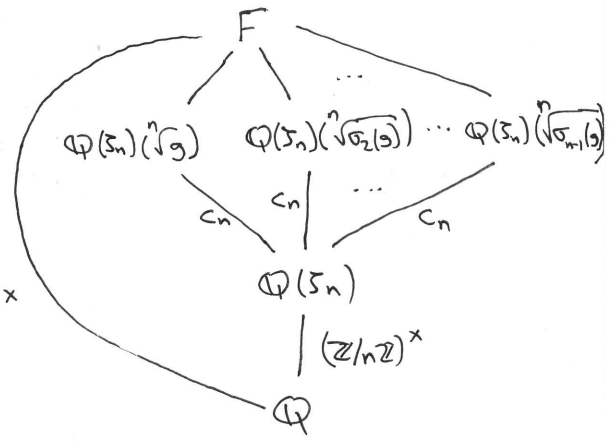
$$K(\zeta_n) = \mathbb{Q}(\zeta_n)(\sqrt[n]{g}) \qquad \text{some } g \in \mathbb{Q}(\zeta_n)^\times$$

That is, every C_n-extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)(\sqrt[n]{g})$ for some g.

The Galois closure F of $\mathbb{Q}(\zeta_n)(\sqrt[n]{g})$ has (usually) Galois group $C_n^{\varphi(n)} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$:

Recall: $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

$\sigma_j : \zeta_n \mapsto \zeta_n^j \longleftrightarrow j$



$$C_n^{\varphi(n)} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times = C_n \wr (\mathbb{Z}/n\mathbb{Z})^\times$$

Choosing a combination of $\sqrt[n]{\sigma_j(g)}$ carefully, we get a C_n-quotient:

Thm Let $g \in \mathbb{Q}(\zeta_n)$, $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_j\}$ as above. Define

$$f_g(x) = \prod_{\ell \in \mathbb{Z}/n\mathbb{Z}} \left(x - \sum_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} \zeta_n^{\ell/k} \prod_{j \in (\mathbb{Z}/n\mathbb{Z})^\times} A_{1/j;k}^{j} \right) \quad ; \quad A_j = \sqrt[n]{\sigma_j(g)} \in \mathbb{C}.$$

Then $f_g(x) \in \mathbb{Q}[x]$ ← and in $\mathbb{Z}[x]$ if $g \in \mathbb{Z}[\zeta_n]$ and can therefore be computed efficiently over $\mathbb{C}$

and for most choices of g it is irreducible with Galois group C_n over $\mathbb{Q}$.

Ex $n=3, 4$. Here $[\mathbb{Q}(\zeta_n):\mathbb{Q}]=2$, let $g=a+b\zeta_n$ ← general element of $\mathbb{Q}(\zeta_n)$

$n=3$ $\quad f_g(x) = x^3 - 3(a^2-ab+b^2)x - a^3-(a-b)^3$

$n=4$ $\quad f_g(x) = x^4 - 4(a^2+b^2)x^2 + 4(a^2+b^2)$

← generic C_3 and C_4 families over $\mathbb{Q}(a,b)$

Ex General n, $g=a+\zeta_n$ implemented as Family(CyclicGroup(n))

(large and unwieldy for large n, degree $n\varphi(n)$ in a)

Q Best families (lowest degree in a) for C_n over $\mathbb{Q}(a)$? ← see Problem P5

§7 Split extensions by abelian groups.

Recall: Embedding problems for $C_4 \twoheadrightarrow C_2$ and $Q_8 \twoheadrightarrow C_2\times C_2$ are not always soluble. For split extensions with abelian kernel they are.

Def A, Q groups. An extension of Q by A is an exact sequence

$$1 \longrightarrow A \longrightarrow G \underset{\varphi}{\overset{\pi}{\rightleftarrows}} Q \longrightarrow 1 \qquad [\text{ i.e. } A \trianglelefteq G,\ G/A \cong Q]$$

It is split (written $G=A:Q$) if $\exists \varphi: Q \to G$ s.t. $\pi\circ\varphi = id$, and non-split (written $G=A.Q$) if not.

- Every finite group can be built from simple groups using extensions (and soluble groups from cyclic groups)

Suppose A is abelian

- Action by conjugation $G \longrightarrow \mathrm{Aut}\,A$ has A in the kernel, so we get
$$\alpha: Q \longrightarrow \mathrm{Aut}\,A$$
$$q \longmapsto (a \mapsto \tilde{q}a\tilde{q}^{-1})$$
$\tilde{q}$ lift of $q \in G/N$ to G.

- A, Q and $\alpha: Q \to \mathrm{Aut}A$ determine G uniquely as
$$G = A \rtimes_\alpha Q = \{(a,q) \mid a\in A, q\in Q\} \text{ with } (a,q)(a',q') = (a\alpha(q)(a'), qq')$$
└ semidirect product

- All extensions of Q by A with action α are classified by $H^2(Q,A)$ (with $0 \in H^2(Q,A) \longleftrightarrow A\rtimes_\alpha Q$, the split extension).

Ex Extensions $1 \longrightarrow \overset{A}{C_4} \longrightarrow G \longrightarrow \overset{Q}{C_2} \longrightarrow 1$.

$\mathrm{Aut}\, C_4 = (\mathbb{Z}/4\mathbb{Z})^\times = \{\pm 1\}$, so there are two possible actions

$\alpha_1 : C_2 \longrightarrow \mathrm{Aut}\, C_4$

generator $\longmapsto$ identity — trivial action

$\alpha_{-1} : C_2 \longrightarrow \mathrm{Aut}\, C_4$

generator $\longmapsto$ $(x \mapsto x^{-1})$ — inversion.

In both cases,

$$H^2(Q,A) = \frac{A^Q}{(\sum_{q \in Q} q)(A)} = \begin{cases} \frac{C_4}{2C_4} \cong \mathbb{Z}/2\mathbb{Z} & \text{if } \alpha = \alpha_1 \\ \frac{2C_4}{0} \cong \mathbb{Z}/2\mathbb{Z} & \text{if } \alpha = \alpha_{-1} \end{cases}$$

(Q cyclic)

so there are two extensions for each action, one split and one not:

$\alpha = \alpha_1$

$1 \longrightarrow C_4 \longrightarrow C_4 \times C_2 \rightleftarrows C_2 \longrightarrow 1$ split.

$1 \longrightarrow C_4 \longrightarrow C_8 \longrightarrow C_2 \longrightarrow 1$ non-split.

$\alpha = \alpha_{-1}$

$1 \longrightarrow C_4 \longrightarrow D_4 \rightleftarrows C_2 \longrightarrow 1$ split.

$1 \longrightarrow C_4 \longrightarrow Q_8 \longrightarrow C_2 \longrightarrow 1$ non-split.