Malle's conjecture for nonic Heisenberg extensions

Peter Koymans
Max Planck Institute for Mathematics

San Diego Number Theory Seminar

1 April 2021

History

A famous theorem due to Hermite states that there are only finitely many number fields with bounded discriminant.

History

A famous theorem due to Hermite states that there are only finitely many number fields with bounded discriminant.

But how many number fields are there with discriminant bounded by X? What if we also specify the Galois group?

History

A famous theorem due to Hermite states that there are only finitely many number fields with bounded discriminant.

But how many number fields are there with discriminant bounded by X? What if we also specify the Galois group?

Conjecture 1 (Inverse Galois problem)

Does every finite group G occur as the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of a finite, normal extension $K/\mathbb{Q}$?

History

A famous theorem due to Hermite states that there are only finitely many number fields with bounded discriminant.

But how many number fields are there with discriminant bounded by X? What if we also specify the Galois group?

Conjecture 1 (Inverse Galois problem)

Does every finite group G occur as the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ of a finite, normal extension $K/\mathbb{Q}$?

A famous theorem due to Shafarevich (1954) shows that the answer is yes for G solvable.

Malle's conjecture

In 2002-2004 Malle conjectured a precise asymptotic for the number of extensions with given Galois group G and discriminant bounded by X.

Malle's conjecture

In 2002-2004 Malle conjectured a precise asymptotic for the number of extensions with given Galois group G and discriminant bounded by X.

For $G \subseteq S_n$ transitive, define

$$N(G, X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, \mathrm{Gal}(K/\mathbb{Q}) \cong_{\text{perm. gr.}} G, \Delta_{K/\mathbb{Q}} \leq X\}.$$

Malle's conjecture

In 2002-2004 Malle conjectured a precise asymptotic for the number of extensions with given Galois group G and discriminant bounded by X.

For $G \subseteq S_n$ transitive, define

$$N(G, X) := \#\{K/\mathbb{Q} : [K : \mathbb{Q}] = n, \mathrm{Gal}(K/\mathbb{Q}) \cong_{\text{perm. gr.}} G, \Delta_{K/\mathbb{Q}} \leq X\}.$$

Here $\mathrm{Gal}(K/\mathbb{Q})$ is defined as follows: if L is the normal closure of K, then $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the n embeddings $K \to \overline{\mathbb{Q}}$.

Malle's conjecture

In 2002-2004 Malle conjectured a precise asymptotic for the number of extensions with given Galois group G and discriminant bounded by X.

For $G \subseteq S_n$ transitive, define

$$N(G,X) := \#\{K/\mathbb{Q} : [K:\mathbb{Q}] = n, \mathrm{Gal}(K/\mathbb{Q}) \cong_{\text{perm. gr.}} G, \Delta_{K/\mathbb{Q}} \leq X\}.$$

Here $\mathrm{Gal}(K/\mathbb{Q})$ is defined as follows: if L is the normal closure of K, then $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the n embeddings $K \to \overline{\mathbb{Q}}$.

This induces a homomorphism $\mathrm{Gal}(L/\mathbb{Q}) \to S_n$, and we define, by abuse of notation, $\mathrm{Gal}(K/\mathbb{Q})$ to be the image of this homomorphism.

Malle's conjecture

In 2002-2004 Malle conjectured a precise asymptotic for the number of extensions with given Galois group G and discriminant bounded by X.

For $G \subseteq S_n$ transitive, define

$$N(G,X) := \#\{K/\mathbb{Q} : [K:\mathbb{Q}] = n, \mathrm{Gal}(K/\mathbb{Q}) \cong_{\text{perm. gr.}} G, \Delta_{K/\mathbb{Q}} \leq X\}.$$

Here $\mathrm{Gal}(K/\mathbb{Q})$ is defined as follows: if L is the normal closure of K, then $\mathrm{Gal}(L/\mathbb{Q})$ acts transitively on the n embeddings $K \to \overline{\mathbb{Q}}$.

This induces a homomorphism $\mathrm{Gal}(L/\mathbb{Q}) \to S_n$, and we define, by abuse of notation, $\mathrm{Gal}(K/\mathbb{Q})$ to be the image of this homomorphism.

Conjecture 2 (Malle's conjecture)

There are $a(G), c(G) > 0$ and $b(G) \in \mathbb{Z}_{>0}$ such that

$$N(G,X) \sim c(G) X^{a(G)} (\log X)^{b(G)-1}.$$

Malle gave explicit values for $a(G)$ and $b(G)$ but NOT for $c(G)$.

The Malle constants

The constant $a(G)$ can be computed as follows. Define for $\sigma \in G \subseteq S_n$

$$\mathrm{ind}(\sigma) := n - |\{\text{orbits of } \sigma\}|.$$

The Malle constants

The constant $a(G)$ can be computed as follows. Define for $\sigma \in G \subseteq S_n$

$$\mathrm{ind}(\sigma) := n - |\{\text{orbits of } \sigma\}|.$$

Then

$$a(G)^{-1} := \min_{\sigma \in G \setminus \{\mathrm{id}\}} \mathrm{ind}(\sigma).$$

Any prime dividing the discriminant of a G-extension has exponent at least $a(G)^{-1}$.

The Malle constants

The constant $a(G)$ can be computed as follows. Define for $\sigma \in G \subseteq S_n$

$$\mathrm{ind}(\sigma) := n - |\{\text{orbits of } \sigma\}|.$$

Then

$$a(G)^{-1} := \min_{\sigma \in G \setminus \{\mathrm{id}\}} \mathrm{ind}(\sigma).$$

Any prime dividing the discriminant of a G-extension has exponent at least $a(G)^{-1}$.

Klüners showed that the proposed $b(G)$ by Malle is not correct.

The Malle constants

The constant $a(G)$ can be computed as follows. Define for $\sigma \in G \subseteq S_n$

$$\mathrm{ind}(\sigma) := n - |\{\text{orbits of } \sigma\}|.$$

Then

$$a(G)^{-1} := \min_{\sigma \in G \setminus \{\mathrm{id}\}} \mathrm{ind}(\sigma).$$

Any prime dividing the discriminant of a G-extension has exponent at least $a(G)^{-1}$.

Klüners showed that the proposed $b(G)$ by Malle is not correct.

Türkelli proposed a new value for $b(G)$.

The Malle constants

The constant $a(G)$ can be computed as follows. Define for $\sigma \in G \subseteq S_n$

$$\mathrm{ind}(\sigma) := n - |\{\text{orbits of } \sigma\}|.$$

Then

$$a(G)^{-1} := \min_{\sigma \in G \setminus \{\mathrm{id}\}} \mathrm{ind}(\sigma).$$

Any prime dividing the discriminant of a G-extension has exponent at least $a(G)^{-1}$.

Klüners showed that the proposed $b(G)$ by Malle is not correct.

Türkelli proposed a new value for $b(G)$.

The value of $a(G)$ is generally believed to be correct. The value of $c(G)$ is sometimes given by an infinite product over primes p, where the factors are certain local densities (Malle–Bhargava principle).

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

- abelian G by Wright;

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- $S_3 \subseteq S_6$ by Bhargava–Wood;

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- $S_3 \subseteq S_6$ by Bhargava–Wood;
- $D_4 \subseteq S_4$ by Cohen–Diaz y Diaz–Olivier;

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- $S_3 \subseteq S_6$ by Bhargava–Wood;
- $D_4 \subseteq S_4$ by Cohen–Diaz y Diaz–Olivier;
- generalized quaternion groups by Klüners;

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- $S_3 \subseteq S_6$ by Bhargava–Wood;
- $D_4 \subseteq S_4$ by Cohen–Diaz y Diaz–Olivier;
- generalized quaternion groups by Klüners;
- any nilpotent group G, in the regular representation, such that all elements of order p are central, where p is the smallest prime dividing $\#G$ by K.–Pagano;

Known cases of Malle's conjecture

Malle's conjecture is known in the following cases:

- abelian G by Wright;
- S_3 by Davenport–Heilbronn;
- S_4, S_5 by Bhargava;
- $S_3 \subseteq S_6$ by Bhargava–Wood;
- $D_4 \subseteq S_4$ by Cohen–Diaz y Diaz–Olivier;
- generalized quaternion groups by Klüners;
- any nilpotent group G, in the regular representation, such that all elements of order p are central, where p is the smallest prime dividing $\#G$ by K.–Pagano;
- direct products $S_n \times A$ for $n \in \{3, 4, 5\}$ and A abelian by Wang (with $\#A$ coprime to some values) and later by Masri–Thorne–Tsai–Wang.

The weak form of Malle's conjecture

The weak form of Malle's conjecture asserts that

$$X^{a(G)} \ll N(G, X) \ll_\epsilon X^{a(G)+\epsilon}.$$

The weak form of Malle's conjecture

The weak form of Malle's conjecture asserts that

$$X^{a(G)} \ll N(G, X) \ll_\epsilon X^{a(G)+\epsilon}.$$

There are no known counterexamples to the weak form.

The weak form of Malle's conjecture

The weak form of Malle's conjecture asserts that

$$X^{a(G)} \ll N(G,X) \ll_\epsilon X^{a(G)+\epsilon}.$$

There are no known counterexamples to the weak form.

The weak form is known for nilpotent G by Klüners–Malle with further progress in the solvable case by Alberts and Alberts–O'Dorney.

The Heisenberg group

Let ℓ be a prime number and let Heis_ℓ be the multiplicative group

$$\begin{pmatrix} 1 & \mathbb{F}_\ell & \mathbb{F}_\ell \\ 0 & 1 & \mathbb{F}_\ell \\ 0 & 0 & 1 \end{pmatrix}.$$

For $\ell = 2$ we get $\mathrm{Heis}_2 \cong D_4$.

The Heisenberg group

Let ℓ be a prime number and let Heis_ℓ be the multiplicative group

$$\begin{pmatrix} 1 & \mathbb{F}_\ell & \mathbb{F}_\ell \\ 0 & 1 & \mathbb{F}_\ell \\ 0 & 0 & 1 \end{pmatrix}.$$

For $\ell = 2$ we get $\mathrm{Heis}_2 \cong D_4$.

Our main theorem counts (non-normal) degree 9 extensions of $\mathbb{Q}$ (up to isomorphism) with Galois closure isomorphic to Heis_3. This amounts to viewing Heis_3 as a transitive subgroup of S_9.

The Heisenberg group

Let ℓ be a prime number and let Heis_ℓ be the multiplicative group

$$\begin{pmatrix} 1 & \mathbb{F}_\ell & \mathbb{F}_\ell \\ 0 & 1 & \mathbb{F}_\ell \\ 0 & 0 & 1 \end{pmatrix}.$$

For $\ell = 2$ we get $\text{Heis}_2 \cong D_4$.

Our main theorem counts (non-normal) degree 9 extensions of $\mathbb{Q}$ (up to isomorphism) with Galois closure isomorphic to Heis_3. This amounts to viewing Heis_3 as a transitive subgroup of S_9.

Theorem 1 (Fouvry–K.)

There is a constant $c > 0$ such that

$$N(\text{Heis}_3, X) \sim cX^{1/4}.$$

The Heisenberg group

Let ℓ be a prime number and let Heis_ℓ be the multiplicative group

$$\begin{pmatrix} 1 & \mathbb{F}_\ell & \mathbb{F}_\ell \\ 0 & 1 & \mathbb{F}_\ell \\ 0 & 0 & 1 \end{pmatrix}.$$

For $\ell = 2$ we get $\text{Heis}_2 \cong D_4$.

Our main theorem counts (non-normal) degree 9 extensions of $\mathbb{Q}$ (up to isomorphism) with Galois closure isomorphic to Heis_3. This amounts to viewing Heis_3 as a transitive subgroup of S_9.

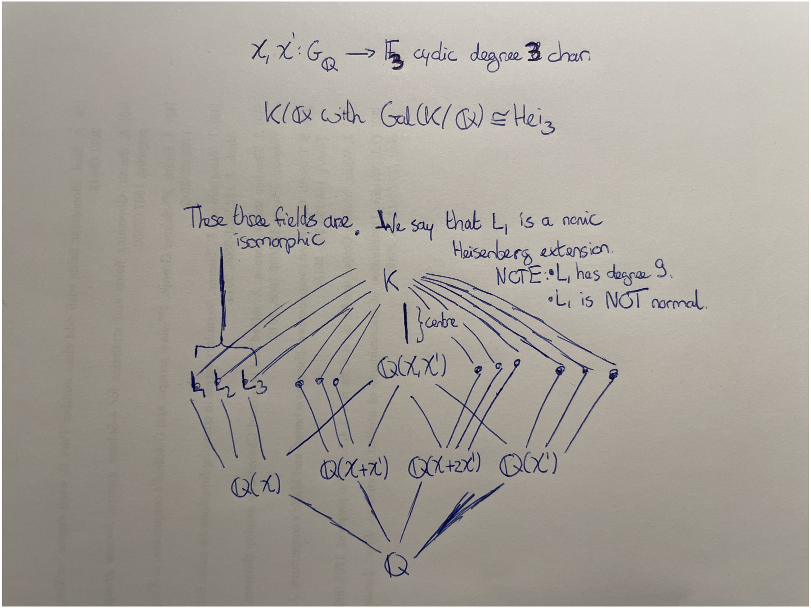
Theorem 1 (Fouvry–K.)

There is a constant $c > 0$ such that

$$N(\text{Heis}_3, X) \sim cX^{1/4}.$$

We give an explicit value for the constant c.

Subfield diagram of Heis$_3$



Comparison with quartic D_4 extensions

Cohen–Diaz y Diaz–Olivier proved that

$$N(\mathrm{Heis}_2, X) \sim \frac{6X}{\pi^2} \sum_{D} \frac{2^{-i(D)}}{D^2} \frac{L(1, D)}{L(2, D)},$$

where the sum is over fundamental quadratic discriminants and $i(D) = 0$ if $D > 0$ and $i(D) = 1$ if $D < 0$.

Comparison with quartic D_4 extensions

Cohen–Diaz y Diaz–Olivier proved that

$$N(\mathrm{Heis}_2, X) \sim \frac{6X}{\pi^2} \sum_D \frac{2^{-i(D)}}{D^2} \frac{L(1,D)}{L(2,D)},$$

where the sum is over fundamental quadratic discriminants and $i(D) = 0$ if $D > 0$ and $i(D) = 1$ if $D < 0$.

Their proof proceeds in two steps:

- count, uniformly in the number field K, the number of quadratic extensions of K with relative discriminant bounded by X;
- sum this function over all quadratic number fields K.

Comparison with quartic D_4 extensions

Cohen–Diaz y Diaz–Olivier proved that

$$N(\mathrm{Heis}_2, X) \sim \frac{6X}{\pi^2} \sum_D \frac{2^{-i(D)}}{D^2} \frac{L(1,D)}{L(2,D)},$$

where the sum is over fundamental quadratic discriminants and $i(D) = 0$ if $D > 0$ and $i(D) = 1$ if $D < 0$.

Their proof proceeds in two steps:

- count, uniformly in the number field K, the number of quadratic extensions of K with relative discriminant bounded by X;
- sum this function over all quadratic number fields K.

Key point: a typical quadratic extension of a quadratic extension of $\mathbb{Q}$ has Galois closure D_4.

Comparison with quartic D_4 extensions

Cohen–Diaz y Diaz–Olivier proved that

$$N(\mathrm{Heis}_2, X) \sim \frac{6X}{\pi^2} \sum_D \frac{2^{-i(D)}}{D^2} \frac{L(1,D)}{L(2,D)},$$

where the sum is over fundamental quadratic discriminants and $i(D) = 0$ if $D > 0$ and $i(D) = 1$ if $D < 0$.

Their proof proceeds in two steps:

- count, uniformly in the number field K, the number of quadratic extensions of K with relative discriminant bounded by X;
- sum this function over all quadratic number fields K.

Key point: a typical quadratic extension of a quadratic extension of $\mathbb{Q}$ has Galois closure D_4.

This fails for cyclic degree 3 extensions. Need a new strategy!

The strategy

Step 1: given two linearly independent characters $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_3$, there exists an Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$ if and only if all ramified primes (not equal to 3) have residue field degree 1 in $\mathbb{Q}(\chi, \chi')$.

The strategy

Step 1: given two linearly independent characters $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_3$, there exists an Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$ if and only if all ramified primes (not equal to 3) have residue field degree 1 in $\mathbb{Q}(\chi, \chi')$.

Step 2: write $N(\mathrm{Heis}_3, X)$ as a certain sum involving cyclic degree 3 characters, that is cubic Dirichlet characters.

The strategy

Step 1: given two linearly independent characters $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_3$, there exists an Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$ if and only if all ramified primes (not equal to 3) have residue field degree 1 in $\mathbb{Q}(\chi, \chi')$.

Step 2: write $N(\mathrm{Heis}_3, X)$ as a certain sum involving cyclic degree 3 characters, that is cubic Dirichlet characters.

Step 3: extract the main term from this character sum using oscillation of characters (Siegel–Walfisz type theorem).

The strategy

Step 1: given two linearly independent characters $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_3$, there exists an Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$ if and only if all ramified primes (not equal to 3) have residue field degree 1 in $\mathbb{Q}(\chi, \chi')$.

Step 2: write $N(\mathrm{Heis}_3, X)$ as a certain sum involving cyclic degree 3 characters, that is cubic Dirichlet characters.

Step 3: extract the main term from this character sum using oscillation of characters (Siegel–Walfisz type theorem).

A similar strategy was used by Heath-Brown to find the distribution of the 2-Selmer groups $\mathrm{Sel}^2(E^d)$ of quadratic twists d of an elliptic curve E, and by Fouvry–Klüners to find the distribution of $2\mathrm{Cl}(K)[4]$.

Lifting bicyclic extensions, I

Let $\rho : G_{\mathbb{Q}} \to \mathbb{F}_\ell^2$ be a surjective homomorphism. When does ρ lift to a surjective homomorphism $\psi : G_{\mathbb{Q}} \to \mathrm{Heis}_\ell$?

Lifting bicyclic extensions, I

Let $\rho : G_{\mathbb{Q}} \to \mathbb{F}_\ell^2$ be a surjective homomorphism. When does ρ lift to a surjective homomorphism $\psi : G_{\mathbb{Q}} \to \mathrm{Heis}_\ell$?

The Heisenberg group is set-theoretically given as $\mathbb{F}_\ell \times \mathbb{F}_\ell^2$ with multiplication given by

$$(a_1, g_1) * (a_2, g_2) = (a_1 + a_2 + \theta(g_1, g_2), g_1 + g_2),$$

Lifting bicyclic extensions, I

Let $\rho : G_{\mathbb{Q}} \to \mathbb{F}_\ell^2$ be a surjective homomorphism. When does ρ lift to a surjective homomorphism $\psi : G_{\mathbb{Q}} \to \mathrm{Heis}_\ell$?

The Heisenberg group is set-theoretically given as $\mathbb{F}_\ell \times \mathbb{F}_\ell^2$ with multiplication given by

$$(a_1, g_1) * (a_2, g_2) = (a_1 + a_2 + \theta(g_1, g_2), g_1 + g_2),$$

where $\theta(g_1, g_2)$ is the 2-cocycle in $H^2(\mathbb{F}_\ell^2, \mathbb{F}_\ell)$ given by

$$(g_1, g_2) \mapsto \pi_1(g_1) \cdot \pi_2(g_2), \quad \pi_1, \pi_2 : \mathbb{F}_\ell^2 \to \mathbb{F}_\ell \text{ projection maps.}$$

Lifting bicyclic extensions, I

Let $\rho : G_{\mathbb{Q}} \to \mathbb{F}_\ell^2$ be a surjective homomorphism. When does ρ lift to a surjective homomorphism $\psi : G_{\mathbb{Q}} \to \mathrm{Heis}_\ell$?

The Heisenberg group is set-theoretically given as $\mathbb{F}_\ell \times \mathbb{F}_\ell^2$ with multiplication given by

$$(a_1, g_1) * (a_2, g_2) = (a_1 + a_2 + \theta(g_1, g_2), g_1 + g_2),$$

where $\theta(g_1, g_2)$ is the 2-cocycle in $H^2(\mathbb{F}_\ell^2, \mathbb{F}_\ell)$ given by

$$(g_1, g_2) \mapsto \pi_1(g_1) \cdot \pi_2(g_2), \quad \pi_1, \pi_2 : \mathbb{F}_\ell^2 \to \mathbb{F}_\ell \text{ projection maps.}$$

Writing $\psi = (\phi, \rho)$ with $\phi : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ any continuous map, we see that ψ is a homomorphism if and only if

$$(\phi(\sigma) + \phi(\tau) + \theta(\rho(\sigma), \rho(\tau)), \rho(\sigma) + \rho(\tau)) = (\phi(\sigma\tau), \rho(\sigma\tau)).$$

Lifting bicyclic extensions, I

Let $\rho : G_{\mathbb{Q}} \to \mathbb{F}_\ell^2$ be a surjective homomorphism. When does ρ lift to a surjective homomorphism $\psi : G_{\mathbb{Q}} \to \mathrm{Heis}_\ell$?

The Heisenberg group is set-theoretically given as $\mathbb{F}_\ell \times \mathbb{F}_\ell^2$ with multiplication given by

$$(a_1, g_1) * (a_2, g_2) = (a_1 + a_2 + \theta(g_1, g_2), g_1 + g_2),$$

where $\theta(g_1, g_2)$ is the 2-cocycle in $H^2(\mathbb{F}_\ell^2, \mathbb{F}_\ell)$ given by

$$(g_1, g_2) \mapsto \pi_1(g_1) \cdot \pi_2(g_2), \quad \pi_1, \pi_2 : \mathbb{F}_\ell^2 \to \mathbb{F}_\ell \text{ projection maps.}$$

Writing $\psi = (\phi, \rho)$ with $\phi : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ any continuous map, we see that ψ is a homomorphism if and only if

$$(\phi(\sigma) + \phi(\tau) + \theta(\rho(\sigma), \rho(\tau)), \rho(\sigma) + \rho(\tau)) = (\phi(\sigma\tau), \rho(\sigma\tau)).$$

Hence a homomorphism ψ exists if and only if θ is trivial when inflated to $H^2(G_{\mathbb{Q}}, \mathbb{F}_\ell)$, where we view $\mathbb{F}_\ell$ as a discrete $G_{\mathbb{Q}}$-module with trivial action.

Lifting bicyclic extensions, II

By class field theory we know that θ is trivial in $H^2(G_{\mathbb{Q}}, \mathbb{F}_\ell)$ if and only if it is trivial in $H^2(G_{\mathbb{Q}_v}, \mathbb{F}_\ell)$ for every place v.

Lifting bicyclic extensions, II

By class field theory we know that θ is trivial in $H^2(G_{\mathbb{Q}}, \mathbb{F}_\ell)$ if and only if it is trivial in $H^2(G_{\mathbb{Q}_v}, \mathbb{F}_\ell)$ for every place v.

Theorem 2 (Michailov)

Let ℓ be an odd prime number. Let $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ be two linearly independent characters. Then there exists a Heisenberg extension $M/\mathbb{Q}$ containing $\mathbb{Q}(\chi)$ and $\mathbb{Q}(\chi')$ if and only if every ramified prime (not equal to ℓ) has residue field degree 1 in the bicyclic field $\mathbb{Q}(\chi, \chi')$.

Lifting bicyclic extensions, II

By class field theory we know that θ is trivial in $H^2(G_{\mathbb{Q}}, \mathbb{F}_\ell)$ if and only if it is trivial in $H^2(G_{\mathbb{Q}_v}, \mathbb{F}_\ell)$ for every place v.

Theorem 2 (Michailov)

Let ℓ be an odd prime number. Let $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ be two linearly independent characters. Then there exists a Heisenberg extension $M/\mathbb{Q}$ containing $\mathbb{Q}(\chi)$ and $\mathbb{Q}(\chi')$ if and only if every ramified prime (not equal to ℓ) has residue field degree 1 in the bicyclic field $\mathbb{Q}(\chi, \chi')$.

If such an extension $M/\mathbb{Q}$ exists, there are infinitely many, which can all be obtained by twisting M by a cyclic degree ℓ character of $G_{\mathbb{Q}}$.

Minimal Heisenberg extensions

Definition 1 (Minimal Heisenberg extensions)

Let $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ be two linearly independent characters. Let M be a Heisenberg extension of $\mathbb{Q}$ containing $\mathbb{Q}(\chi, \chi')$. We say that M is minimal if

Minimal Heisenberg extensions

Definition 1 (Minimal Heisenberg extensions)

Let $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ be two linearly independent characters. Let M be a Heisenberg extension of $\mathbb{Q}$ containing $\mathbb{Q}(\chi, \chi')$. We say that M is minimal if

- *M is unramified at every place v that is unramified in $\mathbb{Q}(\chi, \chi')$;*

Minimal Heisenberg extensions

Definition 1 (Minimal Heisenberg extensions)

Let $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ be two linearly independent characters. Let M be a Heisenberg extension of $\mathbb{Q}$ containing $\mathbb{Q}(\chi, \chi')$. We say that M is minimal if

- *M is unramified at every place v that is unramified in $\mathbb{Q}(\chi, \chi')$;*
- *$M/\mathbb{Q}(\chi, \chi')$ is unramified at all primes with residue field degree 1 in $\mathbb{Q}(\chi, \chi')$.*

Minimal Heisenberg extensions

Definition 1 (Minimal Heisenberg extensions)

Let $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ be two linearly independent characters. Let M be a Heisenberg extension of $\mathbb{Q}$ containing $\mathbb{Q}(\chi, \chi')$. We say that M is minimal if

- *M is unramified at every place v that is unramified in $\mathbb{Q}(\chi, \chi')$;*
- *$M/\mathbb{Q}(\chi, \chi')$ is unramified at all primes with residue field degree 1 in $\mathbb{Q}(\chi, \chi')$.*

Theorem 3 (Fouvry–K.)

If there exists a Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$, then there exists a minimal Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$.

Minimal Heisenberg extensions

Definition 1 (Minimal Heisenberg extensions)

Let $\chi, \chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ be two linearly independent characters. Let M be a Heisenberg extension of $\mathbb{Q}$ containing $\mathbb{Q}(\chi, \chi')$. We say that M is minimal if

- *M is unramified at every place v that is unramified in $\mathbb{Q}(\chi, \chi')$;*
- *$M/\mathbb{Q}(\chi, \chi')$ is unramified at all primes with residue field degree 1 in $\mathbb{Q}(\chi, \chi')$.*

Theorem 3 (Fouvry–K.)

If there exists a Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$, then there exists a minimal Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$.

This is great, because the discriminant of a minimal Heisenberg extension is easily computed.

The discriminant of nonic Heisenberg extensions

For $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell$, define $\Delta(\chi)$ to be the product of the ramified primes in $\mathbb{Q}(\chi)$. Define free(d, a) be the largest divisor of d coprime to a.

The discriminant of nonic Heisenberg extensions

For $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell$, define $\Delta(\chi)$ to be the product of the ramified primes in $\mathbb{Q}(\chi)$. Define free(d, a) be the largest divisor of d coprime to a.

Lemma 4 (Fouvry–K.)

Let ℓ be an odd prime. Let M be a minimal Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$ defined by a character ρ. Then up to factors of ℓ

$$\Delta_{M/\mathbb{Q}} = \Delta(\chi)^{\ell^2(\ell-1)} \mathrm{free}(\Delta(\chi'), \Delta(\chi))^{\ell^2(\ell-1)} = \prod_{p \mid \Delta(\chi)\Delta(\chi')} p^{\ell^2(\ell-1)}.$$

The discriminant of nonic Heisenberg extensions

For $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell$, define $\Delta(\chi)$ to be the product of the ramified primes in $\mathbb{Q}(\chi)$. Define free(d, a) be the largest divisor of d coprime to a.

Lemma 4 (Fouvry–K.)

Let ℓ be an odd prime. Let M be a minimal Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$ defined by a character ρ. Then up to factors of ℓ

$$\Delta_{M/\mathbb{Q}} = \Delta(\chi)^{\ell^2(\ell-1)} \mathrm{free}(\Delta(\chi'), \Delta(\chi))^{\ell^2(\ell-1)} = \prod_{p \mid \Delta(\chi)\Delta(\chi')} p^{\ell^2(\ell-1)}.$$

Now twist ρ by a character $\chi'' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ ramified precisely at the primes dividing d, coprime with $\Delta(\chi)\Delta(\chi')$. Then up to factors of ℓ

$$\Delta_{\mathbb{Q}(\chi,\chi')(\rho+\chi'')/\mathbb{Q}} = d^{\ell^2(\ell-1)} \Delta(\chi)^{\ell^2(\ell-1)} \mathrm{free}(\Delta(\chi'), \Delta(\chi))^{\ell^2(\ell-1)}.$$

The discriminant of nonic Heisenberg extensions

For $\chi : G_{\mathbb{Q}} \to \mathbb{F}_\ell$, define $\Delta(\chi)$ to be the product of the ramified primes in $\mathbb{Q}(\chi)$. Define $\mathrm{free}(d, a)$ be the largest divisor of d coprime to a.

Lemma 4 (Fouvry–K.)

Let ℓ be an odd prime. Let M be a minimal Heisenberg extension containing $\mathbb{Q}(\chi, \chi')$ defined by a character ρ. Then up to factors of ℓ

$$\Delta_{M/\mathbb{Q}} = \Delta(\chi)^{\ell^2(\ell-1)} \mathrm{free}(\Delta(\chi'), \Delta(\chi))^{\ell^2(\ell-1)} = \prod_{p \mid \Delta(\chi)\Delta(\chi')} p^{\ell^2(\ell-1)}.$$

Now twist ρ by a character $\chi'' : G_{\mathbb{Q}} \to \mathbb{F}_\ell$ ramified precisely at the primes dividing d, coprime with $\Delta(\chi)\Delta(\chi')$. Then up to factors of ℓ

$$\Delta_{\mathbb{Q}(\chi,\chi')(\rho+\chi'')/\mathbb{Q}} = d^{\ell^2(\ell-1)} \Delta(\chi)^{\ell^2(\ell-1)} \mathrm{free}(\Delta(\chi'), \Delta(\chi))^{\ell^2(\ell-1)}.$$

Let $\mathbb{Q}(\chi) \subsetneq L \subsetneq \mathbb{Q}(\chi, \chi')(\rho + \chi'')$. Then up to factors of ℓ

$$\Delta_{L/\mathbb{Q}} = d^{\ell(\ell-1)} \Delta(\chi)^{\ell(\ell-1)} \mathrm{free}(\Delta(\chi'), \Delta(\chi))^{(\ell-1)^2}.$$

Wild ramification

To find the exponent of ℓ in the discriminant, recall that $\mathbb{Q}_\ell^*/\mathbb{Q}_\ell^{*\ell}$ is of dimension 2.

Wild ramification

To find the exponent of ℓ in the discriminant, recall that $\mathbb{Q}_\ell^*/\mathbb{Q}_\ell^{*\ell}$ is of dimension 2.

Hence there are 2 linearly independent characters $G_{\mathbb{Q}_\ell} \to \mathbb{F}_\ell$ of which the discriminant is easily computed.

Wild ramification

To find the exponent of ℓ in the discriminant, recall that $\mathbb{Q}_\ell^*/\mathbb{Q}_\ell^{*\ell}$ is of dimension 2.

Hence there are 2 linearly independent characters $G_{\mathbb{Q}_\ell} \to \mathbb{F}_\ell$ of which the discriminant is easily computed.

Theorem 5 (Fouvry–K.)

Let ℓ be an odd prime. Then there exists precisely one Heisenberg extension $M/\mathbb{Q}_\ell$. Its discriminant ideal equals

$$(\ell)^{\ell(\ell+1)(2\ell-2)}.$$

The number of nonic Heisenberg extensions

We have now parametrized nonic Heisenberg extensions and we have computed their discriminant.

The number of nonic Heisenberg extensions

We have now parametrized nonic Heisenberg extensions and we have computed their discriminant.

Theorem 6 (Fouvry–K.)

Let ℓ be an odd prime number. Then

$$N(\mathrm{Heis}_\ell, X) = \frac{1}{\ell^3(\ell-1)^2} \sum_{\substack{\chi,\chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell \\ \chi,\chi' \text{ linearly independent}}} \mathbf{1}_{\theta_{\chi,\chi'}(\sigma,\tau) \text{ trivial}} \cdot \ell^{\omega(\Delta(\chi)\Delta(\chi'))} \cdot T(X, \chi, \chi', \ell),$$

The number of nonic Heisenberg extensions

We have now parametrized nonic Heisenberg extensions and we have computed their discriminant.

Theorem 6 (Fouvry–K.)

Let ℓ be an odd prime number. Then

$$N(\mathrm{Heis}_\ell, X) = \frac{1}{\ell^3(\ell-1)^2} \sum_{\substack{\chi,\chi' : G_{\mathbb{Q}} \to \mathbb{F}_\ell \\ \chi,\chi' \text{ linearly independent}}} \mathbf{1}_{\theta_{\chi,\chi'}(\sigma,\tau) \text{ trivial}} \cdot \ell^{\omega(\Delta(\chi)\Delta(\chi'))} \cdot T(X, \chi, \chi', \ell),$$

where

$$T(X, \chi, \chi', \ell) = \sum_{\substack{d \in \mathbb{Z}_{>0} \\ \gcd(d, \Delta(\chi)\Delta(\chi'))=1 \\ p \mid d \Rightarrow p \equiv 0,1 \bmod \ell \\ d^{\ell(\ell-1)} \leq \frac{X}{\Delta(\chi)^{\ell(\ell-1)} \mathrm{free}(\Delta(\chi'),\Delta(\chi))^{(\ell-1)^2} \mu(\chi,\chi',d)}}} \mu^2(d) \cdot (\ell-1)^{\omega(d)}.$$

A character sum

How do we compute the indicator function $\mathbf{1}_{\theta_{\chi,\chi'}(\sigma,\tau)\text{ trivial}}$?

A character sum

How do we compute the indicator function $\mathbf{1}_{\theta_{\chi,\chi'}(\sigma,\tau)\text{ trivial}}$?

Viewing χ_1, χ_2 as Dirichlet characters of order ℓ (so taking values in $\mathbb{C}^*$)

$$\mathbf{1}_{\theta_{\chi_1,\chi_2}(\sigma,\tau)\text{ trivial}} = \prod_{\substack{r \mid \Delta(\chi_1)\Delta(\chi_2) \\ r \neq \ell}} \frac{1}{\ell} \left(\sum_{\substack{(z_1,z_2) \in \mathbb{F}_\ell^2 \\ \chi_1^{z_1}\chi_2^{z_2} \text{ unr. at } r}} (\chi_1^{z_1}\chi_2^{z_2})(r) \right).$$

Evaluating the character sum for $\ell = 3$

We restrict the sum to pairs (χ, χ') with $\Delta(\chi)$ small (i.e. smaller than a power of $\log X$), and with $\Delta(\chi')$ large (i.e. close to $X^{1/4}$).

Evaluating the character sum for $\ell = 3$

We restrict the sum to pairs (χ, χ') with $\Delta(\chi)$ small (i.e. smaller than a power of $\log X$), and with $\Delta(\chi')$ large (i.e. close to $X^{1/4}$).

The main term comes from the r dividing $\Delta(\chi')$ and not dividing $\Delta(\chi)$. Indeed, the prime r contributes the following

$$1 + \chi(r) + \chi^2(r)$$

in the above product for $\mathbf{1}_{\theta_{\chi,\chi'}(\sigma,\tau) \text{ trivial}}$.

Evaluating the character sum for $\ell = 3$

We restrict the sum to pairs (χ, χ') with $\Delta(\chi)$ small (i.e. smaller than a power of $\log X$), and with $\Delta(\chi')$ large (i.e. close to $X^{1/4}$).

The main term comes from the r dividing $\Delta(\chi')$ and not dividing $\Delta(\chi)$. Indeed, the prime r contributes the following

$$1 + \chi(r) + \chi^2(r)$$

in the above product for $\mathbf{1}_{\theta_{\chi,\chi'}(\sigma,\tau) \text{ trivial}}$.

Since χ has small conductor (and r could be small), we get no oscillation when summing over χ.

Evaluating the character sum for $\ell = 3$

We restrict the sum to pairs (χ, χ') with $\Delta(\chi)$ small (i.e. smaller than a power of $\log X$), and with $\Delta(\chi')$ large (i.e. close to $X^{1/4}$).

The main term comes from the r dividing $\Delta(\chi')$ and not dividing $\Delta(\chi)$. Indeed, the prime r contributes the following

$$1 + \chi(r) + \chi^2(r)$$

in the above product for $\mathbf{1}_{\theta_{\chi,\chi'}(\sigma,\tau) \text{ trivial}}$.

Since χ has small conductor (and r could be small), we get no oscillation when summing over χ.

For r dividing $\Delta(\chi)$ (and say not dividing $\Delta(\chi')$), we get

$$1 + \chi'(r) + \chi'^2(r).$$

Evaluating the character sum for $\ell = 3$

We restrict the sum to pairs (χ, χ') with $\Delta(\chi)$ small (i.e. smaller than a power of $\log X$), and with $\Delta(\chi')$ large (i.e. close to $X^{1/4}$).

The main term comes from the r dividing $\Delta(\chi')$ and not dividing $\Delta(\chi)$. Indeed, the prime r contributes the following

$$1 + \chi(r) + \chi^2(r)$$

in the above product for $\mathbf{1}_{\theta_{\chi,\chi'}(\sigma,\tau) \text{ trivial}}$.

Since χ has small conductor (and r could be small), we get no oscillation when summing over χ.

For r dividing $\Delta(\chi)$ (and say not dividing $\Delta(\chi')$), we get

$$1 + \chi'(r) + \chi'^2(r).$$

Since χ' has huge conductor and r is small, we get oscillation when summing over χ'. This follows from the Siegel–Walfisz theorem.

What about $\ell > 3$?

The algebraic results are valid for all odd primes ℓ, but we use that $\ell = 3$ when evaluating the character sum for the following reasons:

What about $\ell > 3$?

The algebraic results are valid for all odd primes ℓ, but we use that $\ell = 3$ when evaluating the character sum for the following reasons:

- $\mathbb{Z}[\zeta_3]$ is a PID. This is very convenient, since any cyclic degree 3 character equals $(\cdot/\pi)_{\mathbb{Z}[\zeta_3],3}$ with π a prime of residue field degree 1 in $\mathbb{Z}[\zeta_3]$;

What about $\ell > 3$?

The algebraic results are valid for all odd primes ℓ, but we use that $\ell = 3$ when evaluating the character sum for the following reasons:

- $\mathbb{Z}[\zeta_3]$ is a PID. This is very convenient, since any cyclic degree 3 character equals $(\cdot/\pi)_{\mathbb{Z}[\zeta_3],3}$ with π a prime of residue field degree 1 in $\mathbb{Z}[\zeta_3]$;
- we make use of cubic reciprocity in $\mathbb{Z}[\zeta_3]$ to rewrite the cubic residue character $(\cdot/\pi)_{\mathbb{Z}[\zeta_3],3}$.

What about $\ell > 3$?

The algebraic results are valid for all odd primes ℓ, but we use that $\ell = 3$ when evaluating the character sum for the following reasons:

- $\mathbb{Z}[\zeta_3]$ is a PID. This is very convenient, since any cyclic degree 3 character equals $(\cdot/\pi)_{\mathbb{Z}[\zeta_3],3}$ with π a prime of residue field degree 1 in $\mathbb{Z}[\zeta_3]$;
- we make use of cubic reciprocity in $\mathbb{Z}[\zeta_3]$ to rewrite the cubic residue character $(\cdot/\pi)_{\mathbb{Z}[\zeta_3],3}$.

It is easy to extend our results to any odd prime ℓ for which $\mathbb{Z}[\zeta_\ell]$ is a PID (i.e. $\ell \in \{3, 5, 7, 11, 13, 17, 19\}$).

What about $\ell > 3$?

The algebraic results are valid for all odd primes ℓ, but we use that $\ell = 3$ when evaluating the character sum for the following reasons:

- $\mathbb{Z}[\zeta_3]$ is a PID. This is very convenient, since any cyclic degree 3 character equals $(\cdot/\pi)_{\mathbb{Z}[\zeta_3],3}$ with π a prime of residue field degree 1 in $\mathbb{Z}[\zeta_3]$;
- we make use of cubic reciprocity in $\mathbb{Z}[\zeta_3]$ to rewrite the cubic residue character $(\cdot/\pi)_{\mathbb{Z}[\zeta_3],3}$.

It is easy to extend our results to any odd prime ℓ for which $\mathbb{Z}[\zeta_\ell]$ is a PID (i.e. $\ell \in \{3, 5, 7, 11, 13, 17, 19\}$).

It is plausible that our results can also be extended to any odd prime ℓ.

That's it!

Thank you for your attention!