Finite subgroups of $\mathrm{PGL}_2(\mathbb{Q})$ and number fields with large class groups

Jean Gillibert (joint with Pierre Gillibert)

LFANT seminar, Bordeaux, April 4, 2023

The general framework

- K : a number field
- $\mathrm{Cl}(K)$: its ideal class group

The general framework

- K : a number field
- $\mathrm{Cl}(K)$: its ideal class group

Basic fact: $\mathrm{Cl}(K)$ is a finite abelian group.

The general framework

- K : a number field
- $\mathrm{Cl}(K)$: its ideal class group

Basic fact: $\mathrm{Cl}(K)$ is a finite abelian group.

Natural questions to ask:

1. What is its size?
2. What is its structure?

The general framework

- K : a number field
- $\mathrm{Cl}(K)$: its ideal class group

Basic fact: $\mathrm{Cl}(K)$ is a finite abelian group.

Natural questions to ask:

1. What is its size?
2. What is its structure?
3. Does these questions have a quantitative answer, depending, say, on the size of the discriminant of K?

A classical result on the size

Assume K runs through **imaginary quadratic fields**. It was conjectured by Gauss, and proved by Heilbronn (1934) that:

$$\lim_{\mathrm{Disc}(K)\to-\infty} \mathrm{Cl}(K) = +\infty.$$

where $\mathrm{Disc}(K)$ denotes the discriminant of K.

A classical result on the size

Assume K runs through **imaginary quadratic fields**. It was conjectured by Gauss, and proved by Heilbronn (1934) that:

$$\lim_{\mathrm{Disc}(K)\to -\infty} \mathrm{Cl}(K) = +\infty.$$

where $\mathrm{Disc}(K)$ denotes the discriminant of K.

On the other hand, it was also conjectured by Gauss that infinitely many **real quadratic fields** have class number one. This problem remains open.

A question about the structure

If $n > 1$ is an integer and M is a finite abelian group, we denote by $\operatorname{rank}_n M$ the largest integer r such that M contains $(\mathbb{Z}/n\mathbb{Z})^r$ as a subgroup.

A question about the structure

If $n > 1$ is an integer and M is a finite abelian group, we denote by $\operatorname{rank}_n M$ the largest integer r such that M contains $(\mathbb{Z}/n\mathbb{Z})^r$ as a subgroup.

Conjecture (Folklore)

Let $d > 1$ and $n > 1$ be two integers. Then $\operatorname{rank}_n \mathrm{Cl}(K)$ is unbounded when K runs through the number fields of degree $[K : \mathbb{Q}] = d$.

A question about the structure

If $n > 1$ is an integer and M is a finite abelian group, we denote by $\mathrm{rank}_n M$ the largest integer r such that M contains $(\mathbb{Z}/n\mathbb{Z})^r$ as a subgroup.

Conjecture (Folklore)

Let $d > 1$ and $n > 1$ be two integers. Then $\mathrm{rank}_n \mathrm{Cl}(K)$ is unbounded when K runs through the number fields of degree $[K : \mathbb{Q}] = d$.

When $n = d$, and more generally when n divides d, this conjecture follows easily from class field theory.

When n and d are coprime, there is not a single case where this Conjecture is known to hold.

It is a classical result (Cornell, 1979) that every finite abelian group is a subgroup of the ideal class group of some cyclotomic extension of $\mathbb{Q}$. In particular, $\operatorname{rank}_n \mathrm{Cl}(K)$ is unbounded when K runs through cyclotomic fields.

It is a classical result (Cornell, 1979) that every finite abelian group is a subgroup of the ideal class group of some cyclotomic extension of $\mathbb{Q}$. In particular, $\operatorname{rank}_n \mathrm{Cl}(K)$ is unbounded when K runs through cyclotomic fields.

In 2021, Mishra, Schoof and Washington proved the same result for real cyclotomic fields.

It is a classical result (Cornell, 1979) that every finite abelian group is a subgroup of the ideal class group of some cyclotomic extension of $\mathbb{Q}$. In particular, $\operatorname{rank}_n \mathrm{Cl}(K)$ is unbounded when K runs through cyclotomic fields.

In 2021, Mishra, Schoof and Washington proved the same result for real cyclotomic fields.

The folklore Conjecture is harder because K varies amongst fields of fixed degree. In fact, a positive answer to this Conjecture would follow from the Cohen-Lenstra heuristics.

Known results beyond the quadratic case

Values of n, d, and r for which we know there exist infinitely many number fields K of degree d with $\mathrm{rank}_n \mathrm{Cl}(K) \geq r$.

Author(s)	Year	n	d	r
Brumer, Rosen	1965	> 1	$d = n$	∞
Ishida	1975	2	prime	$d - 1$
Nakano	1984	> 1	> 1	$\lfloor \frac{d}{2} \rfloor + 1$
	1985	2	> 1	d
Nakano	1988	2	3	6
Levin	2007	> 1	> 1	$\left\lceil \lfloor \frac{d+1}{2} \rfloor + \frac{d}{n-1} - n \right\rceil$
Kulkarni	2017	2	3	8
Levin-Gillibert	2019	2	3	11

The Galois case

Galois variant of the Conjecture: same question, but require in addition that $K/\mathbb{Q}$ is Galois.

The Galois case

Galois variant of the Conjecture: same question, but require in addition that $K/\mathbb{Q}$ is Galois.

Seems to be a harder problem? Yes and no:

The Galois case

Galois variant of the Conjecture: same question, but require in addition that $K/\mathbb{Q}$ is Galois.

Seems to be a harder problem? Yes and no:

- the quadratic case (intensively studied) is Galois (!)

The Galois case

Galois variant of the Conjecture: same question, but require in addition that $K/\mathbb{Q}$ is Galois.

Seems to be a harder problem? Yes and no:

- the quadratic case (intensively studied) is Galois (!)
- Galois extensions have symmetries that make life easier

The Galois case

Galois variant of the Conjecture: same question, but require in addition that $K/\mathbb{Q}$ is Galois.

Seems to be a harder problem? Yes and no:

- the quadratic case (intensively studied) is Galois (!)
- Galois extensions have symmetries that make life easier

The following result is not often cited, according to MathSciNet.

Theorem (Nakano, 1986)

For any $n > 1$, there exist infinitely many cyclic cubic fields K such that $\operatorname{rank}_n \mathrm{Cl}(K) \geq 2$.

Theorem (Nakano, 1986)

For any $n > 1$, there exist infinitely many cyclic cubic fields K such that $\operatorname{rank}_n \mathrm{Cl}(K) \geq 2$.

This is striking:

Theorem (Nakano, 1986)

For any $n > 1$, there exist infinitely many cyclic cubic fields K such that $\operatorname{rank}_n \mathrm{Cl}(K) \geq 2$.

This is striking:

- the field is assumed to be Galois, but the bound is as good as the one for general degree d fields: $\left\lfloor \frac{d}{2} \right\rfloor + 1$

Theorem (Nakano, 1986)

For any $n > 1$, there exist infinitely many cyclic cubic fields K such that $\operatorname{rank}_n \operatorname{Cl}(K) \geq 2$.

This is striking:

- the field is assumed to be Galois, but the bound is as good as the one for general degree d fields: $\left\lfloor \frac{d}{2} \right\rfloor + 1$
- cubic Galois fields are totally real, hence their unit group has rank 2. In Nakano's paper on general degree d, fields are required to have as much complex embeddings as possible (hence smallest possible unit group).

Why do we care about units? because, from our perspective, they tend to reduce the size of the class group.

Nakano considers a polynomial of the form

$$x^3 - \left(\frac{y^n - 3}{2}\right) x^2 - \left(\frac{y^n + 3}{2}\right) x - 1,$$

where x is the indeterminate, and $y \in \mathbb{Z}$ is a parameter.

He proves, under a technical condition on y, that the splitting field K of this polynomial satisfies $\operatorname{rank}_n \mathrm{Cl}(K) \geq 2$.

Nakano considers a polynomial of the form

$$x^3 - \left(\frac{y^n - 3}{2}\right) x^2 - \left(\frac{y^n + 3}{2}\right) x - 1,$$

where x is the indeterminate, and $y \in \mathbb{Z}$ is a parameter.

He proves, under a technical condition on y, that the splitting field K of this polynomial satisfies $\operatorname{rank}_n \mathrm{Cl}(K) \geq 2$.

On the other hand, K is known to be a cyclic Galois extension of the rationals, of degree 3. It is a member of the family

$$x^3 - tx^2 - (t+3)x - 1,$$

which is the **generic** cyclic cubic field.

Nakano's trick: we have the following factorisation

$$
\begin{aligned}
& x^3 - \left(\frac{y^n - 3}{2}\right) x^2 - \left(\frac{y^n + 3}{2}\right) x - 1 \\
&\quad = \frac{1}{2}\left((2x^3 + 3x^2 - 3x - 2) - y^n(x^2 + x)\right) \\
&\quad = \frac{1}{2}\left((x-1)(x+2)(2x+1) - y^n x(x+1)\right).
\end{aligned}
$$

This yields, in the field K, the relation

$$(x-1)(x+2)(2x+1) = y^n x(x+1)$$

Nakano's assumption: y is coprime to 6.

Then our polynomial has integral coefficients, hence x is an algebraic integer, and in fact **is a unit** (its minimal polynomial has constant coefficient -1).

Nakano's assumption: y is coprime to 6.

Then our polynomial has integral coefficients, hence x is an algebraic integer, and in fact **is a unit** (its minimal polynomial has constant coefficient -1).

Now, the **Galois conjugates** of x, which are

$$-\frac{1}{x+1} \quad \text{and} \quad -\left(1+\frac{1}{x}\right)$$

are also units, and in particular $x+1$ is a unit.

The right-hand side of the relation

$$(x-1)(x+2)(2x+1) = y^n x(x+1)$$

is a unit times a n-th power, and on the left-hand side we have three coprime ideals (again, y is coprime to 6).

Conclusion : $(x-1)$, $(x+2)$ and $(2x+1)$ are n-th powers of ideals I_1, I_2 and I_3.

The right-hand side of the relation

$$(x-1)(x+2)(2x+1) = y^n x(x+1)$$

is a unit times a n-th power, and on the left-hand side we have three coprime ideals (again, y is coprime to 6).

Conclusion : $(x-1)$, $(x+2)$ and $(2x+1)$ are n-th powers of ideals I_1, I_2 and I_3.

End of Nakano's proof (analytic number theory): there exist infinitely many values of $y \in \mathbb{Z}$ for which the smallest relation between I_1, I_2 and I_3 is the one given by the above identity:

$$I_1 I_2 I_3 = (y).$$

In particular, any two of these ideals generate a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^2$ in the class group of K.

We ask:

- are there nice families of cyclic fields of larger degree?
- if yes, can we generalize Nakano's result?
- what are the underlying geometric objects?

We ask:

- are there nice families of cyclic fields of larger degree?
- if yes, can we generalize Nakano's result?
- what are the underlying geometric objects?

Advantage of the geometric approach: the analytic number theory trick is replaced by Hilbert's irreducibility theorem.

Only the first part of the proof (construction of the polynomial with nice factorisation) needs to be generalized.

Serre's book Topics in Galois Theory

Serre explains how to construct, from a finite subgroup G of $\mathrm{PGL}_2(\mathbb{Q}) = \mathrm{Aut}(\mathbb{P}^1)$, a one-parameter family of Galois extensions of $\mathbb{Q}$ with group G: it suffices to find a rational map

$$h : \mathbb{P}^1 \to \mathbb{P}^1$$

which is G-invariant, and has degree $\#G$.

Then this map is a Galois cover of curves with group G, hence corresponds to a regular Galois extension of $\mathbb{Q}(t)$ with group G.

Nakano's construction, revisited

The automorphism

$$\sigma : z \mapsto -\frac{1}{z+1}$$

had order 3, and the map

$$h : x \mapsto \frac{(x-1)(x+2)(2x+1)}{x(x+1)}$$

is invariant under σ. For a generic $t \in \mathbb{P}^1$, the splitting field of $h^{-1}(t)$ is a cubic Galois extension. But the relation $h(x) = t$ is equivalent to

$$(x-1)(x+2)(2x+1) - tx(x+1) = 0.$$

We recover Nakano's family, with t instead of y^n.

The finite subgroups of $PGL_2(\mathbb{Q})$

We now reformulate our questions:

The finite subgroups of $\mathrm{PGL}_2(\mathbb{Q})$

We now reformulate our questions:

- can we replace σ (or order three) by an element of larger order in $\mathrm{PGL}_2(\mathbb{Q})$?
- can we generalize Nakano's factorisation trick?

The finite subgroups of $\mathrm{PGL}_2(\mathbb{Q})$

We now reformulate our questions:

- can we replace σ (or order three) by an element of larger order in $\mathrm{PGL}_2(\mathbb{Q})$?
- can we generalize Nakano's factorisation trick?

It is well-known that any cyclic group is a subgroup of $\mathrm{PGL}_2(\mathbb{C})$.

The finite subgroups of $\mathrm{PGL}_2(\mathbb{Q})$

We now reformulate our questions:

- can we replace σ (or order three) by an element of larger order in $\mathrm{PGL}_2(\mathbb{Q})$?
- can we generalize Nakano's factorisation trick?

It is well-known that any cyclic group is a subgroup of $\mathrm{PGL}_2(\mathbb{C})$.

Unfortunately, very few of them are defined over $\mathbb{Q}$, more precisely the finite cyclic subgroups of $\mathrm{PGL}_2(\mathbb{Q})$ are

$$\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}$$

to which one should add the dihedral groups D_2, D_3, D_4 and D_6.

Nakano's map

All the trick lies in this map h, which is both invariant under σ, and has a nice factorization

$$h : x \mapsto \frac{(x-1)(x+2)(2x+1)}{x(x+1)}.$$

Where does the factorization comes from?

Nakano's map

All the trick lies in this map h, which is both invariant under σ, and has a nice factorization

$$h : x \mapsto \frac{(x-1)(x+2)(2x+1)}{x(x+1)}.$$

Where does the factorization comes from? We have

$$\sigma(1) = -1/2, \quad \sigma(-1/2) = -2$$

and

$$\sigma(0) = -1, \quad \sigma(-1) = \infty.$$

In other words, the set of zeroes (resp. poles) of h is an orbit under the action of σ.

A general construction

Lemma

Let $G \leq \mathrm{PGL}_2(\mathbb{Q})$ be a finite subgroup. Let $a, b \in \mathbb{P}^1(\mathbb{Q})$ be two points which do not lie in the same orbit under the action of G. Then the map

$$h : \mathbb{P}^1 \to \mathbb{P}^1; \quad x \mapsto \prod_{\sigma \in G} \frac{x - \sigma(a)}{x - \sigma(b)}$$

is a Galois cover with group G.

Curves with large Picard group

Lemma

Let G, a and b as before. Let $n > 1$ be an integer which is coprime to the orders of the stabilizers of a and b, and let $\lambda \in \mathbb{Q}^\times$.
Then the polynomial

$$\prod_{\sigma \in G} (x - \sigma(a)) - \lambda y^n \prod_{\sigma \in G} (x - \sigma(b))$$

defines a geometrically irreducible curve C over $\mathbb{Q}$, such that:

(1) *the y-coordinate map $C \to \mathbb{P}^1$ is a Galois cover with group G;*

(2) *the Picard group of C contains a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{\#\,\mathrm{orb}(a) + \#\,\mathrm{orb}(b) - 2}$.*

The parameter λ allows to normalize the polynomial so that its roots are algebraic units (key ingredient in Nakano's proof).

From geometry to arithmetic (Levin 2007)

Let C be a smooth projective geometrically irreducible curve over $\mathbb{Q}$, and let $n > 1$ be an integer. Let $D_1, \ldots, D_s$ be divisors on C whose classes in $\mathrm{Pic}(C)$ generate a subgroup isomorphic to $(\mathbb{Z}/n\mathbb{Z})^s$, and let $g_1, \ldots, g_s$ be rational functions on C such that $\mathrm{div}(g_i) = nD_i$ for all i. Assume that there exists a finite map $\phi : C \to \mathbb{P}^1$ of degree $d > 1$ such that, for all $t \in \mathbb{N}$, the point $P_t := \phi^{-1}(t)$ has the property that

$$g_1(P_t), \ldots, g_s(P_t) \text{ define classes in } \mathrm{Sel}^n(\mathbb{Q}(P_t)), \text{ where}$$
$$\mathrm{Sel}^n(K) := \{\gamma \in K^\times/(K^\times)^n; \forall v \text{ finite place of } K,\ v(\gamma) \equiv 0 \pmod{n}\}.$$

Then for all but $O(\sqrt{N})$ values $t \in \{1, \ldots, N\}$, the field $\mathbb{Q}(P_t)$ satisfies $[\mathbb{Q}(P_t) : \mathbb{Q}] = d$ and

$$\mathrm{rank}_n \, \mathrm{Cl}(\mathbb{Q}(P_t)) \geq s - \mathrm{rank}_{\mathbb{Z}} \, \mathcal{O}^\times_{\mathbb{Q}(P_t)}.$$

Moreover, there are infinitely many isomorphism classes of such $\mathbb{Q}(P_t)$.

It remains to apply to our curves this geometric machinery, where $\phi = \frac{y-y_0}{N}$ for a careful choice of y_0 and N (i.e. a congruence condition on $y \pmod{N}$). We thus obtain by specialization of y infinitely many fields $K/\mathbb{Q}$ with

(1) $Gal(K/\mathbb{Q}) = G$

(2) $\operatorname{rank}_n \mathrm{Cl}(K) \geq \#\operatorname{orb}(a) + \#\operatorname{orb}(b) - 2 - \operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K^\times$

Note that $\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K^\times = \#G - 1$ or $\frac{\#G}{2} - 1$ (K is either totally real or totally complex).

When $\#\operatorname{orb}(a) = \#\operatorname{orb}(b) = \#G$, then K is totally real and the resulting lower bound on the rank is $\#G - 1$.

Surprisingly, the totally complex case yields the same bound.

The main result

Reminder: the finite subgroups of $\mathrm{PGL}_2(\mathbb{Q})$ are

$$\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z},$$
$$D_2 = (\mathbb{Z}/2\mathbb{Z})^2, \quad D_3 = \mathfrak{S}_3, \quad D_4, \quad D_6,$$

The main result

Reminder: the finite subgroups of $\mathrm{PGL}_2(\mathbb{Q})$ are

$$\begin{gathered}\mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/3\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/6\mathbb{Z}, \\ D_2 = (\mathbb{Z}/2\mathbb{Z})^2, \quad D_3 = \mathfrak{S}_3, \quad D_4, \quad D_6,\end{gathered}$$

Theorem

For any of these groups, and for any integer n coprime to 6, there exist infinitely many number fields K such that

(1) *$K/\mathbb{Q}$ is Galois with group G;*

(2) $\mathrm{rank}_n \mathrm{Cl}(K) \geq \#G - 1$.

This result is quantitative: we produce explicitly a positive density of such fields, when ordered by discriminant.

Some comments

It was proved by Nakano that, given $n > 1$ and $(r_1, r_2) \in \mathbb{N}^2$, there exist infinitely many number fields K with r_1 real places and r_2 complex places such that

$$\operatorname{rank}_n \mathrm{Cl}(K) \geq r_2 + 1.$$

The only improvements are for $(r_1, r_2) = (3, 0)$ (Nakano's cyclic cubic fields), or for specific values of n.

Some comments

It was proved by Nakano that, given $n > 1$ and $(r_1, r_2) \in \mathbb{N}^2$, there exist infinitely many number fields K with r_1 real places and r_2 complex places such that

$$\operatorname{rank}_n \mathrm{Cl}(K) \geq r_2 + 1.$$

The only improvements are for $(r_1, r_2) = (3, 0)$ (Nakano's cyclic cubic fields), or for specific values of n.

Our Theorem improves on Nakano's inequality for all n coprime to 6, in the following cases:

$$(r_1, r_2) = (4, 0), (6, 0), (0, 3), (0, 4) \text{ and } (0, 6).$$

Cyclic quartic fields with n-rank ≥ 3

Consider the polynomial

$$\begin{aligned} C_4P &= \frac{1}{6}\left((x-2)(2x+1)(x+3)(3x-1) + y^n x(x-1)(x+1)\right) \\ &= x^4 + \left(\frac{y^n+7}{6}\right)x^3 - 6x^2 - \left(\frac{y^n+7}{6}\right)x + 1. \end{aligned}$$

Assume n is odd. Then there exist infinitely many values of $y \in \mathbb{Z}$ (with $y \equiv 5 \pmod{12}$ and $5 \nmid y$), such that the corresponding field has class group of n-rank ≥ 3.

For X large enough, the number of such fields whose discriminant is bounded above by X is $\gg X^{1/6n}$.

Cyclic sextic fields with n-rank ≥ 5

Consider the polynomial

$$C_6 P = \frac{1}{120}((x-3)(x+4)(2x+1)(3x-2)(4x-5)(5x-1) \\ + y^n x(x-1)(x+1)(x-2)(2x-1))$$

Assume n is coprime to 6. Then there exist infinitely many values of $y \in \mathbb{Z}$ such that the corresponding field has class group of n-rank ≥ 5.

For X large enough, the number of such fields whose discriminant is bounded above by X is $\gg X^{1/10n}$.

The symmetric group $\mathfrak{S}_3$

The splitting field of the polynomial

$$x^6+3x^5+8668877802x^4+17337755599x^3+8668877802x^2+3x+1$$

is a totally imaginary Galois extension of $\mathbb{Q}$ with group $\mathfrak{S}_3$.
One computes with Pari/GP that its ideal class group has 5-rank exactly 6, which is one more than expected.

We found many similar examples, which is surprising since we were able to compute a ridiculously small number of examples.
(It takes a huge amount of time to compute class groups of fields of degree $d > 2$.)

Future directions:

- Emma Lehmer's quintic polynomial (cyclic quintic field)

$$x^5 + t^2x^4 - 2(t^3 + 3t^2 + 5t + 5)x^3 + (t^4 + 5t^3 + 11t^2 + 15t + 5)x^2 + (t^3 + 4t^2 + 10t + 10)x + 1$$

  which corresponds to the covering of modular curves $X_1(25) \to X_0(25) \simeq \mathbb{P}^1$.
- More general coverings of modular curves?
- If $G \leq \mathrm{PGL}_3(\mathbb{Q})$ is a finite subgroup, then $\mathbb{P}^2/G$ is rational (Trepalin 2014), which yields a two-parameter family of Galois extensions.

Thank you for your attention!