On Gerth's conjectures

Peter Koymans
Universiteit Leiden

DIAMANT symposium

Veldhoven, Nederland, April 2019

Introduction

Class groups were first studied by Gauss in the language of binary quadratic forms.

Introduction

Class groups were first studied by Gauss in the language of binary quadratic forms.

Recently, class groups have gotten a great deal of attention from the standpoint of arithmetic statistics, where one strives to prove results on the "average" behavior of arithmetic objects.

Introduction

Class groups were first studied by Gauss in the language of binary quadratic forms.

Recently, class groups have gotten a great deal of attention from the standpoint of arithmetic statistics, where one strives to prove results on the "average" behavior of arithmetic objects.

One of the leading problems in this area are the conjectures of Cohen and Lenstra on the "average" behavior of class groups in the family of imaginary (or real) quadratic number fields ordered by discriminant.

Class groups

Let K be a number field. Every non-zero fractional ideal I of K can uniquely be factored as

$$I = \prod_{\mathfrak{p} \text{ prime of } \mathcal{O}_K} \mathfrak{p}^{e_p}$$

for some integer exponents e_p of which only finitely many are non-zero.

Class groups

Let K be a number field. Every non-zero fractional ideal I of K can uniquely be factored as

$$I = \prod_{\mathfrak{p} \text{ prime of } \mathcal{O}_K} \mathfrak{p}^{e_p}$$

for some integer exponents e_p of which only finitely many are non-zero.

The non-zero fractional ideals I of K form a group under ideal multiplication, called I_K.

Class groups

Let K be a number field. Every non-zero fractional ideal I of K can uniquely be factored as

$$I = \prod_{\mathfrak{p} \text{ prime of } \mathcal{O}_K} \mathfrak{p}^{e_p}$$

for some integer exponents e_p of which only finitely many are non-zero.

The non-zero fractional ideals I of K form a group under ideal multiplication, called I_K.

An ideal I is called principal if there exists $\alpha \in K$ such that $I = (\alpha)$. This gives a subgroup P_K of I_K given by the principal ideals. Then we define the class group of K as

$$\mathrm{Cl}(K) := I_K / P_K,$$

which is a finite abelian group.

The Cohen-Lenstra heuristics

Let p be an odd prime. When K varies among imaginary quadratic fields ordered by their discriminant D_K, the group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

The Cohen-Lenstra heuristics

Let p be an odd prime. When K varies among imaginary quadratic fields ordered by their discriminant D_K, the group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

More formally, Cohen and Lenstra conjectured that

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian p-group A.

The Cohen-Lenstra heuristics

Let p be an odd prime. When K varies among imaginary quadratic fields ordered by their discriminant D_K, the group $\mathrm{Cl}(K)[p^\infty]$ is believed to behave as a random finite, abelian p-group.

More formally, Cohen and Lenstra conjectured that

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{p^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian p-group A.

They also made a similar conjecture for real quadratic fields

$$\lim_{X\to\infty} \frac{|\{K \text{ re. quadr.} : |D_K| < X \text{ and } \mathrm{Cl}(K)[p^\infty] \cong A\}|}{|\{K \text{ re. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=2}^{\infty}\left(1-\frac{1}{p^i}\right)}{|A||\mathrm{Aut}(A)|},$$

where one should now think of $\mathrm{Cl}(K)[p^\infty]$ as the quotient of a random abelian group.

Genus theory

Note that $p = 2$ is excluded from the Cohen and Lenstra conjectures. The reason for this is that the group $\mathrm{Cl}(K)[2]$ has a very predictable behavior unlike $\mathrm{Cl}(K)[p]$ for p odd.

Genus theory

Note that $p = 2$ is excluded from the Cohen and Lenstra conjectures. The reason for this is that the group $\mathrm{Cl}(K)[2]$ has a very predictable behavior unlike $\mathrm{Cl}(K)[p]$ for p odd.

The description of $\mathrm{Cl}(K)[2]$ is due to Gauss and is known as genus theory. We have that

$$|\mathrm{Cl}(K)[2]| = 2^{\omega(D_K)-1}$$

and $\mathrm{Cl}(K)[2]$ is generated by the ramified prime ideals of $\mathcal{O}_K$.

Gerth's modification

Since the group $\mathrm{Cl}(K)[2]$ is no longer random, Gerth proposed the following modification of the Cohen-Lenstra conjectures. Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $(2\mathrm{Cl}(K))[2^\infty]$ that behaves randomly.

Gerth's modification

Since the group $\mathrm{Cl}(K)[2]$ is no longer random, Gerth proposed the following modification of the Cohen-Lenstra conjectures. Instead of $\mathrm{Cl}(K)[2^\infty]$, it is the group $(2\mathrm{Cl}(K))[2^\infty]$ that behaves randomly.

To be precise, Gerth conjectured the following

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X, (2\mathrm{Cl}(K))[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{2^i}\right)}{|\mathrm{Aut}(A)|}$$

for every finite, abelian 2-group A, and similarly for real quadratics.

Governing fields

For a finite abelian group A, we define $\mathrm{rk}_{2^k}(A) := \dim_{\mathbb{F}_2} 2^{k-1}A/2^kA$.
Example

$$A = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Then we have $\mathrm{rk}_2(A) = 3$, $\mathrm{rk}_4(A) = \mathrm{rk}_8(A) = 1$ and $\mathrm{rk}_{2^k}(A) = 0$ for every integer $k \geq 4$.

Governing fields

For a finite abelian group A, we define $\mathrm{rk}_{2^k}(A) := \dim_{\mathbb{F}_2} 2^{k-1}A/2^kA$.
Example

$$A = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}.$$

Then we have $\mathrm{rk}_2(A) = 3$, $\mathrm{rk}_4(A) = \mathrm{rk}_8(A) = 1$ and $\mathrm{rk}_{2^k}(A) = 0$ for every integer $k \geq 4$.

Cohn and Lagarias conjectured that for each integer $k \geq 1$ and each integer $d \not\equiv 2 \bmod 4$, there exists a normal field extension $M_{d,k}$ over $\mathbb{Q}$ and a class function $\phi_{d,k} : \mathrm{Gal}(M_{d,k}/\mathbb{Q}) \to \mathbb{Z}_{\geq 0}$ such that

$$\phi_{d,k}(\mathrm{Frob}_{M_{d,k}/\mathbb{Q}}(p)) = \mathrm{rk}_{2^k}\mathrm{Cl}(\mathbb{Q}(\sqrt{dp}))$$

for all primes p coprime with $2d$.

The Cohn and Lagarias conjecture

Theorem 1 (Stevenhagen, 1989)

The Cohn and Lagarias conjecture is true for all values of d and all values of $1 \leq k \leq 3$.

The Cohn and Lagarias conjecture

Theorem 1 (Stevenhagen, 1989)

The Cohn and Lagarias conjecture is true for all values of d and all values of $1 \leq k \leq 3$.

No progress since then! It is still an open problem if $M_{d,k}$ exists for any value of k with $k > 3$. However, we have the following.

The Cohn and Lagarias conjecture

Theorem 1 (Stevenhagen, 1989)

The Cohn and Lagarias conjecture is true for all values of d and all values of $1 \leq k \leq 3$.

No progress since then! It is still an open problem if $M_{d,k}$ exists for any value of k with $k > 3$. However, we have the following.

Theorem 2 (K.-Milovic, 2018)

Assume a short character sum conjecture. Then $M_{-4,4}$ does not exist.

The breakthrough of Smith

Smith realized that it is no longer possible to govern a single 2^k-rank by a Chebotarev symbol, but instead that one can still *compare* class groups.

The breakthrough of Smith

Smith realized that it is no longer possible to govern a single 2^k-rank by a Chebotarev symbol, but instead that one can still *compare* class groups.

From this he was able to prove Gerth's conjecture.

Theorem 3 (Smith, 2017)

We have for every finite, abelian 2-group A

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X, (2\mathrm{Cl}(K))[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{2^i}\right)}{|\mathrm{Aut}(A)|}.$$

The breakthrough of Smith

Smith realized that it is no longer possible to govern a single 2^k-rank by a Chebotarev symbol, but instead that one can still *compare* class groups.

From this he was able to prove Gerth's conjecture.

Theorem 3 (Smith, 2017)

We have for every finite, abelian 2-group A

$$\lim_{X\to\infty} \frac{|\{K \text{ im. quadr.} : |D_K| < X, (2\mathrm{Cl}(K))[2^\infty] \cong A\}|}{|\{K \text{ im. quadr.} : |D_K| < X\}|} = \frac{\prod_{i=1}^{\infty}\left(1-\frac{1}{2^i}\right)}{|\mathrm{Aut}(A)|}.$$

Using the same techniques, Smith solved the congruent number problem.

A reflection principle

So how does one compare class groups? Use “reflection principles”.

A reflection principle

So how does one compare class groups? Use "reflection principles".

The following theorem due to Stevenhagen is a typical example of a reflection principle, and is a special case of Smith's reflection principle.

A reflection principle

So how does one compare class groups? Use "reflection principles".

The following theorem due to Stevenhagen is a typical example of a reflection principle, and is a special case of Smith's reflection principle.

Theorem 4 (Stevenhagen, 1993)

Let p be a prime that splits completely in $K := \mathbb{Q}(\zeta_{16}, \sqrt[4]{2})$. This is equivalent to $8 \mid h_{-4p}$, $8 \mid h_{-8p}$ and $8 \mid h_{8p}^{+}$. If p splits completely in $K(\sqrt{1+\zeta_8})$, we have

$$16 \mid h_{8p}^{+} \Leftrightarrow 16 \mid h_{-8p} \text{ and } 16 \mid h_{-4p},$$

while if p does not split completely in $K(\sqrt{1+\zeta_8})$

$$16 \mid h_{8p}^{+} \Leftrightarrow 16 \mid h_{-8p} \text{ and } 8 \parallel h_{-4p}.$$

Cyclic extensions

Let l be an odd prime. There is a natural analogue for degree l cyclic extensions K of $\mathbb{Q}$. Then $\mathrm{Cl}(K)$ is a $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-module.

Cyclic extensions

Let l be an odd prime. There is a natural analogue for degree l cyclic extensions K of $\mathbb{Q}$. Then $\mathrm{Cl}(K)$ is a $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-module.

Picking an identification of $\mathrm{Gal}(K/\mathbb{Q})$ with $\langle \zeta_l \rangle$, we get a $\mathbb{Z}[\zeta_l]$-module, since the norm element in $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ acts as zero on $\mathrm{Cl}(K)$.

Cyclic extensions

Let l be an odd prime. There is a natural analogue for degree l cyclic extensions K of $\mathbb{Q}$. Then $\mathrm{Cl}(K)$ is a $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-module.

Picking an identification of $\mathrm{Gal}(K/\mathbb{Q})$ with $\langle \zeta_l \rangle$, we get a $\mathbb{Z}[\zeta_l]$-module, since the norm element in $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ acts as zero on $\mathrm{Cl}(K)$.

The isomorphism type of the resulting $\mathbb{Z}[\zeta_l]$-module does not depend on the chosen identification.

Cyclic extensions

Let l be an odd prime. There is a natural analogue for degree l cyclic extensions K of $\mathbb{Q}$. Then $\mathrm{Cl}(K)$ is a $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$-module.

Picking an identification of $\mathrm{Gal}(K/\mathbb{Q})$ with $\langle \zeta_l \rangle$, we get a $\mathbb{Z}[\zeta_l]$-module, since the norm element in $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$ acts as zero on $\mathrm{Cl}(K)$.

The isomorphism type of the resulting $\mathbb{Z}[\zeta_l]$-module does not depend on the chosen identification.

Hence we may view $\mathrm{Cl}(K)[l^\infty]$ as a $\mathbb{Z}_l[\zeta_l]$-module, and one may think of it as a random module in the appropriate sense.

Another conjecture of Gerth

Gerth conjectured that $((1-\zeta_l)\mathrm{Cl}(K))[l^\infty]$ is a random $\mathbb{Z}_l[\zeta_l]$-module.

Another conjecture of Gerth

Gerth conjectured that $((1-\zeta_l)\mathrm{Cl}(K))[l^\infty]$ is a random $\mathbb{Z}_l[\zeta_l]$-module.

Using the breakthrough of Smith, we proved this conjecture.

Theorem 5 (K.-Pagano, 2018)

Assume GRH and let l be an odd prime. Then for all finitely generated, torsion $\mathbb{Z}_l[\zeta_l]$-modules A the limit

$$\lim_{X\to\infty} \frac{|\{K \text{ cyc. deg. } l : |D_K| < X, ((1-\zeta_l)\mathrm{Cl}(K))[l^\infty] \cong A\}|}{|\{K \text{ cyc. deg. } l : |D_K| < X\}|}$$

exists, and is equal to

$$\frac{\prod_{i=2}^{\infty}\left(1-\frac{1}{l^i}\right)}{|A||\mathrm{Aut}_{\mathbb{Z}_l[\zeta_l]}(A)|}.$$

Questions

Questions?