Martinet's question on Hilbert 2-class field towers

Victor Wang

Massachusetts Institute of Technology
Duluth REU 2015
Advised by Joe Gallian

January 7, 2016

Background: Class group and Hilbert class field

- A number field K has a (finite abelian) *ideal class group* $\mathrm{Cl}(K)$ measuring the failure of unique factorization.
- Class field theory distinguishes the *Hilbert class field* K^1 (Galois, abelian over K) with $\mathrm{Gal}(K^1/K) \simeq \mathrm{Cl}(K)$ (theme: extrinsic vs. intrinsic).
- Example: $K = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{(-4)(-3)})$ is a UFD, so $K^1 = K$.

Background: Class group and Hilbert class field

- A number field K has a (finite abelian) *ideal class group* $\mathrm{Cl}(K)$ measuring the failure of unique factorization.
- Class field theory distinguishes the *Hilbert class field* K^1 (Galois, abelian over K) with $\mathrm{Gal}(K^1/K) \simeq \mathrm{Cl}(K)$ (theme: extrinsic vs. intrinsic).
- Example: $K = \mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{(-4)(-3)})$ is a UFD, so $K^1 = K$.
- One definition of K^1: the maximal *abelian* extension L of K *unramified* at not just the usual (nonzero) *finite* primes $\wp \in \operatorname{Spec} \mathcal{O}_K$, but also...
- "unramified at the *infinite* primes", i.e. no *real embedding* $K \hookrightarrow \mathbb{R}$ extends to an embedding $L \hookrightarrow \mathbb{C}$ with nonreal image.

Background: Hilbert class field towers and p^∞ version

- Can iterate $K^{i+1} := (K^i)^1$ to get *Hilbert class field tower*

$$K \subseteq K^1 \subseteq K^2 \subseteq \cdots \subseteq K^\infty$$

(infinite tower of extensions), with *top* $K^\infty := \bigcup_{n \geq 0} K^n$.
- We call the tower *finite* iff $[K^\infty : K] < \infty$ (tower stabilizes); otherwise *infinite*. (Aside: the tower is finite iff K can be embedded in a UFD.)

Background: Hilbert class field towers and p^∞ version

- Can iterate $K^{i+1} := (K^i)^1$ to get *Hilbert class field tower*

$$K \subseteq K^1 \subseteq K^2 \subseteq \cdots \subseteq K^\infty$$

  (infinite tower of extensions), with *top* $K^\infty := \bigcup_{n \geq 0} K^n$.
- We call the tower *finite* iff $[K^\infty : K] < \infty$ (tower stabilizes); otherwise *infinite*. (Aside: the tower is finite iff K can be embedded in a UFD.)
- Our focus: analogous p-tower built from Hilbert p-class fields.
- Fix a prime p. Let $K^1_{(p)} \leq K^1$ be the *Hilbert p-class field* of K, i.e. the maximal p-power-degree Galois sub-extension of K^1/K.

Background: History of towers

- History: Artin et al. (1920s) thought a refinement of Minkowski discriminant bound might prove uniform finiteness of towers (c.f. familiar $\mathbb{Q}$ case), despite

Theorem (Scholz (1929))

For any prime p and every integer $n \geq 1$, there exists a C_p-extension $K/\mathbb{Q}$ such that $K_{(p)}^{n+1} \neq K_{(p)}^{n}$.

- But Artin, Furtwängler, and Scholz at least suspected the "group-theoretical method" would not prove uniform finiteness.

Background: History of towers

- History: Artin et al. (1920s) thought a refinement of Minkowski discriminant bound might prove uniform finiteness of towers (c.f. familiar $\mathbb{Q}$ case), despite

Theorem (Scholz (1929))

For any prime p and every integer $n \geq 1$, there exists a C_p-extension $K/\mathbb{Q}$ such that $K_{(p)}^{n+1} \neq K_{(p)}^{n}$.

- But Artin, Furtwängler, and Scholz at least suspected the "group-theoretical method" would not prove uniform finiteness.
- In fact, it more or less proves the opposite...

Golod–Shafarevich criterion for infinitude of towers

- But Artin, Furtwängler, and Scholz at least suspected the "group-theoretical method" would not prove uniform finiteness.
- In fact, it more or less proves the opposite...

Theorem (Vinberg/Gaschütz refinement of Golod–Shafarevich (1960s))

Fix a number field K (with unit group $\mathcal{O}_K^\times$) and a prime p. Then K has infinite p-tower if

$$\operatorname{rank}_p \operatorname{Cl}(K) \geq 2 + 2\sqrt{1 + \operatorname{rank}_p(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p)}.$$

Golod–Shafarevich criterion for infinitude of towers

- But Artin, Furtwängler, and Scholz at least suspected the "group-theoretical method" would not prove uniform finiteness.
- In fact, it more or less proves the opposite...

Theorem (Vinberg/Gaschütz refinement of Golod–Shafarevich (1960s))

Fix a number field K (with unit group $\mathcal{O}_K^\times$) and a prime p. Then K has infinite p-tower if

$$\operatorname{rank}_p \mathrm{Cl}(K) \geq 2 + 2\sqrt{1 + \operatorname{rank}_p(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p)}.$$

- $\operatorname{rank}_p(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^p)$ is easily computed using Dirichlet's unit theorem.
- $\operatorname{rank}_p \mathrm{Cl}(K)$ is easy in special cases (esp. using genus theory).

Martinet's question (specialize to imaginary quadratics)

- Recap: **Golod–Shafarevich criterion** in terms of class group and unit group of K.
- Let's specialize Golod–Shafarevich to K an imaginary quadratic number field.

Corollary

An imaginary quadratic K has infinite 2-tower if $\operatorname{rank}_2 \mathrm{Cl}(K) \geq 5$*, i.e. if the discriminant Δ_K has 6 prime factors (genus theory).*

Question (Martinet (1978))

What if $\operatorname{rank}_2 \mathrm{Cl}(K) = 4$*, i.e. if Δ_K has 5 prime factors? Must K still always have infinite 2-tower?*

Martinet's question (specialize to imaginary quadratics)

- Recap: **Golod–Shafarevich criterion** in terms of class group and unit group of K.
- Let's specialize Golod–Shafarevich to K an imaginary quadratic number field.

Corollary

An imaginary quadratic K has infinite 2-tower if $\operatorname{rank}_2 \mathrm{Cl}(K) \geq 5$, i.e. if the discriminant Δ_K has 6 prime factors (genus theory).

Question (Martinet (1978))

What if $\operatorname{rank}_2 \mathrm{Cl}(K) = 4$, i.e. if Δ_K has 5 prime factors? Must K still always have infinite 2-tower?

Remark

No known counterexamples. Martinet was inspired also by Odlyzko (1976) "root discriminant" bounds, as root discriminant $|\Delta_K|^{1/[K:\mathbb{Q}]}$ is constant in unramified towers.

Background: Prime discriminants and genus theory

- Extrapolating from $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{(-4)(-3)})$ earlier: for any quadratic number field K with t (finite) ramified primes, we have a unique discriminant factorization

$$\Delta_K = p_1^* \cdots p_t^*$$

into t pairwise coprime *prime (power) discriminants* p_i^*, ...

Background: Prime discriminants and genus theory

- Extrapolating from $\mathbb{Q}(\sqrt{3}) = \mathbb{Q}(\sqrt{(-4)(-3)})$ earlier: for any quadratic number field K with t (finite) ramified primes, we have a unique discriminant factorization

$$\Delta_K = p_1^* \cdots p_t^*$$

into t pairwise coprime *prime (power) discriminants* p_i^*, ...

- ... defined so that $2^* \in \{+8, -8, -4\}$ and

$$p^* = (-1)^{(p-1)/2} p \equiv 1 \pmod 4$$

for odd primes p.

- Classical genus theory (dating back to Euler and Gauss) gives $\operatorname{rank}_2 \operatorname{Cl}(K) \in \{t-1, t-2\}$, and more.
- *Relative* genus theory relates 2-rank with ramification in general, even over base fields other than $\mathbb{Q}$...

Main idea in literature for Martinet's question

- Let $K/\mathbb{Q}$ be an imaginary quadratic with $\Delta_K = p_1^* \cdots p_5^* < 0$ (as in Martinet's question on infinitude of $K_{(2)}^{\infty}/K$).
- Take $L/\mathbb{Q}$ a finite subfield of $K_{(2)}^{\infty}/\mathbb{Q}$ (the 2-tower of K).
- **Golod–Shafarevich** says that field $KL = L(\sqrt{\Delta_K})$, hence K, has an infinite 2-tower if $\operatorname{rank}_2 \mathrm{Cl}(KL) \geq 2 + 2\sqrt{1 + [L : \mathbb{Q}]}$.

$$\begin{tikzcd}[column sep=small]
 & KL = L(\sqrt{\Delta_K}) \arrow[dl, dash, "\text{unramified}"'] \arrow[dr, dash] & \\
K = \mathbb{Q}(\sqrt{\Delta_K}) \arrow[dr, dash] & & L \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

genus theory: $\operatorname{rank}_2 \mathrm{Cl}(KL) \gtrsim \operatorname{ram}(KL/L)$

Say $L/\mathbb{Q}$ is unramified at $m \geq 1$ primes $p_1, \ldots, p_m$ dividing Δ_K. Then the main (i.e. non-archimedean) contribution to $\operatorname{ram}(KL/L)$ is **splitting** $\#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$ in $L/\mathbb{Q}$.

Main idea in literature for Martinet's question

- Let $K/\mathbb{Q}$ be an imaginary quadratic with $\Delta_K = p_1^* \cdots p_5^* < 0$ (as in Martinet's question on infinitude of $K_{(2)}^{\infty}/K$).
- Take $L/\mathbb{Q}$ a finite subfield of $K_{(2)}^{\infty}/\mathbb{Q}$ (the 2-tower of K).
- **Golod–Shafarevich** says that field $KL = L(\sqrt{\Delta_K})$, hence K, has an infinite 2-tower if $\operatorname{rank}_2 \mathrm{Cl}(KL) \geq 2 + 2\sqrt{1 + [L : \mathbb{Q}]}$.

$$\begin{tikzcd}
 & KL = L(\sqrt{\Delta_K}) \arrow[dl, dash, "\text{unramified}"'] \arrow[dr, dash] & \\
K = \mathbb{Q}(\sqrt{\Delta_K}) \arrow[dr, dash] & & L \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

genus theory: $\operatorname{rank}_2 \mathrm{Cl}(KL) \gtrsim \operatorname{ram}(KL/L)$

idea: want large $\#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$

Say $L/\mathbb{Q}$ is unramified at $m \geq 1$ primes $p_1, \ldots, p_m$ dividing Δ_K. Then the main (i.e. non-archimedean) contribution to $\operatorname{ram}(KL/L)$ is **splitting** $\#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$ in $L/\mathbb{Q}$.

Previous progress on Martinet's question, in terms of Δ_K

- Recap: For Martinet's question, suffices to find suitable L with large **splitting** count $\#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$.
- Mouhib (2010), improving on Sueyoshi (2004), proved infinite 2-towers when $\Delta_K = p_1^* \cdots p_5^*$ has exactly 1 *negative* prime discriminant, say p_5^*, using $L \approx \mathbb{Q}(\sqrt{p_1^*}, \ldots, \sqrt{p_4^*})$ (totally real, so hard to extend method).

Previous progress on Martinet's question, in terms of Δ_K

- Recap: For Martinet's question, suffices to find suitable L with large **splitting** count $\#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$.
- Mouhib (2010), improving on Sueyoshi (2004), proved infinite 2-towers when $\Delta_K = p_1^* \cdots p_5^*$ has exactly 1 *negative* prime discriminant, say p_5^*, using $L \approx \mathbb{Q}(\sqrt{p_1^*}, \ldots, \sqrt{p_4^*})$ (totally real, so hard to extend method).

The other best results mimic Martinet (1978), by taking L inside the *(narrow) genus field* $\mathbb{Q}(\sqrt{p_1^*}, \ldots, \sqrt{p_5^*})$ of $K = \mathbb{Q}(\sqrt{\Delta_K})$.

- Hajir (1996, 2000), Benjamin (2001, 2002), and Sueyoshi (2004, 2009, 2010) systematically established infinite 2-towers in many *Rédei matrix* (1930s) cases, i.e. by casework on pairwise Kronecker symbols $(\frac{p_i^*}{p_j})$.
- However, many cases remain open, especially for small $\operatorname{rank}_4 \operatorname{Cl}(K)$.

Schmithals' 2-class field idea for Martinet's question

- Goal (recap): find $L/\mathbb{Q} \subseteq K^{\infty}_{(2)}/\mathbb{Q}$ with lots of **splitting**.
- Schmithals' idea (1980): take $L = F^{1}_{(2)}$ (Hilbert 2-class field) for a (quadratic) field F.
- Motivation: *decomposition law*, e.g. if a rational prime p is **inert** in $F/\mathbb{Q}$, then the prime ideal $p\mathcal{O}_F$ is **principal**, hence **totally split** in F^1/F, so also totally split in L/F.

Schmithals' 2-class field idea for Martinet's question

- Goal (recap): find $L/\mathbb{Q} \subseteq K^{\infty}_{(2)}/\mathbb{Q}$ with lots of **splitting**.
- Schmithals' idea (1980): take $L = F^{1}_{(2)}$ (Hilbert 2-class field) for a (quadratic) field F.
- Motivation: *decomposition law*, e.g. if a rational prime p is **inert** in $F/\mathbb{Q}$, then the prime ideal $p\mathcal{O}_F$ is **principal**, hence **totally split** in F^1/F, so also totally split in L/F.
- (In fact, it is *harder* to guarantee lots of splitting in $L/\mathbb{Q}$ when p splits in $F/\mathbb{Q}\ldots$)

Theorem (W. (2015))

For distinct primes $\ell_1, \ell_2 \equiv 1 \pmod 4$, let $F = \mathbb{Q}(\sqrt{\ell_1 \ell_2})$. If p is prime with $(\frac{\ell_1}{p}) = (\frac{\ell_2}{p}) = -1$, then (p) splits into exactly 2 primes in the extension $L/\mathbb{Q}$.

Remark

Dominguez, Miller, and Wong (2013) used a similar result to prove infinitude of imaginary quadratic fields with $\#\mathrm{Cl}(F)$ of any given 2-adic valuation.

Progress on Martinet's question from Schmithals' 2-class field idea

- Goal (recap): find suitable $L/\mathbb{Q} \subseteq K_{(2)}^{\infty}/\mathbb{Q}$ with lots of **splitting**, i.e. $\#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$ should be large.
- Recap: Schmithals' idea (1980) of looking at $L = F_{(2)}^1$ for a choice of quadratic field F.

Progress on Martinet's question from Schmithals' 2-class field idea

- Goal (recap): find suitable $L/\mathbb{Q} \subseteq K^{\infty}_{(2)}/\mathbb{Q}$ with lots of **splitting**, i.e. $\#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid p_1 \cdots p_m\}$ should be large.
- Recap: Schmithals' idea (1980) of looking at $L = F^1_{(2)}$ for a choice of quadratic field F.
- Choosing among $F \subseteq K^{\infty}_{(2)}$ with 4 prime discriminants, Benjamin (2015) partially addressed several open cases with $\operatorname{rank}_4 \operatorname{Cl}(K) \in \{1, 2\}$.
- Choosing among $F \subseteq K^{\infty}_{(2)}$ with 3 or 2 prime discriminants, we (2015) do the same when $\operatorname{rank}_4 \operatorname{Cl}(K) \in \{0, 2\}$, using tools of the following flavor.

Lemma (W. (2015))

Say $p_4^*, p_5^* > 0$, and let $F := \mathbb{Q}(\sqrt{p_4^* p_5^*})$. If $8 \mid \#\operatorname{Cl}(F)$ and at least 1 of p_1, p_2, p_3 is inert in $F/\mathbb{Q}$, then K has infinite 2-tower.

Example for Martinet's question

Lemma (W. (2015))

Say $p_4^*, p_5^* > 0$, and let $F := \mathbb{Q}(\sqrt{p_4^* p_5^*})$. If $8 \mid \#\mathrm{Cl}(F)$ and at least 1 of p_1, p_2, p_3 is inert in $F/\mathbb{Q}$, then K has infinite 2-tower.

- When the Lemma fails, it is natural to ask (assuming K has infinite 2-tower) *where* the failure comes from: **Golod–Shafarevich**, or the **genus theory** input?

Example for Martinet's question

Lemma (W. (2015))

Say $p_4^*, p_5^* > 0$*, and let* $F := \mathbb{Q}(\sqrt{p_4^* p_5^*})$*. If* $8 \mid \#\mathrm{Cl}(F)$ *and at least* 1 *of* p_1, p_2, p_3 *is inert in* $F/\mathbb{Q}$*, then* K *has infinite* 2*-tower.*

- When the Lemma fails, it is natural to ask (assuming K has infinite 2-tower) *where* the failure comes from: **Golod–Shafarevich**, or the **genus theory** input?

Example (W. (2015))

Take $K = \mathbb{Q}(\sqrt{(-7)(-3)(-8)(+29)(+5)})$, with $(\frac{+29}{7}) = +1$ and $(\frac{+5}{7}) = -1$, so 7 is inert in $F := \mathbb{Q}(\sqrt{(+29)(+5)})$. Here F has class number 4, so its Hilbert 2-class field $L := F^1_{(2)}$ coincides with its Hilbert class field F^1, which can be computed in SageMath. (The Lemma fails here since $\#\mathrm{Cl}(F) = 4$.)

Example (cont'd) for Martinet's question

Take $K = \mathbb{Q}(\sqrt{(-7)(-3)(-8)(+29)(+5)})$, with $(\frac{+29}{7}) = +1$ and $(\frac{+5}{7}) = -1$, so 7 is inert in $F := \mathbb{Q}(\sqrt{(+29)(+5)})$. Here F has class number 4, so its Hilbert 2-class field $L := F^1_{(2)}$ coincides with its Hilbert class field F^1.

- The **genus theory** input gives an a priori lower bound on $\operatorname{rank}_2 \operatorname{Cl}(KL)$ from the **splitting** of $7, 3, 2$ in $L/\mathbb{Q}$:

$$\begin{aligned}\operatorname{rank}_2 \operatorname{Cl}(KL) &\geq \#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid (-7)(-3)(-8)\} - 1 \\ &\geq 4 + 2 + 2 - 1 = 7.\end{aligned}$$

Example (cont'd) for Martinet's question

Take $K = \mathbb{Q}(\sqrt{(-7)(-3)(-8)(+29)(+5)})$, with $(\frac{+29}{7}) = +1$ and $(\frac{+5}{7}) = -1$, so 7 is inert in $F := \mathbb{Q}(\sqrt{(+29)(+5)})$. Here F has class number 4, so its Hilbert 2-class field $L := F^1_{(2)}$ coincides with its Hilbert class field F^1.

- The **genus theory** input gives an a priori lower bound on $\operatorname{rank}_2 \mathrm{Cl}(KL)$ from the **splitting** of $7, 3, 2$ in $L/\mathbb{Q}$:

$$\begin{aligned}\operatorname{rank}_2 \mathrm{Cl}(KL) &\geq \#\{\wp \in \operatorname{Spec} \mathcal{O}_L : \wp \mid (-7)(-3)(-8)\} - 1 \\ &\geq 4 + 2 + 2 - 1 = 7.\end{aligned}$$

- In fact, here the bound is tight: the class group $\mathrm{Cl}(KL)$ has cyclic direct sum decomposition $(336, 336, 4, 4, 2, 2, 2)$ (assuming the generalized Riemann hypothesis for a reasonable SageMath run-time), so 2-**rank exactly** 7**—just shy of the** $2 + 2\sqrt{8+1} = 8$ **needed** for Golod–Shafarevich.
- But **Golod–Shafarevich does not take into account the** 4-**rank** of 4, or the 8- and 16- ranks of 2, so it would be nice to have a strengthening incorporating such data.

Thanks for listening!