G-extensions of number fields

Existence

Of course, any field K has a G-ext. L, namely the triv. ext. But the following question is open.

Question (Inverse Galois problem)
Is every finite group G the Galois grp. of some Galois ext. (= field G-ext.) $L|\mathbb{Q}$?

Rmk known for S_n, A_n, abelian groups, solvable groups, all sporadic finite simple groups except M_{23}, ...

Rmk Any fin. group G embeds into $S_{|G|}$. Therefore, G is the Galois group of some Galois ext. $L|K$:

$$\begin{tikzcd}
L \arrow[dr, dash, "G"] \arrow[dd, dash, "S_{|G|}"'] & \\
& K \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}$$

Counting

Fix a field K and a finite group G. For any fct. $\mathrm{inv}: \{\text{nondeg. } G\text{-ext. of } K\} \to \mathbb{R} \cup \{\infty\}$, let

$$N_{\mathrm{inv}}(T) = \#\{\underline{\text{field}}\ G\text{-ext. } L|K : \mathrm{inv}(L) \leq T\}.$$

[$\mathrm{inv}(L) = \infty$ means that L is ignored / forbidden.]

<u>Question</u> How does $N_{\mathrm{inv}}(T)$ grow as $T \to \infty$?

We need to restrict the set of allowed invariant functions to make sense of this!

<u>Def</u> An <u>invponent</u> is a fct. $d: G \to \mathbb{R}^{\geq 0} \cup \{\infty\}$ satisfying the following properties:

a) $d(hgh^{-1}) = d(g)$ $\forall g, h \in G$ (so d is a class function $d: \{\text{conj. cl. of } G\} \to \mathbb{R}^{\geq 0} \cup \{\infty\}$)

b) $d(g^n) = d(g)$ $\forall g \in G$ $\forall n \in (\mathbb{Z}/|G|\mathbb{Z})^\times$
(if $\langle g \rangle = \langle g' \rangle$, then $d(g) = d(g')$)

c) $d(g) = 0$ if and only if $g = \mathrm{id}$

Def Let d be an invponent and let k be a nonarch. local field with residue field $\mathbb{F}_q$ of characteristic $p \nmid |G|$. Every nondeg. G-ext. $L|k$ is tamely ramified, so $I(L|k) \subseteq G$ is cyclic. Define the <u>invariant associated to d</u> by

$$\mathrm{inv} : \{\text{nondeg. } G\text{-ext. of } k\} \longrightarrow \mathbb{R} \cup \{\infty\}$$
$$L \longmapsto q^{d(g)}, \text{ where}$$
$$I(L|k) = \langle g \rangle .$$

Ex $\mathrm{inv}(L) = 1 \underset{e)}{\Longleftrightarrow} \tau = \mathrm{id} \Leftrightarrow I(L|k) = 1 \Leftrightarrow L|k$ unram.

Def Let K be a number field. We say that an invariant inv of nondeg. G-ext. of K is <u>compatible with</u> an invponent d if for each place v of K, there is a <u>local invariant</u> inv_v of nondeg. G-ext. of K_v such that

i) For any nondeg. G-ext. $L|K$,

$$\mathrm{inv}(L) = \prod_v \mathrm{inv}_v(L \otimes_K K_v).$$

ii) For all but fin. many ("<u>exceptional</u>") places v, the local invariant inv_v is the invariant associated to d.

Rmk Since any L is ramified only at fin. many places v, $\prod_v \mathrm{inv}_v(L \otimes_K K_v)$ is really a finite product.

Def The <u>a-number</u> of d is

$$a = a(d) = \min_{id \neq g \in G} d(g) > 0.$$

Let $\zeta = \zeta_{|G|}$, $U[= U(K)] = Gal(K(\zeta)|K) \leq (\mathbb{Z}/|G|\mathbb{Z})^\times$

$$(\zeta \mapsto \zeta^r) \mapsto r$$

Consider the action of $U \leq (\mathbb{Z}/|G|\mathbb{Z})^\times$ on the set of conjugacy classes C of G given $r.C = C^r$. (Note that $d(r.C) = d(C)$ by property b).)

The <u>b-number</u> is

$$b = b(d, K) = \begin{cases} 1, & a = \infty \\ \#(U \backslash \{\text{conj. cl. } C : d(C) = a\}), & a < \infty. \end{cases}$$

<u>Malle's conjecture on steroids (MCS)</u>

Let K be a number field with invariant inv compatible with invponent d. Then, there is a constant $C = C_{inv} \geq 0$ such that

$$N_{inv}(T) \sim C \cdot T^{\frac{1}{a(d)}} \cdot (\log T)^{b(d,K)-1} \quad \text{for } T \to \infty.$$

<u>Exe A</u> MCS is true when $a(d) = \infty$ (i.e. $d(g) = \infty$ for all $g \neq id$):

$N_{inv}(T) \sim C \cdot T^0 \cdot (\log T)^0 = C$ for $T \to \infty$,

i.e. there are only fin. many field G-ext. $L|K$ s.t. $inv(L) < \infty$.

<u>Pf</u> For all nonexceptional places v, we have $inv_v(L \otimes_K K_v) < \infty$ only if L is unram. at v.

Hence, any L with $inv(L) < \infty$ can be ramified at only the fin. many exceptional v. For each exceptional v, there are only fin. many nondeg. G-ext. of K_v.

$\Rightarrow$ The disc. D_L is bounded.

$\Rightarrow$ There are only fin many possible L. $\square$

Exe B Assume $G \neq 1$.

$$\mathrm{disc}(L) := |\mathrm{Nm}_{K|\mathbb{Q}} D_{L|K}| = \frac{|D_L|}{|D_K|^{[L:K]}}$$

rel. disc. formula

is compatible with

$$d(g) = |G| \cdot \left(1 - \frac{1}{\mathrm{ord}(g)}\right)$$

(cf. computation of discr. of tamely ramified ext. of local fields).

$a(d) = |G| \cdot (1 - \frac{1}{p})$ where p is the smallest prime factor of $|G|$.

$$b(d, K) = \begin{cases} 1, & G = C_p, K = \mathbb{Q} \quad \left(U = (\mathbb{Z}/p\mathbb{Z})^\times \circlearrowright \{0 \neq a \in \mathbb{Z}/p\mathbb{Z}\}\right) \\ p-1, & G = C_p, K = \mathbb{Q}(\zeta_p) \quad \left(U = 1 \circlearrowright \{0 \neq a \in \mathbb{Z}/p\mathbb{Z}\}\right) \\ \left[\frac{n}{2}\right], & G = S_n, K \text{ arbitrary} \\ & (U \text{ acts trivially on } \{\text{conj. cl. } C \text{ of order } 2\}) \\ \vdots \end{cases}$$

Ese C Let $H \subseteq G$. Then,

$$\mathrm{disc}^H(L) := \mathrm{disc}(L^H) = |\mathrm{Nm}_{K|\mathbb{Q}} D_{L^H|K}| = \frac{|D_{L^H}|}{|D_K|^{[L:K]}}$$

is compatible with

$d(g) = [G:H] - \#$(cycles in the perm. representing left-mult by g in G/H)

Ese C.1 Let $n \geq 2$, $G = S_n$, $H = \mathrm{Stab}(1) \subseteq S$

set of perm. of $\{1, \dots, n\}$ fixing 1

We obtain a natural identification

$G/H \Longleftrightarrow \{1, \dots, n\}$, which is S_n-equivariant.

$\Rightarrow d(g) = n - \#$(cycles in $g \in S_n$)

$\Rightarrow a(d) = 1$ (and $d(g) = 1 \Leftrightarrow g$ has cycle type $(2, 1, \dots, 1)$ $\Leftrightarrow g$ is a transposition)

$b(d, K) = 1$ (all transpositions in S_n lie in the same conjugacy class).

Hence MCS $\Rightarrow N_{\mathrm{disc}\,H}(T) \sim C_n \cdot T$ for $T \to \infty$.

$\quad\quad\quad\quad //$

$\#\{$deg. n field ext. $L'|K$
whose Galois closure has
Galois group S_n
and s.t. $\mathrm{disc}(L') \leq T\}$

<u>Exc C.2</u> Let $n \geq 2$, G any transitive subgr. of S_n,

$H = G \cap \mathrm{Stab}(1) \subseteq G$.

We again obtain the G-equiv. bij.

$G/H \longleftrightarrow \{1, \dots, n\}$.

$\Rightarrow d(g) = n - \#(\text{cycles in } g \in S_n)$.

<u>If G contains a transposition</u>:

$a(d) = 1$

Any two transp. in a transitive subgr. G of S_n are conjugate.

$\Rightarrow b(d, K) = 1$.

Hence, MCS $\Rightarrow N_{\mathrm{disc}\,H}(T) \sim C_{n,G} \cdot T$ for $T \to \infty$

$\quad\quad\quad\quad //$

$\#\{$deg. n field ext. $L'|K$ whose Gal. closure
has Gal. grp. $G \subseteq S_n$ (up to conj.)
and $\mathrm{disc}(L') \leq T\}$

If G contains no transp.:

$a(d) \geq 2$

Hence, MCS $\Rightarrow$

$N_{\mathrm{disc}\, H}(T) \ll T^{\frac{1}{2}} (\log T)^{b-1}$ for $T \to \infty$.

$\shortparallel$

$\#\{$deg. n field ext. $L'|K$
whose Gal. closure
has Galois group $G \leq S_n$
and $\mathrm{disc}(L') \leq T\}$

Cor of ex. C.1, C.2

MCS $\Rightarrow \#\{$deg. n field ext. $L'|K$ s.t. $\mathrm{disc}(L') \leq T\} \sim c_n' \cdot T$
for $T \to \infty$

Furthermore, ordering L' by $\mathrm{disc}(L')$,

$\mathbb{P}($Gal. cl. of $L'|K$ has Gal. grp. S_n $|$ L' as above$) = 1$

if and only if n is prime.

Pf $\mathbb{P} = 1 \iff \nexists$ transitive subgr. $G \subsetneqq S_n$ containing
a transposition

$\iff n$ prime. $\square$

<u>Ex</u> If $n = r \cdot s$ with $r, s \geq 2$, partition $\{1, \dots, n\}$ into r sets $A_1, \dots, A_r$ of sizes s. Then,

$$G := \{ g \in S_n \mid \exists \pi \in S_r : \forall 1 \leq t \leq r : \forall i \in A_t : g(i) \in A_{\pi(t)} \}$$

is a transitive proper subgroup of S_n and contains a transposition.