LECTURE 4

To construct regular $SL_2(\mathbb{F}_3)$-extensions, we use an alternative characterisation of Q_8-fields due to Bucht:

<u>Thm</u> (Bucht 1910) A biquadratic extension $K(\sqrt{u}, \sqrt{v})$ of K is embeddable in a Q_8-extension of K $\iff$ $\exists\, \alpha, \beta, \gamma \in K$ so that

$$u = (1+\alpha^2+\alpha^2\beta^2)(1+\beta^2+\beta^2\gamma^2) \cdot \text{ square in } K$$
$$v = (1+\beta^2+\beta^2\gamma^2)(1+\gamma^2+\gamma^2\alpha^2) \cdot \text{ square in } K$$
$$(\Rightarrow uv = (1+\gamma^2+\gamma^2\alpha^2)(1+\alpha^2+\alpha^2\beta^2) \cdot \text{ square in } K\ )$$

This is symmetric in
$$\begin{tikzcd}[column sep=small] \alpha \arrow[r] & \beta \arrow[dl] \\ \gamma \arrow[u] & \end{tikzcd}$$
, in other words this construction respects the action of $C_3 \subseteq \operatorname{Aut} Q_8$.

So we take
K = any C_3-extension of $\mathbb{Q}$; $g :=$ generator of $\mathrm{Gal}(K/\mathbb{Q}) = C_3$

α = general enough element of K (*)

$\beta = g(\alpha)$, $\gamma = g(\beta)$

Define u, v, w as above, and (unravelling Witt's Theorem)

$$F := K\left(\sqrt{u}, \sqrt{v}, \sqrt{1 + (1-\alpha\beta\gamma)\left(\tfrac{1}{\sqrt{u}} + \tfrac{1}{\sqrt{v}} + \tfrac{1}{\sqrt{w}}\right)}\ \right)$$

is a quaternion extension of K which has Galois group $SL_2(\mathbb{F}_3)$ over k.

Taking $k = \mathbb{Q}(t)$ we get a regular family. In fact, Faddeyev showed that (*) is always possible, and deduced

<u>Thm</u> (Faddeyev 1945) If k is Hilbertian, every C_3-extension of k can be embedded in a $SL_2(\mathbb{F}_3)$-extension of k.

Obvious question: Does this generalise to other groups $N \rtimes Q$ when N is non-abelian? This would be a big step towards getting all soluble groups over $\mathbb{Q}(t)$.

<u>Conjecture</u> (Dèbes-Deschamps) Every split embedding problem (lifting a Q-extension to a $N \rtimes Q$-extension for any N) is soluble over every Hilbertian field k.

↖ stronger than Inverse Galois Problem

§11 Descent to subgroups.

<u>Question</u> $K/\mathbb{Q}(a,b,\dots)$ family with Galois group U.

$G < U$ subgroup

Is there a subfamily with Galois group G?

Not always; if yes, would solve IGP, as any $G < S_n$.

<u>Ex</u> $G = C_3$, $U = S_3$

- S_3-family x^3+x+a, $\Delta = -27a^2-4$

Want to find a rat. fnc. $a(t)$ such that $-27a(t)^2-4 =$ square. Then $x^3+x+a(t)$ has $\mathrm{Gal} \subseteq C_3$

$b^2 = -27a^2-4$ genus 0 curve, no $\mathbb{Q}$-pts

- S_3-family x^3+ax+1, $\Delta = -4a^3-27b^2$

$b^2 = -4a^3-27$ elliptic curve E, may have $\mathbb{Q}$-pts, but no rational maps $\mathbb{P}^1 \dashrightarrow E$ (so could solve $\mathcal{I}_{C_3/\mathbb{Q}}$ but not $\mathcal{I}_{C_3/\mathbb{Q}(t)}$ with it)

- S_3-family x^3+ax+b over $\mathbb{Q}(a,b)$, $\Delta = -4a^3-27b^2$

$S: c^2 = -4a^3-27b^2$ cubic surface, rational $\mathbb{P}^2_{A,B} \dashrightarrow S$

$a = -\frac{1}{4}(27A^2+B^2)$
$b = -\frac{a}{4}(27A^2+B^2)$
$c = -\frac{b}{4}(27A^2+B^2)$

$\rightsquigarrow$ C_3-family $/\mathbb{Q}(a,b)$: $x^3-(27a^2+b^2)x-2a(27a^2+b^2)$, generic.

Smallest groups for which $\mathcal{I}_{G/\mathbb{Q}(t)}$ is unknown: Small Group(64,i)

<u>Ex</u> There are 10 groups of order 64 that are not semi-abelian;

$i = 8, 9, 10, 11, 12, 13, 14$ nilpotency class 3; these 7 have been proved to have regular families $/\mathbb{Q}(t)$ Schoeps

$i = 41, 42, 43$ nilpotency class 4; unknown $/\mathbb{Q}(t)$.
$G_1 \; G_2 \; G_3$

$G_1 = 16t156 < 16t256 < 16t498 < 16t909 < 16t1181 = SD_{16}^2 \rtimes C_2^2$

semi abelian; easy to construct families using resultants

$G_2 = 16t144 < 16t379 < 16t679 < 16t972 < 16t1193 = D_8^2 \rtimes C_2^2$

Descent works for G_1 and gives a regular family $/\mathbb{Q}(t)$

Presumably for G_2 as well? G_3 only acts on 32 points - computationally harder.

This method is very powerful in practice - subfields are often given by eqns that define a genus 0 curve, or a rational surface, or an elliptic surface with a section, or a higher-dim. variety with rational curves, but seems very hard to understand it theoretically and predict when it works.

§12 Rigidity

<u>Thm</u> (Riemann Existence Thm.) G finite group generated by $g_1, \dots, g_\ell$; $g_1 g_2 \cdots g_\ell = 1$.
$S = \{P_1, \dots, P_\ell\} \in \mathbb{P}^1(\mathbb{C})$. Then there exists a Galois G-cover

$$X \xrightarrow{\varphi} \mathbb{P}^1(\mathbb{C}) \qquad [G \leq \mathrm{Aut}\, X, \ X/G = \mathbb{P}^1]$$

unramified outside S and ramification gp $\langle g_i \rangle < G$ over P_i.

<u>Cor</u> $\mathcal{I}_{G/\mathbb{C}(t)}$ is true for every group G.

<u>Proof</u> Pick any generators $g_1, \dots, g_{\ell-1}$ of G, let $g_\ell := (g_1 \cdots g_\ell)^{-1}$ so that $g_1 \cdots g_\ell = 1$.
Pick $P_1, \dots, P_\ell \in \mathbb{P}^1(\mathbb{C})$ arbitrary. Riemann existence $\Rightarrow$

$$\begin{matrix} X \\ \downarrow \varphi \\ \mathbb{P}^1(\mathbb{C}) \end{matrix} \quad \rightsquigarrow \quad \begin{matrix} \mathbb{C}(X) \\ G| \\ \mathbb{C}(t) \end{matrix}$$

automatically regular as $\mathbb{C} = \overline{\mathbb{C}}$. ∎

The problem is descending from $\mathbb{C}$ to $\mathbb{Q}$. A general principle in Galois theory is that "things that are unique are defined over $\mathbb{Q}$".
Generally, the covers given by Thm are not unique, but one can impose conditions on the g_i to force $X \xrightarrow{\varphi} \mathbb{P}^1$ to be unique and defined over $\mathbb{Q}$:

G finite group

$C_1, \dots, C_\ell$ conjugacy classes

$$\Sigma := \{(g_1, \dots, g_\ell) \mid g_i \in C_i, \ g_1 g_2 \cdots g_\ell = 1, \ \langle g_1, g_2, \dots, g_\ell \rangle = G\}$$

possibly $\emptyset$

$\circlearrowleft$ G acts by conjugation

g has a fixed pt on Σ $\iff$ $g \cdot (g_1, \dots, g_\ell) = (g_1, \dots, g_\ell)$

$\iff$ g commutes with the g_i $\overset{g_i \text{ generate } G}{\iff}$ $g \in Z(G)$.

$\boxed{\text{Suppose } Z(G) = \{1\}}$. Then the action $G \circlearrowright \Sigma$ is free.

<u>Def</u> $(C_1, \dots, C_\ell)$ is a <u>rigid</u> ℓ-tuple of conjugacy classes if $|\Sigma| = |G|$,
equivalently the action of G on Σ is transitive (one orbit).

Def A conjugacy class $C \subseteq G$ is <u>rational</u> if

$g \in C \Rightarrow g^k \in C$ for all k coprime to order of g.

Ex $G = S_n$ conj. classes $\overset{1:1}{\longleftrightarrow}$ cycle types

Cycle type is unchanged under $g \mapsto g^k$ [e.g. transposition^k = transposition for $(k,2)=1$]

$\Rightarrow$ Every conjugacy class in S_n is rational.

Ex $G = C_3 = \{1, g, g^2\}$

$\{1\}$ rational conjugacy class

$\{g\} \underset{x \mapsto x^2}{\overset{x \mapsto x^2}{\rightleftarrows}} \{g^2\}$ not rational

$G=C_3$	1	g	g^2
1	1	1	1
χ	1	ζ_3	ζ_3^2
χ^2	1	ζ_3^2	ζ_3

rational conjugacy class

$x \mapsto x^2$

$x \mapsto x^2$

Rmk C is rational $\Leftrightarrow$ $\chi(C) \in \mathbb{Q}$ for every irr. character χ of G

Generally, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the conjugacy classes through its action on the columns of the character table.

Thm (Basic Rigidity Theorem – Belyi, Fried, Matzat, Shih, Thompson).

Let $(C_1, \dots, C_\ell)$ be a rigid ℓ-tuple of rational conjugacy classes, and $P_1, \dots, P_\ell \in \mathbb{P}^1(\mathbb{Q})$.

Then there exists a unique regular G-covering $X \to \mathbb{P}^1_{\mathbb{Q}}$ defined over $\mathbb{Q}$, that is unramified outside $\{P_1, \dots, P_\ell\}$ and has inertia at P_i gen. by elt. of C_i.

Thm (Variant; Serre) If $(C_1, \dots, C_\ell)$ is a rigid ℓ-tuple, stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $(P_1, \dots, P_\ell) \subseteq \mathbb{P}^1(\overline{\mathbb{Q}})$ is anti-isomorphic as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-set to $(C_1, \dots, C_\ell)$ then there is a regular G-covering $X \to \mathbb{P}^1_{\mathbb{Q}}$ defined over $\mathbb{Q}$ that is unramified outside $\{P_1, \dots, P_\ell\}$ and has inertia at P_i gen. by elt. of C_i.

Ex $G = PSL_2(\mathbb{F}_7) \cong GL_3(\mathbb{F}_2)$ second non-abelian simple group; order 168

class	C_1	C_2	C_3	C_4	C_5	C_6
elt. order	1	2	3	4	7	7
size	1	21	56	42	24	24
ρ_1	1	1	1	1	1	1
ρ_2	3	-1	0	1	$\frac{-1+\sqrt{-7}}{2}$	$\frac{-1-\sqrt{-7}}{2}$
ρ_3	3	-1	0	1	$\frac{-1-\sqrt{-7}}{2}$	$\frac{-1+\sqrt{-7}}{2}$
ρ_4	6	2	0	0	-1	-1
ρ_5	7	-1	1	-1	0	0
ρ_6	8	0	-1	0	1	1

Lemma In any group G and conj. classes $C_1, \dots, C_\ell$

$$\#\{(g_1,\dots,g_\ell) \mid g_i \in C_i,\ g_1 g_2 \cdots g_\ell = 1\} = \frac{1}{|G|} \cdot |C_1| \cdots |C_\ell| \sum_{\chi \in \mathrm{Irr}\, G} \frac{\chi(C_1) \cdots \chi(C_\ell)}{\chi(1)^{\ell-2}}$$

Applying this to (C_3, C_5, C_6) we find

$$\#\{(g_3,g_5,g_6) \mid g_3 \in C_3,\ g_5 \in C_5,\ g_6 \in C_6,\ g_3 g_5 g_6 = 1\} =$$

$$= \frac{1}{168} \cdot 56 \cdot 24 \cdot 24 \cdot \left(\frac{1 \cdot 1 \cdot 1}{1} + \frac{-1 \cdot 1 \cdot 1}{8} \right) = \frac{1}{3 \cdot 7 \cdot 8} \cdot 7 \cdot 8 \cdot 3 \cdot 8 \cdot 3 \cdot 8 \cdot \frac{7}{8} = 168.$$

Every such (g_3, g_5, g_6) generates G, (← find one example by hand, then we know there are ≥ 168 of them)

so (C_3, C_5, C_6) is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable rigid triple.

By the Rigidity Thm., $PSL_2(\mathbb{F}_7)$ is a Galois group over $\mathbb{Q}(t)$.

Rmk Shih proved (with a different method involving modular curves), that $PSL_2(\mathbb{F}_p)$ is a Galois group over $\mathbb{Q}$ when $\left(\frac{2}{p}\right) = -1$, $\left(\frac{3}{p}\right) = -1$, or $\left(\frac{7}{p}\right) = -1$.

applies to $p = 7$.

There are many variants of the rigidity method, and it was used to realise all sporadic simple groups but M_{23} over $\mathbb{Q}(t)$, and other simple groups.