Finding p-class towers of length 3

Michael Bush
Washington and Lee University

(joint work with Daniel Mayer)

May 25, 2013

Basic definitions

Let K be a number field.

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.

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.

Motivation

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 field tower of K is finite.

Proof.

($\Leftarrow$) If the *HCF* tower is finite then $Cl(K_n) = 1$ for some n, so we can take $L = K_n$.
($\Rightarrow$) If $\mathcal{O}_L$ is a UFD then we have $Cl(L) = 1$. This means that L does not have any nontrivial unramified abelian extensions and so $L = LK_1 \supseteq K_1$. Repeating this argument we have $K_n \subseteq L$ for all n and hence the HCF tower must be finite.

□

Motivation

Theorem (Golod-Shafarevich 1964)

Embedding problem has a negative answer. Gave explicit examples of K and p such that the Hilbert p-class field tower of K is infinite ($\Rightarrow$ infinite HCF).

Example

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

Finite towers

Despite a long history, very view 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 field tower of length 3.

Example (B-Mayer)

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

This contradicts an earlier statement about this field by Scholz and Taussky.

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 observed that if K is imaginary quadratic and p is an odd prime then G is a Schur σ-group.

Definition

Let p be odd and 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 $\overline{x} \to \overline{x}^{-1}$.

Finite Schur σ-groups

Theorem (Koch-Venkov,1975)

$$d \geq 3 \;\Rightarrow\; G \text{ infinite.}$$

So, for odd p, an imaginary quadratic field with finite p-class field tower must have associated Galois group with either $d = 1$ or 2 generators.

If the length is greater than 1, then $d = 2$.

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 is $\{H_i^{ab}\}_{i=1}^4$ where $H_i^{ab} = H_i/[H_i, H_i]$.

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.

Finite Schur σ-groups ($d = 2$, $p = 3$)

Let $G' = [G, G]$ and $G'' = [G', G']$.

Theorem (B-Mayer)

Let K be a complex quadratic field and let $G^{(2)} = G_{K,3}/G''_{K,3}$. If

(i) $(G^{(2)})^{ab} \cong [3, 3]$,

(ii) the TTT of $G^{(2)}$ is $[[9, 27], [3, 9]^3]$ or $[[27, 81], [3, 9]^3]$, and

(iii) the TKT of $G^{(2)}$ is (H_2, H_2, H_3, H_1),

then $G_{K,3}$ has derived length 3, ie. K has a 3-class tower of length 3.

One can verify that the field $K = \mathbb{Q}(\sqrt{-9748})$ satisfies the conditions in the theorem.

The proof

We make use of O'Brien's algorithm (1990) for enumerating d-generated p-groups.

Lower 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**.

Vertices at level n:

d-generated p-groups of p-class n.

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

If G has p-class n and H has p-class $n-1$ then we have an edge

$$G \to H \quad \Leftrightarrow \quad G/P_{n-1}(G) \cong H.$$

Enumeration subject to constraints

We impose the constraints in the theorem to narrow down the search. This is effective because they involve **inherited properties**.

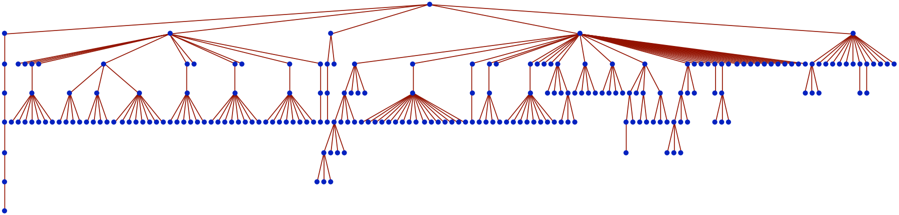
Example

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 the search.

In this case, the given conditions are strong enough that all groups below a certain level are eliminated and the search terminates returning a **complete** and **finite** list of candidates.

Figure : Subtree of the full O'Brien tree ($p = 3$ and $d = 2$).

Computing descendants of each vertex (group) boils down to computing orbits of a certain linear group acting on subspaces of a finite dimensional vector space over $\mathbb{F}_p$.



Work in progress

- Find examples of 3-class towers of length ≥ 4.
- Find results for other choices of p and/or that are independent of machine computation.
- Understand distribution of $G_{K,p}$ as K varies.

Conjecture (Boston-B-Hajir)

Let G be a Schur σ-group of generator rank d. Among imaginary quadratic fields K such that $Cl_p(K)$ has rank d, ordered by discriminant, the probability that $G_{K,p}$ is isomorphic to G is equal to

$$\frac{1}{|\mathrm{Aut}_\sigma(G)|} \cdot \frac{1}{p^{d^2}} \prod_{k=1}^{d} (p^d - p^{d-k})^2$$