Galois groups of unramified 3-extensions of imaginary quadratic fields

Michael Bush
Smith College

October 3, 2009

Some background

p prime number.

$K/\mathbb{Q}$ finite extension.

$\mathcal{O}_K$ = ring of integers of K = integral closure of $\mathbb{Z}$ in K.

Hilbert class 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.

One way in which towers first arose was in connection with the following:

Embedding Problem

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

It can be shown that:

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

One way in which towers first arose was in connection with the following:

Embedding Problem

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

It can be shown that:

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

Golod-Shafarevich (1964) – Answered NO to embedding problem by giving examples of K with infinite p-class towers.

Key ideas

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

G is a pro-p group – compact, totally disconnected topological group whose finite quotients are p-groups.

Key ideas

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

G is a pro-p group – compact, totally disconnected topological group whose finite quotients are p-groups.

Presentations of pro-p groups and cohomology

Generator rank: $d = \dim H^1(G, \mathbb{F}_p)$
Relation rank: $r = \dim H^2(G, \mathbb{F}_p)$

Key ideas

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

G is a pro-p group – compact, totally disconnected topological group whose finite quotients are p-groups.

Presentations of pro-p groups and cohomology

Generator rank: $d = \dim H^1(G, \mathbb{F}_p)$
Relation rank: $r = \dim H^2(G, \mathbb{F}_p)$

Theorem (Golod-Shafarevich; refined by Gaschutz-Vinberg)

$$G \text{ finite } p\text{-group} \Rightarrow r > \frac{d^2}{4}.$$

Galois cohomology:

$$0 \leq r - d \leq r_1 + r_2 - \delta$$

where r_1 = number of real embeddings;
r_2 = number of conjugate pairs of complex embeddings;

$$\delta = \begin{cases} 0, & \text{if } K \text{ contains } p\text{th root of unity;} \\ 1, & \text{otherwise.} \end{cases}$$

Galois cohomology:

$$0 \le r - d \le r_1 + r_2 - \delta$$

where r_1 = number of real embeddings;
r_2 = number of conjugate pairs of complex embeddings;

$$\delta = \begin{cases} 0, & \text{if } K \text{ contains } p\text{th root of unity;} \\ 1, & \text{otherwise.} \end{cases}$$

p odd prime, K imaginary quadratic ($\neq \mathbb{Q}(\zeta_3)$ if $p = 3$):

$r_1 = 0$, $r_2 = 1$, $\delta = 1$.

$$0 \le r - d \le 0 + 1 - 1 = 0 \quad \text{thus} \quad r = d.$$

$$G_{K,p} \text{ finite} \Rightarrow d = r > \frac{d^2}{4} \Rightarrow d < 4.$$

Thus $d \ge 4 \Rightarrow G_{K,p}$ infinite.

$p = 2$, K imaginary quadratic:

$r_1 = 0$, $r_2 = 1$, $\delta = 0$.

$$0 \leq r - d \leq 0 + 1 - 0 = 0 \quad \text{thus} \quad r \leq d + 1.$$

$$G_{K,2} \text{ finite } \Rightarrow\ d + 1 \geq r > \frac{d^2}{4} \Rightarrow d < 2\sqrt{2} + 2.$$

Thus $d \geq 5 \ \Rightarrow\ G_{K,2}$ infinite.

$p = 2$, K imaginary quadratic:

$r_1 = 0$, $r_2 = 1$, $\delta = 0$.

$$0 \leq r - d \leq 0 + 1 - 0 = 0 \quad \text{thus} \quad r \leq d + 1.$$

$$G_{K,2} \text{ finite } \Rightarrow \; d + 1 \geq r > \frac{d^2}{4} \Rightarrow d < 2\sqrt{2} + 2.$$

Thus $d \geq 5 \; \Rightarrow \; G_{K,2}$ infinite.

Finding K with p-class group of large rank leads to examples with infinite p-class towers.

Example:

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

What happens when d is smaller than the given bounds?

Two types of result:

(i) $G_{K,p}$ infinite via indirect application of Golod-Shafarevich Theorem.

(ii) Various finiteness results. eg. $Cl_2(K) \cong C_2 \times C_2 \Rightarrow G_{K,2}$ finite.

Group theoretic restrictions often play an important role.

Schur σ-groups

If K imaginary quadratic, p odd prime, then $G = G_{K,p}$ satisfies:

- $d = r$.
- $G^{ab} := G/[G, G]$ is finite abelian.
- There exists an automorphism $\sigma : G \to G$ with $\sigma^2 = 1$ and such that $\overline{\sigma} : G^{ab} \to G^{ab}$ maps $\overline{x} \to \overline{x}^{-1}$.

Such a group is called a **Schur σ-group.**

Schur σ-groups

If K imaginary quadratic, p odd prime, then $G = G_{K,p}$ satisfies:

- $d = r$.
- $G^{ab} := G/[G, G]$ is finite abelian.
- There exists an automorphism $\sigma : G \to G$ with $\sigma^2 = 1$ and such that $\overline{\sigma} : G^{ab} \to G^{ab}$ maps $\overline{x} \to \overline{x}^{-1}$.

Such a group is called a **Schur σ-group.**

Using this additional structure one can refine Golod-Shafarevich's bound.

Theorem (Koch-Venkov,1975)

K imaginary quadratic, p odd prime.

$$d \geq 3 \ \Rightarrow \ G_{K,p} \text{ infinite.}$$

Finite Schur σ-groups

$$G_{K,p} \text{ finite } \Rightarrow \begin{cases} \text{d} = 1, \text{ cyclic group;} \\ \text{d} = 2. \end{cases}$$

Finite nonabelian Schur σ-groups must satisfy $d = 2$. What sort of groups can arise?

Finite Schur σ-groups

$$G_{K,p} \text{ finite } \Rightarrow \begin{cases} \text{d} = 1, \text{ cyclic group;} \\ \text{d} = 2. \end{cases}$$

Finite nonabelian Schur σ-groups must satisfy $d = 2$. What sort of groups can arise?

One approach to finding such groups is to try "random" presentations: $G = \langle x, y \mid w_1, w_2 \rangle$.

Finite Schur σ-groups

$$G_{K,p} \text{ finite } \Rightarrow \begin{cases} \text{d} = 1, \text{ cyclic group;} \\ \text{d} = 2. \end{cases}$$

Finite nonabelian Schur σ-groups must satisfy $d = 2$. What sort of groups can arise?

One approach to finding such groups is to try "random" presentations: $G = \langle x, y \mid w_1, w_2 \rangle$.

Relations w_1 and w_2 can be selected so that the map $\sigma : F \to F$ (where F free on $\{x, y\}$) defined

$$x \mapsto x^{-1}$$

$$y \mapsto y^{-1}$$

induces a σ-automorphism on G.

For example, take $w_i = w^{-1}\sigma(w)$ or $w\sigma(w)$ for some $w \in F$.

For each group G we check whether it is finite (as a pro-p group) – Take abstract f.p. group and compute p-quotients. Stabilization implies finiteness.

For each group G we check whether it is finite (as a pro-p group) – Take abstract f.p. group and compute p-quotients. Stabilization implies finiteness.

Such experimentation lead to the following family of pro-3 groups:

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

where

$$\begin{aligned} t &= yxyx^{-1}y \\ r_n &= x^3y^{-3^n} \quad \text{for } n \geq 1. \end{aligned}$$

Theorem (Bartholdi–B.)

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 $\lfloor \log_2(3n+3) \rfloor$.

If these groups could be realized as Galois groups $G_{K,p}$ it would imply the existence of arbitrarily large finite p-class towers (open problem).

Sketch of proof:

Let $H_n = \langle x, y \mid x^3, y^{3^n}, t^{-1}\sigma(t)\rangle$.

Can show:

$$1 \to C \to G_n \to H_n \to 1$$

with C central, cyclic of order 3.

The groups H_n form an inverse system.

$$\varprojlim H_n = H \cong \langle x, y \mid x^3, t^{-1}\sigma(t)\rangle$$

Key Lemma

Let $\alpha \in \mathbb{Z}_3$ satisfy $\alpha^2 = -2$. The map $\rho : H \to P \subseteq \mathrm{SL}_2(\mathbb{Z}_3)$, given by

$$x \mapsto \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad y \mapsto \alpha \begin{pmatrix} 0 & 1/2 \\ 1 & -1 \end{pmatrix},$$

is an isomorphism between H and a pro-3 Sylow subgroup P of $\mathrm{SL}_2(\mathbb{Z}_3)$.

With this explicit realization of H it is now possible to compute properties of the groups H_n and then for G_n.

A different approach to finding examples

Rather than picking random presentations, one could try to search systematically through finite p-groups with $d = 2$ generators. (This sort of approach first used by Boston and Leedham-Green in 2002.)

A different approach to finding examples

Rather than picking random presentations, one could try to search systematically through finite p-groups with $d = 2$ generators. (This sort of approach first used by Boston and Leedham-Green in 2002.)

This can be done using the p-group generation algorithm (E. O'Brien, 1990). Groups with fixed generator rank d are arranged in a tree structure. The algorithm takes a group and computes the (finite) list of descendants.

Starting from the root $\prod_{k=1}^{d} C_p$ one can (in theory) compute the tree down to any level. Every d-generated group occurs somewhere in this tree.

Tree structure for d-generated p-groups

Lower p-central series:

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

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

Tree structure for d-generated p-groups

Lower p-central series:

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

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.

Tree structure for d-generated p-groups

Lower p-central series:

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

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

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

We are interested in Schur σ-groups.

Possession of a σ-automorphism is an inherited property. While generating the tree, whenever we encounter a group without a σ-automorphism we can ignore it and its descendants (we “prune the tree”).

We are interested in Schur σ-groups.

Possession of a σ-automorphism is an inherited property. While generating the tree, whenever we encounter a group without a σ-automorphism we can ignore it and its descendants (we "prune the tree").

For those groups that remain we compute cohomology to determine when the condition $d = r$ is satisfied.

Current status of computation: $p = 3$, $d = 2$

Have computed the top levels of the tree when $p = 3$ and $d = 2$ using Magma.

Currently there are 1429 vertices. They split into three types:

- 797 Dead vertices - groups that do not have a σ-automorphism.
- 219 Internal vertices - groups that have a σ-automorphism and whose descendants have been computed.
- 413 Leaves - groups where only partial information is available.

Current status of computation: $p = 3$, $d = 2$

Have computed the top levels of the tree when $p = 3$ and $d = 2$ using Magma.

Currently there are 1429 vertices. They split into three types:

- 797 Dead vertices - groups that do not have a σ-automorphism.
- 219 Internal vertices - groups that have a σ-automorphism and whose descendants have been computed.
- 413 Leaves - groups where only partial information is available.

Of the 413 leaves, 323 possess a σ-automorphism but descendants have not been computed. For the remaining 90, finding a σ-automorphism has not been attempted (size issues).

Current status of computation: $p = 3$, $d = 2$

Have computed the top levels of the tree when $p = 3$ and $d = 2$ using Magma.

Currently there are 1429 vertices. They split into three types:

- 797 Dead vertices - groups that do not have a σ-automorphism.
- 219 Internal vertices - groups that have a σ-automorphism and whose descendants have been computed.
- 413 Leaves - groups where only partial information is available.

Of the 413 leaves, 323 possess a σ-automorphism but descendants have not been computed. For the remaining 90, finding a σ-automorphism has not been attempted (size issues).

Of the $219 + 323 = 542$ groups that possess a σ-automorphism, only 31 satisfy the additional constraint $d = r$.

Figure: The 219 Internal Vertices.

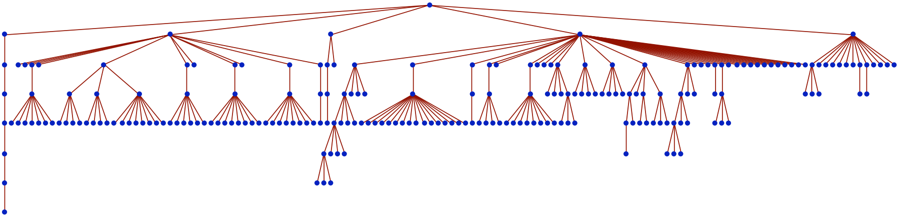
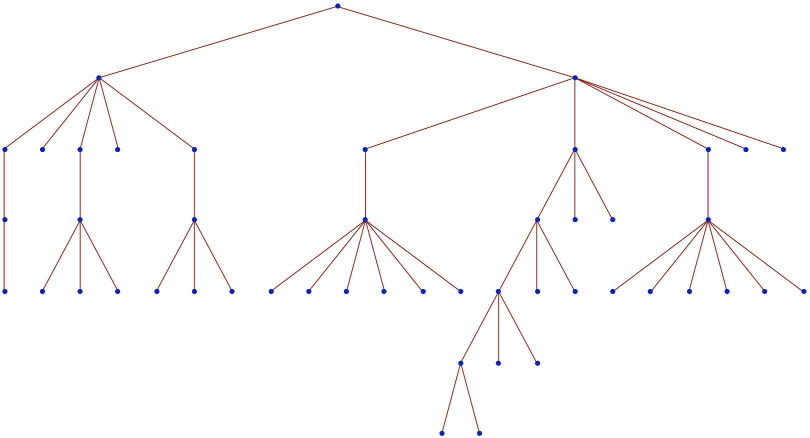


Figure: Subtree generated by the 31 Schur σ-groups.



Some new families

The following presentations appear to describe two new families:

$$G_{1,n} = \langle x, y \mid r_{1,n}^{-1}\sigma(r_{1,n}), t^{-1}\sigma(t)\rangle$$

$$G_{2,n} = \langle x, y \mid r_{2,n}^{-1}\sigma(r_{2,n}), t^{-1}\sigma(t)\rangle$$

where

$$\begin{aligned} t &= yxyx^{-1}y \\ r_{1,n} &= yx^2yx^5yx^{3^n-7} \\ r_{2,n} &= yxyxyx^{3^n-2} \end{aligned}$$

for $n \geq 1$.

From their positions in the tree one would expect both $G_{1,n}$ and $G_{2,n}$ to be descendants of quotients of the same pro-3 group.

This group would appear to be

$$H = \langle x, y \mid r_\infty^{-1}\sigma(r_\infty), t^{-1}\sigma(t)\rangle$$

where t is as before, and

$$r_\infty = yx^2yx^5yx^{-7} \quad \text{or} \quad yxyxyx^{-2}.$$

From their positions in the tree one would expect both $G_{1,n}$ and $G_{2,n}$ to be descendants of quotients of the same pro-3 group.

This group would appear to be

$$H = \langle x, y \mid r_\infty^{-1}\sigma(r_\infty), t^{-1}\sigma(t)\rangle$$

where t is as before, and

$$r_\infty = yx^2yx^5yx^{-7} \quad \text{or} \quad yxyxyx^{-2}.$$

Although similar these two families are less interesting than the previous example in one respect. Their derived lengths appear constant $(= 2)$ in each case.

Things to do:

- Find other families (especially with increasing derived length).

Things to do:

- Find other families (especially with increasing derived length).
- Replace computational conjectures with proofs.

Things to do:

- Find other families (especially with increasing derived length).
- Replace computational conjectures with proofs.
- $p > 3$?

Things to do:

- Find other families (especially with increasing derived length).
- Replace computational conjectures with proofs.
- $p > 3$?
- Realization of abstract groups as Galois groups $G_{K,p}$.