Heuristics for narrow class groups of abelian number fields

Ben Breen
Joint work with Noam Elkies, Ila Varma, and John Voight.

Dartmouth College

June 12, 2020

Heuristics for narrow class groups

1. Motivation: Cohen-Lenstra
2. Conjectures/results: Abelian number fields of odd degree
3. Model: 2-Selmer group of a number field

Cohen-Lenstra

$\mathrm{Cl}(F)$ The class group — a finite abelian group.

F number field.

Cohen-Lenstra

$\mathrm{Cl}(F)$ The class group — a finite abelian group.

F number field.

Question: What does the class group of a general number field look like as a finite abelian group?

Cohen-Lenstra

Let p be an odd prime. Let $\mathrm{Cl}(F)_p$ denote the Sylow p-subgroup of the class group. Let G_p be a fixed finite abelian p-group.

Cohen-Lenstra

Let p be an odd prime. Let $\mathrm{Cl}(F)_p$ denote the Sylow p-subgroup of the class group. Let G_p be a fixed finite abelian p-group.

Conjecture (Cohen-Lenstra 1984)

As F varies over imaginary quadratic fields ordered by absolute discriminant, the frequency for which $\mathrm{Cl}(F)_p \simeq G_p$ is inversely proportional to $|\operatorname{Aut}(G_p)|$.

Cohen-Lenstra

Let p be an odd prime. Let $\mathrm{Cl}(F)_p$ denote the Sylow p-subgroup of the class group. Let G_p be a fixed finite abelian p-group.

Conjecture (Cohen-Lenstra 1984)

As F varies over imaginary quadratic fields ordered by absolute discriminant, the frequency for which $\mathrm{Cl}(F)_p \simeq G_p$ *is inversely proportional to* $|\operatorname{Aut}(G_p)|$.

Example: Consider the abelian groups of order 9.

Cohen-Lenstra

Let p be an odd prime. Let $\mathrm{Cl}(F)_p$ denote the Sylow p-subgroup of the class group. Let G_p be a fixed finite abelian p-group.

Conjecture (Cohen-Lenstra 1984)

As F varies over imaginary quadratic fields ordered by absolute discriminant, the frequency for which $\mathrm{Cl}(F)_p \simeq G_p$ is inversely proportional to $|\mathrm{Aut}(G_p)|$.

Example: Consider the abelian groups of order 9.

1. $G_3 = \mathbb{Z}/9\mathbb{Z}$ has $|\mathrm{Aut}(G_3)| = 6$.

Cohen-Lenstra

Let p be an odd prime. Let $\mathrm{Cl}(F)_p$ denote the Sylow p-subgroup of the class group. Let G_p be a fixed finite abelian p-group.

Conjecture (Cohen-Lenstra 1984)

As F varies over imaginary quadratic fields ordered by absolute discriminant, the frequency for which $\mathrm{Cl}(F)_p \simeq G_p$ is inversely proportional to $|\mathrm{Aut}(G_p)|$.

Example: Consider the abelian groups of order 9.

1. $G_3 = \mathbb{Z}/9\mathbb{Z}$ has $|\mathrm{Aut}(G_3)| = 6$.
2. $G_3 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has $|\mathrm{Aut}(G_3)| = 48$.

Cohen-Lenstra

Let p be an odd prime. Let $\mathrm{Cl}(F)_p$ denote the Sylow p-subgroup of the class group. Let G_p be a fixed finite abelian p-group.

Conjecture (Cohen-Lenstra 1984)

As F varies over imaginary quadratic fields ordered by absolute discriminant, the frequency for which $\mathrm{Cl}(F)_p \simeq G_p$ *is inversely proportional to* $|\mathrm{Aut}(G_p)|$.

Example: Consider the abelian groups of order 9.

1. $G_3 = \mathbb{Z}/9\mathbb{Z}$ has $|\mathrm{Aut}(G_3)| = 6$.
2. $G_3 = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ has $|\mathrm{Aut}(G_3)| = 48$.

We expect these 3-groups to occur as the 3-Sylow subgroup of the class group in the relative proportions $8 : 1$.

Heuristics for ray class groups

Let $\mathfrak{m}$ be a modulus, i.e., a formal product of an integral ideal and a set of real infinite primes.

Heuristics for ray class groups

Let $\mathfrak{m}$ be a modulus, i.e., a formal product of an integral ideal and a set of real infinite primes.

The class group $\mathrm{Cl}(F)$ is the first in a collection of *ray class groups* $\mathrm{Cl}_{\mathfrak{m}}(F)$ associated to a number field — each a finite abelian group.

Heuristics for ray class groups

Let $\mathfrak{m}$ be a modulus, i.e., a formal product of an integral ideal and a set of real infinite primes.

The class group $\mathrm{Cl}(F)$ is the first in a collection of *ray class groups* $\mathrm{Cl}_{\mathfrak{m}}(F)$ associated to a number field — each a finite abelian group.

Distributions of ray class groups

My research focuses on extending the Cohen-Lenstra heuristics to distributions of ray class groups. Specifically, I focus on two interlinked ray class groups: the narrow class group $\mathrm{Cl}^{+}(F)$ and the ray class group $\mathrm{Cl}_4(F)$ of conductor (4).

Relation between 2 and ∞

Let F be a number field with r_1 real places and r_2 complex places. If A is an abelian group and $m \in \mathbb{Z}_{>0}$, we write

$$A[m] := \{a \in A : a^m = 1\}.$$

Relation between 2 and ∞

Let F be a number field with r_1 real places and r_2 complex places. If A is an abelian group and $m \in \mathbb{Z}_{>0}$, we write

$$A[m] := \{a \in A : a^m = 1\}.$$

Relation between 2 and ∞

The 2-torsion subgroups of the narrow class group and the ray class group of conductor (4) are linked by the relation

$$\mathrm{Cl}_4(F)[2] \simeq \mathrm{Cl}^+(F)[2] \oplus (\mathbb{Z}/2\mathbb{Z})^{r_2}.$$

Relation between 2 and ∞

Let F be a number field with r_1 real places and r_2 complex places. If A is an abelian group and $m \in \mathbb{Z}_{>0}$, we write

$$A[m] := \{a \in A : a^m = 1\}.$$

Relation between 2 and ∞

The 2-torsion subgroups of the narrow class group and the ray class group of conductor (4) are linked by the relation

$$\mathrm{Cl}_4(F)[2] \simeq \mathrm{Cl}^+(F)[2] \oplus (\mathbb{Z}/2\mathbb{Z})^{r_2}.$$

These ray class groups must be modeled simultaneously!

Conjectures/results

Abelian number fields of odd degree

Abelian number fields of odd degree

Let $F \,|\, \mathbb{Q}$ be an abelian extension of odd degree, $\mathbb{Z}_F^\times$ be the units in the ring of integers of F, and $G_F := \mathrm{Gal}(F \,|\, \mathbb{Q})$ the galois group.

Abelian number fields of odd degree

Let $F \mid \mathbb{Q}$ be an abelian extension of odd degree, $\mathbb{Z}_F^\times$ be the units in the ring of integers of F, and $G_F := \mathrm{Gal}(F \mid \mathbb{Q})$ the galois group.

Galois Modules

The action of the galois group on the 2-torsion subgroup of a ray class group $\mathrm{Cl}_\mathfrak{m}(F)[2]$ transforms it into $\mathbb{F}_2[G_F]$-modules.

Abelian number fields of odd degree

Let $F \mid \mathbb{Q}$ be an abelian extension of odd degree, $\mathbb{Z}_F^{\times}$ be the units in the ring of integers of F, and $G_F := \mathrm{Gal}(F \mid \mathbb{Q})$ the galois group.

Galois Modules

The action of the galois group on the 2-torsion subgroup of a ray class group $\mathrm{Cl}_{\mathfrak{m}}(F)[2]$ transforms it into $\mathbb{F}_2[G_F]$-modules.

Since $|G_F|$ is odd then every $\mathbb{F}_2[G_F]$-module is semisimple, i.e, it admits a decomposition as a direct sum of irreducible modules.

Duality

Duality

For $g \in G$, the map $g \mapsto g^{-1}$ induces a map $\iota\colon \mathbb{F}_2[G] \to \mathbb{F}_2[G]$. For an irreducible $\mathbb{F}_2[G]$-module V, we can identify $V \subseteq \mathbb{F}_2[G]$ and then define the **dual module** as $V^\vee := \iota(V)$.

This notion extends to any $\mathbb{F}_2[G]$-module M and we define a module to be **self-dual** if $\mathrm{M} \simeq \mathrm{M}^\vee$.

Duality

Duality

For $g \in G$, the map $g \mapsto g^{-1}$ induces a map $\iota\colon \mathbb{F}_2[G] \to \mathbb{F}_2[G]$. For an irreducible $\mathbb{F}_2[G]$-module V, we can identify $V \subseteq \mathbb{F}_2[G]$ and then define the **dual module** as $V^\vee := \iota(V)$.

This notion extends to any $\mathbb{F}_2[G]$-module M and we define a module to be **self-dual** if $\mathrm{M} \simeq \mathrm{M}^\vee$.

Relation between 2 and ∞ (revisted)

Theorem (Gras)

Let $F \mid \mathbb{Q}$ be an odd galois number field. Then

$$\mathrm{Cl}_4(F)[2] \quad \simeq \quad \mathrm{Cl}^+(F)[2]^\vee.$$

Duality: When is every $\mathbb{F}_2[G]$-module self-dual?

Duality

Let G be a finite abelian group with exponent m. There is a simple criteria to detect when non self-dual $\mathbb{F}_2[G]$-modules exists.

$$\left(\begin{array}{c} \text{Every } \mathbb{F}_2[G]\text{-} \\ \text{module is self-dual} \end{array} \right) \longleftrightarrow \left(\begin{array}{c} -1 \text{ is a power} \\ \text{of 2 in } (\mathbb{Z}/m\mathbb{Z})^\times \end{array} \right)$$

Duality: When is every $\mathbb{F}_2[G]$-module self-dual?

Duality

Let G be a finite abelian group with exponent m. There is a simple criteria to detect when non self-dual $\mathbb{F}_2[G]$-modules exists.

$$\left(\begin{array}{c}\text{Every } \mathbb{F}_2[G]\text{-}\\ \text{module is self-dual}\end{array}\right) \longleftrightarrow \left(\begin{array}{c}-1 \text{ is a power}\\ \text{of 2 in } (\mathbb{Z}/m\mathbb{Z})^\times\end{array}\right)$$

Examples

Duality: When is every $\mathbb{F}_2[G]$-module self-dual?

Duality

Let G be a finite abelian group with exponent m. There is a simple criteria to detect when non self-dual $\mathbb{F}_2[G]$-modules exists.

$$\begin{pmatrix} \text{Every } \mathbb{F}_2[G]\text{-} \\ \text{module is self-dual} \end{pmatrix} \longleftrightarrow \begin{pmatrix} -1 \text{ is a power} \\ \text{of 2 in } (\mathbb{Z}/m\mathbb{Z})^\times \end{pmatrix}$$

Examples

- $G = \mathbb{Z}/3\mathbb{Z}$ — Every module is self-dual.

Duality: When is every $\mathbb{F}_2[G]$-module self-dual?

Duality

Let G be a finite abelian group with exponent m. There is a simple criteria to detect when non self-dual $\mathbb{F}_2[G]$-modules exists.

$$\left(\begin{array}{c}\text{Every } \mathbb{F}_2[G]\text{-} \\ \text{module is self-dual}\end{array}\right) \longleftrightarrow \left(\begin{array}{c}-1 \text{ is a power} \\ \text{of 2 in } (\mathbb{Z}/m\mathbb{Z})^\times\end{array}\right)$$

Examples

- $G = \mathbb{Z}/3\mathbb{Z}$ — Every module is self-dual.
- $G = \mathbb{Z}/5\mathbb{Z}$ — Every module is self-dual.

Duality: When is every $\mathbb{F}_2[G]$-module self-dual?

Duality

Let G be a finite abelian group with exponent m. There is a simple criteria to detect when non self-dual $\mathbb{F}_2[G]$-modules exists.

$$\left(\begin{array}{c}\text{Every } \mathbb{F}_2[G]\text{-} \\ \text{module is self-dual}\end{array}\right) \longleftrightarrow \left(\begin{array}{c}-1 \text{ is a power} \\ \text{of 2 in } (\mathbb{Z}/m\mathbb{Z})^\times\end{array}\right)$$

Examples

- $G = \mathbb{Z}/3\mathbb{Z}$ — Every module is self-dual.
- $G = \mathbb{Z}/5\mathbb{Z}$ — Every module is self-dual.
- $G = \mathbb{Z}/7\mathbb{Z}$ — There are two irreducible non self-dual modules.

Conjectures/results: 2-torsion in narrow class groups

Relationship $\mathrm{Cl}^+(F)$ and $\mathrm{Cl}(F)$

The class group and narrow class group only differ in their 2-Sylow subgroups. We now focus on their 2-torsion subgroups.

Conjectures/results: 2-torsion in narrow class groups

Relationship $\mathrm{Cl}^+(F)$ and $\mathrm{Cl}(F)$

The class group and narrow class group only differ in their 2-Sylow subgroups. We now focus on their 2-torsion subgroups.

Theorem (Taylor-Oriat)

Let F be an abelian number field with odd exponent m. If every $\mathbb{F}_2[G_F]$-module is self-dual (equivalently $-1 \equiv 2^t \pmod{m}$ for some $t \in \mathbb{Z}_{>0}$) then

$$\mathrm{Cl}^+(F)[2] \simeq \mathrm{Cl}(F)[2].$$

Remark

This covers cyclic cubic and quintic number fields ($n = 3, 5$).

Conjectures/results: 2-torsion in narrow class groups

Let F be a cyclic number field of degree seven.

Theorem (B-Varma-Voight)

If $\mathrm{Cl}(F)[2]$ *is not self-dual, then*

$$\mathrm{Cl}^+(F)[2] \simeq \mathrm{Cl}(F)[2] \oplus (\mathbb{Z}/2\mathbb{Z})^3.$$

Additionally, $\mathrm{Cl}^+(F)[2]$ *is self-dual.*

Conjecture (B-Varma-Voight)

If $\mathrm{Cl}(F)[2]$ *is self-dual, then*

$$\mathrm{Cl}^+(F)[2] \simeq \begin{cases} \mathrm{Cl}(F)[2] & \textit{with probability } 7/9; \\ \mathrm{Cl}(F)[2] \oplus (\mathbb{Z}/2\mathbb{Z})^3 & \textit{with probability } 2/9. \end{cases}$$

Unit signature ranks

Unit signature ranks

The **unit signature rank** $\mathrm{sgnrk}(\mathbb{Z}_F^\times)$ is the dimension of the image of the group homomorphism

$$\mathrm{sgn}_\infty : \mathbb{Z}_F^\times \to \prod_{v|\infty} \{\pm 1\} \simeq \mathbb{F}_2^{r_1}$$

which records the signs of a unit in $\mathbb{Z}_F^\times$ under each real embedding.

Unit signature ranks

Unit signature ranks

The **unit signature rank** $\mathrm{sgnrk}(\mathbb{Z}_F^\times)$ is the dimension of the image of the group homomorphism

$$\mathrm{sgn}_\infty\colon \mathbb{Z}_F^\times \to \prod_{v\mid\infty}\{\pm 1\} \simeq \mathbb{F}_2^{r_1}$$

which records the signs of a unit in $\mathbb{Z}_F^\times$ under each real embedding.

The unit signature rank is bounded between $1 \leq \mathrm{sgnrk}(\mathbb{Z}_F^\times) \leq r_1$ with the latter occurring only when $\mathrm{Cl}^+(F) \simeq \mathrm{Cl}(F)$.

Unit signature ranks

Predictions

A cyclic cubic number field has $\operatorname{sgnrk}(\mathbb{Z}_F^\times) = 1, 3$. How frequently do each of these possibilities occur?

Unit signature ranks

Predictions

A cyclic cubic number field has $\mathrm{sgnrk}(\mathbb{Z}_F^\times) = 1, 3$. How frequently do each of these possibilities occur?

Conjecture (B-Varma-Voight)

As F varies over cyclic cubic number fields, the probability that $\mathrm{sgnrk}(\mathbb{Z}_F^\times) = 1$ *is approximately* 3%.

Unit signature ranks

Predictions

A cyclic cubic number field has $\mathrm{sgnrk}(\mathbb{Z}_F^\times) = 1, 3$. How frequently do each of these possibilities occur?

Conjecture (B-Varma-Voight)

As F varies over cyclic cubic number fields, the probability that $\mathrm{sgnrk}(\mathbb{Z}_F^\times) = 1$ is approximately 3%.

Theorem (B-Elkies-Varma-Voight)

There are infinitely many cyclic cubic number fields which have $\mathrm{sgnrk}(\mathbb{Z}_F^\times) = 1$.

Computational support

We tested our conjecture by sampled cyclic cubic number fields with large conductor. Let $\mathcal{N}_3(X)$ denote a sample of 10,000 cyclic cubic fields with conductor less than X.

Table: Data for signature ranks of (sampled) cyclic cubic fields.

Family	Property	Proportion of Family satisfying Property			Prediction
		$X = 10^5$	$X = 10^6$	$X = 10^7$	
$\mathcal{N}_3(X)$	$\text{sgnrk}(\mathbb{Z}_F^\times) = 1$	0.023	0.024	0.026	~ 0.0301
$1/\sqrt{N} = .01$	$\text{sgnrk}(\mathbb{Z}_F^\times) = 3$	0.977	0.976	0.974	~ 0.9709

Thanks

Thanks!

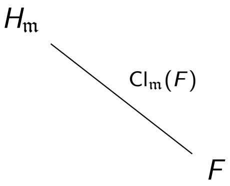
Model

Selmer groups of number fields

Class fields

Class fields

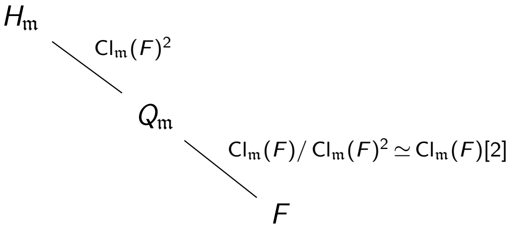
Let $H_{\mathfrak{m}} \mid F$ be the ray class field of conductor $\mathfrak{m}$, i.e, an abelian extension of F with $\mathrm{Gal}(H_{\mathfrak{m}} \mid F) \simeq \mathrm{Cl}_{\mathfrak{m}}(F)$.



Class fields

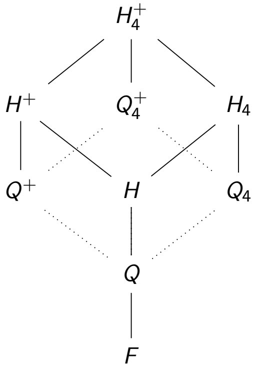
Class fields and 2-torsion

Let $Q_{\mathfrak{m}} \subseteq H_{\mathfrak{m}}$ be the maximal subfield of exponent dividing 2 (the compositum of all quadratic extensions of F inside $H_{\mathfrak{m}}$).



Class fields

Let $H_4^+ \mid F$ be the narrow ray class field of modulus 4 — the relationship between 2 and ∞ is captured in the subfield Q_4^+.



Legend

$H_4^+ \leftrightarrow \mathrm{Cl}_4^+(F)$

$H^+ \leftrightarrow \mathrm{Cl}^+(F)$

$H_4 \leftrightarrow \mathrm{Cl}_4(F)$

$H \leftrightarrow \mathrm{Cl}(F)$

Selmer group (of a number field)

The **2-Selmer group of a number field** is

$$\mathrm{Sel}_2(F) := \{z \in F^\times \,:\, (z) = \mathfrak{a}^2 \text{ for a fractional ideal } \mathfrak{a}\}/F^{\times 2}.$$

Explicitly, this is the subgroup of $F^\times/F^{\times 2}$ corresponding to $Q_4^+ \mid F$.

Selmer group (of a number field)

The **2-Selmer group of a number field** is

$$\mathrm{Sel}_2(F) := \{z \in F^\times : (z) = \mathfrak{a}^2 \text{ for a fractional ideal } \mathfrak{a}\}/F^{\times 2}.$$

Explicitly, this is the subgroup of $F^\times/F^{\times 2}$ corresponding to $Q_4^+ \mid F$.

Conclusion

The 2-Selmer group of a number field neatly packages the relationship between 2 and ∞ into a single mathematical object. My research focus on modeling the local image of $\mathrm{Sel}_2(F)$

Ramification in quadratic extensions

Class field theory tells us that the 2-Selmer group is the subset of $F^\times/F^{\times 2}$ corresponding to all quadratic extensions of F that are unramified away from 2 and ∞.

Ramification in quadratic extensions

Class field theory tells us that the 2-Selmer group is the subset of $F^\times/F^{\times 2}$ corresponding to all quadratic extensions of F that are unramified away from 2 and ∞.

Main Idea: Let F_v denote the completion of F with respect to a place v. For any quadratic extension of F, the ramification above the place v can be determined locally from the map

$$F^\times/(F^\times)^2 \to F_v^\times/(F_v^\times)^2.$$