Construction of fields with solvable Galois group

Carlo Sircana
Technische Universität Kaiserslautern

24/09/2018, Tübingen
Annual meeting SFB TRR 195

Theory and Practice

Shafarevich's theorem

Let G be a solvable group. Then there exists a number field K such that $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$.

Constructive problem

Let G be a solvable group and $B \in \mathbf{N}$. Find all the number fields K such that $\mathrm{Gal}(K/\mathbf{Q}) \simeq G$ and $\mathrm{disc}(K) \leq B$.

Finding a number field means finding $f \in \mathbf{Q}[x]$ such that $K \simeq \mathbf{Q}[x]/(f)$.

Class field theory

Since G is solvable, we construct K as a tower of abelian extensions.

$$G \;—\; G_1 = [G,G] \;—\; \cdots \;——\; G_{n-1} \;——\; \{e\}$$

$$\mathbf{Q} \;—\; K_1 = \mathrm{Fix}(G_1) \;—\; \cdots \;——\; K_{n-1} \;——\; K$$

We use Class Field Theory to construct these extensions.

Objects to be computed

- Ray Class Groups
- Conductor and discriminant of abelian extensions
- Automorphisms
- Invariant subgroups of Ray Class Groups under the Galois action

Brauer Obstruction

Let $K/\mathbf{Q}$ be a Galois extensions with group G and assume that we want to find an extension L/K of degree p (a prime number) with $\mathrm{Gal}(L/\mathbf{Q}) = \tilde{G}$.

$$1 \to \mu_p \longrightarrow \tilde{G} \longrightarrow G \to 1$$

The extension correspond to a cocycle $c \in \mathrm{H}^2(G, \mu_p)$.

Theorem

The problem has a solution if and only if c is zero in $\mathrm{H}^2(G, K^\times)$.

There is an isomorphism $\mathrm{H}^2(G, K^\times) \simeq \mathrm{Br}(K|\mathbf{Q})$ and we check if the corresponding crossed product algebra is split.

Some numerical results

If G is a transitive permutation group of degree n and $0 \leq r \leq n$, we set $d_0(n, r, G)$ to be the smallest value of $|d_K|$, where $[K : \mathbf{Q}] = n$, K has r real embeddings, and if L is the Galois closure of K over $\mathbf{Q}$, then $\mathrm{Gal}(L/\mathbf{Q}) \cong G$ as a permutation group on the embeddings of K in L.

Results

- $d_0(15, 1, D_{15}) = 239^7$,
- $d_0(15, 3, D_5 \times C_3) = 7^{12} \cdot 17^6$,
- $d_0(15, 5, S_3 \times C_5) = 2^{10} \cdot 11^{13}$,
- $d_0(36, 36, C_9 \rtimes C_4) = 1129^{27}$,
- $d_0(36, 0, C_9 \rtimes C_4) = 3^{88} \cdot 29^{27}$.