Schur σ-groups

Michael Bush
Washington and Lee University

August 5, 2013

Motivation

Let K be a number field and let $\mathcal{O}_K$ be the ring of integers of K.

$\mathcal{O}_K$ is sometimes a UFD (Unique Factorization Domain) and sometimes not.

Embedding Problem

Does there always exist a finite extension L/K such that $\mathcal{O}_L$ is a UFD?

Motivation

Proposition

There exists L/K finite with $\mathcal{O}_L$ a UFD $\Leftrightarrow$ Hilbert class tower of K is finite.

Hilbert class field tower of K

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \ldots$$

where K_{n+1} = maximal unramified *abelian* extension of K_n. We have $\mathrm{Gal}\,(K_{n+1}/K_n) \cong Cl(K_n)$ for all $n \geq 0$.

Motivation

Hilbert p-class field tower of K

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \ldots$$

where K_{n+1} = maximal unramified *abelian* p-extension of K_n.

Theorem (Golod-Shafarevich, 1964)

Embedding problem has a negative answer. Gave explicit examples of K with infinite Hilbert p-class tower for a prime p
($\Rightarrow$ infinite Hilbert class tower).

Example

$K = \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13})$ has infinite 2-class tower.

Schur σ-groups

Let $K^\infty = \cup_{n\geq 0} K_n$ and $G = G_{K,p} = \mathrm{Gal}(K^\infty/K)$.

Koch and Venkov (1975): If K is imaginary quadratic and p is an odd prime then G is a Schur σ-group.

Definition

Let G be a pro-p group with generator rank d and relation rank r. G is called a **Schur σ-group** if:

- $d = r$ ("balanced presentation").
- $G^{ab} := G/[G,G]$ is a *finite* abelian group.
- There exists an automorphism $\sigma : G \to G$ with $\sigma^2 = 1$ and such that $\overline{\sigma} : G^{ab} \to G^{ab}$ maps $\overline{x} \mapsto \overline{x}^{-1}$.

Finite Schur σ-groups and towers

Theorem (Koch-Venkov,1975)

If G is a Schur σ-group (p odd) and $d \geq 3$ then G is infinite.

An imaginary quadratic field with finite p-class tower (p odd) must have associated Galois group G with either $d = 1$ or 2 generators.

If $d = 1$ then G is cyclic and the tower has length 1. It follows that if the tower is finite of length > 1 then $d = 2$.

Finite Schur σ-groups and towers

Despite a long history, very few finite examples are known. Until relatively recently all of the known examples of finite towers had length either 1 or 2.

Example (B, 2003)

The field $K = \mathbb{Q}(\sqrt{-d})$ for $d = 445$, 1015 and 1595 has 2-class tower of length 3.

Many more examples have subsequently been found by Nover.

Example (B-Mayer, 2012)

The field $K = \mathbb{Q}(\sqrt{-9748})$ has 3-class tower of length 3.

In case you were wondering...

Finite Schur σ-groups with arbitrarily large derived length do exist.

Let $F = F\langle x, y\rangle$ be the free pro-3 group with $\sigma : F \to F$ defined by $x \mapsto x^{-1}$ and $y \mapsto y^{-1}$.
Define

$$G_n = \langle x, y \mid r_n^{-1}\sigma(r_n), t^{-1}\sigma(t)\rangle$$

where $t = yxyx^{-1}y$ and $r_n = x^3y^{-3^n}$ for $n \geq 1$.

Theorem (Bartholdi–B, 2007)

For $n \geq 1$,

- G_n is a finite 3-group of order 3^{3n+2}.
- G_n is nilpotent of class $2n + 1$.
- G_n has derived length $\lfloor \log_2(3n + 3)\rfloor$.

Invariants of finite Schur σ-groups ($d = 2$, $p = 3$)

A 2-generated 3-group G has 4 subgroups $\{H_i\}_{i=1}^4$ of index 3.

Definition

The **Transfer Target Type (TTT) of** G consists of the 4 groups H_i^{ab} where $H_i^{ab} = H_i/[H_i, H_i]$ is the abelianization of H_i.

Definition

The **Transfer Kernel Type (TKT) of** G consists of the kernels of the transfer (Verlagerung) maps from G^{ab} to H_i^{ab} for $i = 1$ to 4.

If $G = G_{K,3}$ then the TTT and TKT of G are explicitly computable in terms of K and certain low degree extensions (3-class groups and capitulation).

Invariants of finite Schur σ-groups ($d = 2$, $p = 3$)

Theorem (B-Mayer, 2012)

Let G be a Schur σ-group satisfying:

(i) $G^{ab} \cong [3,3]$

(ii) $TTT(G) = \{[3,9]^3, [9,27]\}$, and

(iii) $TKT(G) = (\overline{H_1}, \overline{H_4}, \overline{H_3}, \overline{H_1})$ where $\overline{H_i}$ denotes the subgroup in G^{ab} corresponding to H_i.

Then G is one of two possible finite 3-groups of order 3^8. Both have derived length 3.

Corollary

If $G = \mathrm{G}_3^{\infty}(K)$ satisfies the conditions above then K has 3-class tower of length exactly 3. e.g. $K = \mathbb{Q}(\sqrt{-9748})$.

The p-group generation algorithm

We make use of O'Brien's p-group generation algorithm (1990) to find candidates for certain special quotients of G (and eventually G itself).

This approach was first used by Boston and Leedham-Green (2002) on a slightly different but related problem.

Lower exponent p-central series of G

$$G = P_0(G) \geq P_1(G) \geq P_2(G) \geq \dots$$

where $P_n(G) = P_{n-1}(G)^p[G, P_{n-1}(G)]$ for each $n \geq 1$.

If $P_{n-1}(G) \neq 1$ and $P_n(G) = 1$ then we say G has **p-class n**.

The p-group generation algorithm

All d-generated p-groups can be arranged in a tree with root $(\mathbb{Z}/p\mathbb{Z})^d$ at level 1 and the groups of p-class n at level n.

We define edge relations between groups in successive levels as follows:

Edges between vertices at level n and $n-1$:

If G has p-class n and H has p-class $n-1$ then we include an edge $G \to H$ if and only if $G/P_{n-1}(G) \cong H$.

The algorithm provides an effective method for finding the (finitely many) immediate descendants of a given group G and hence enumerating the groups in the tree down to any level.

A sketch of the proof

Theorem (B-Mayer, 2012)

Let G be a Schur σ-group satisfying:

(i) $G^{ab} \cong [3,3]$

(ii) $TTT(G) = \{[3,9]^3, [9,27]\}$, and

(iii) $TKT(G) = (\overline{H_1}, \overline{H_4}, \overline{H_3}, \overline{H_1})$ where $\overline{H_i}$ denotes the subgroup in G^{ab} corresponding to H_i.

Then G is one of two possible finite 3-groups of order 3^8. Both have derived length 3.

We impose the constraints in the theorem to narrow down the search for larger and larger quotients $G/P_c(G)$. This is effective because they involve **inherited properties**.

Inherited Properties

Example

If G_2 is any descendant of G_1 then G_1 is a quotient of G_2 and so G_1^{ab} is a quotient of G_2^{ab}. If we are looking for groups G with $G^{ab} \cong [3,3]$ and we encounter a group G_1 with $G_1^{ab} \cong [3,9]$ or $[3,3,3]$ (or worse) then we can eliminate G_1 and **all of its descendants** from our search.

Similar statements can be made for the abelianizations H_i^{ab}, the kernels of the transfer maps (once G^{ab} has stabilized), the existence of a σ-automorphism etc.

We also make use of a stabilization result due to Nover.

Example

If G_2 is an immediate descendant of G_1 with $G_2^{ab} \cong G_1^{ab}$ then G_i^{ab} remains fixed for all further descendants G_i of G_2.

A sketch of the proof (cont'd)

Starting from $G_1 = G/P_1(G) = [3,3]$, we find unique candidates for the quotients $G_c = G/P_c(G)$ for $2 \leq c \leq 4$ and 2 candidates for G_5.

There are 0 candidates for G_6. ie. no groups of 3-class 6 exist whose structure is consistent with the constraints in the theorem.

Key Observation

If G were infinite then there would be p-class c quotients $G/P_c(G)$ consistent with the constraints for all $c \geq 1$. Hence, **G must be finite**.

The constraints are satisfied exactly for the 2 candidates of 3-class 5 so G must be one of those two groups.

Things to do

- Find criteria for finite towers of length ≥ 4.
- Find results for other choices of p and/or that are independent of machine computation.
- Nonabelian version of the Cohen-Lenstra heuristics (joint work with Boston and Hajir).

THANKS FOR YOUR ATTENTION!