From covers of curves to large class groups

Jean Gillibert (joint with Yuri Bilu)

International Conference on Class Groups of Number Fields and Related Topics, HRI, Allahabad
September 4, 2017

The general problem

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

The general problem

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

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

The general problem

- 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 problem

- 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 $\mathrm{rank}_n M$ 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 $\mathrm{rank}_n M$ the largest integer r such that M contains $(\mathbb{Z}/n\mathbb{Z})^r$ as a subgroup.

The following conjecture is widely believed to be true:

Conjecture (Folklore)

Let $n > 1$ be an integer. Then $\mathrm{rank}_n \mathrm{Cl}(K)$ is unbounded when K runs through all quadratic fields.

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.

The following conjecture is widely believed to be true:

Conjecture (Folklore)

Let $n > 1$ be an integer. Then $\mathrm{rank}_n \mathrm{Cl}(K)$ is unbounded when K runs through all quadratic fields.

More generally, this conjecture is believed to hold for fields of arbitrary (fixed) degree > 1.

Table of values n and r for which it is known that there exist infinitely many quadratic fields K with $\text{rank}_n \text{Cl}(K) \geq r$.

Author(s)	Year	Type	n	r
Gauss	19th c.	imaginary, real	2	∞
Nagell	1922	imaginary	> 1	1
Yamamoto	1970	imaginary	> 1	2
Yamamoto, Weinberger	1970, 1973	real	> 1	1
Craig	1973	imaginary real	3 3	3 2
Craig	1977	imaginary real	3 3	4 3
Diaz	1978	real	3	4
Mestre	1980	imaginary, real	$5, 7$	2
Mestre	1992	imaginary, real	5	3

Class field theory approach

Let K be a number field, and let H be its Hilbert class field (maximal everywhere unramified abelian extension of K).

According to class field theory, we have a canonical isomorphism

$$\mathrm{Gal}(H/K) \simeq \mathrm{Cl}(K).$$

Class field theory approach

Let K be a number field, and let H be its Hilbert class field (maximal everywhere unramified abelian extension of K).

According to class field theory, we have a canonical isomorphism

$$\mathrm{Gal}(H/K) \simeq \mathrm{Cl}(K).$$

It follows from Galois theory that, given an abelian group Γ, an everywhere unramified Galois extensions of K with group Γ corresponds to a surjective morphism $\mathrm{Cl}(K) \twoheadrightarrow \Gamma$.

Strategy for making $\mathrm{rank}_n \mathrm{Cl}(K)$ large

If one is able to construct an everywhere unramified extension of K with Galois group $(\mathbb{Z}/n\mathbb{Z})^r$, this implies that

$$\mathrm{rank}_n \mathrm{Cl}(K) \geq r,$$

because $\mathrm{Cl}(K)$ has $(\mathbb{Z}/n\mathbb{Z})^r$ as a quotient.

Specialization of covers of curves

Consider the following setting:

- C is a smooth, geometrically irreducible, projective curve defined over some number field k.
- $D \to C$ is an étale (unramified) geometrically irreducible Galois cover of C with group $(\mathbb{Z}/n\mathbb{Z})^r$.

Specialization of covers of curves

Consider the following setting:

- C is a smooth, geometrically irreducible, projective curve defined over some number field k.
- $D \to C$ is an étale (unramified) geometrically irreducible Galois cover of C with group $(\mathbb{Z}/n\mathbb{Z})^r$.

Basic idea: if $P \in C(\overline{k})$ is a point, and if K is the field of definition of P, then one can specialize (or pull-back) the cover $D \to C$ into a Galois extension L/K.

Advantages of this technique

Advantages of this technique

- It is technically easier to construct unramified covers of curves than everywhere unramified extensions of number fields.

Advantages of this technique

- It is technically easier to construct unramified covers of curves than everywhere unramified extensions of number fields.
- By varying the point P, one cover $D \to C$ allows to build infinitely many field extensions L/K.

Advantages of this technique

- It is technically easier to construct unramified covers of curves than everywhere unramified extensions of number fields.
- By varying the point P, one cover $D \to C$ allows to build infinitely many field extensions L/K.
- Gives a theoretical framework for generalizing results by Mestre in the $n = 5$ case!

Problems which arise immediately

Problems which arise immediately

1. When specializing the cover $D \to C$, the extension L/K obtained has in general a smaller Galois group than $D \to C$.

Problems which arise immediately

1. When specializing the cover $D \to C$, the extension L/K obtained has in general a smaller Galois group than $D \to C$.
2. The extension L/K obtained is in general ramified.

Problems which arise immediately

1. When specializing the cover $D \to C$, the extension L/K obtained has in general a smaller Galois group than $D \to C$.
2. The extension L/K obtained is in general ramified.

Hints:

1. Hilbert's irreducibility theorem ensures us that for infinitely many points P, the extension L/K has the same Galois group as the cover $D \to C$.
2. According to the Chevalley-Weil theorem, the extension L/K is unramified outside places of bad reduction of C, and places dividing n.

Hilbert's irreducibility theorem

Consider a finite morphism $t : C \to \mathbb{P}^1$ of degree d. By applying Hilbert's irreducibility theorem to the composite cover

$$D \xrightarrow{\phi} C \xrightarrow{t} \mathbb{P}^1$$

one finds that there exist infinitely many $\alpha \in \mathbb{P}^1(k)$ whose inverse image by $t \circ \phi$ is irreducible.

Hilbert's irreducibility theorem

Consider a finite morphism $t : C \to \mathbb{P}^1$ of degree d. By applying Hilbert's irreducibility theorem to the composite cover

$$D \xrightarrow{\ \phi\ } C \xrightarrow{\ t\ } \mathbb{P}^1$$

one finds that there exist infinitely many $\alpha \in \mathbb{P}^1(k)$ whose inverse image by $t \circ \phi$ is irreducible.

For such α, the point $P = t^{-1}(\alpha)$ is defined over a field K of degree $[K : k] = d$, and $\phi^{-1}(P)$ is defined over a Galois extension L/K with Galois group $(\mathbb{Z}/n\mathbb{Z})^r$.

Chevalley-Weil theorem

For each field K as above, the extension L/K is unramified outside the finite set

$$S := \{\text{places of bad reduction of } C\} \cup \{\text{places dividing } n\} \\ \cup \{\text{places at infinity}\}.$$

Chevalley-Weil theorem

For each field K as above, the extension L/K is unramified outside the finite set

$$S := \{\text{places of bad reduction of } C\} \cup \{\text{places dividing } n\} \\ \cup \{\text{places at infinity}\}.$$

In order to avoid ramification, we shall impose local conditions at each place in S.

Geometric Krasner's Lemma

Let:

Geometric Krasner's Lemma

Let:

- v be a place of k.
- $P_0 \in C(k)$ be a rational point of C.
- L_0 be the field of definition of $\phi^{-1}(P_0)$.

Geometric Krasner's Lemma

Let:

- v be a place of k.
- $P_0 \in C(k)$ be a rational point of C.
- L_0 be the field of definition of $\phi^{-1}(P_0)$.

Lemma (Geometric Krasner's Lemma)

If $P \in C(\overline{k})$ is v-adically close enough from P_0, then the factorization of places above v in the extension L/K is similar to the factorization of v in the extension L_0/k.

Totally split primes

Special case of Geometric Krasner's Lemma:
Assume that the inverse image of P_0 by ϕ consists only of k-rational points, so that $L_0 = k$.

Totally split primes

Special case of Geometric Krasner's Lemma:
Assume that the inverse image of P_0 by ϕ consists only of k-rational points, so that $L_0 = k$.

Then, if P is v-adically close enough from P_0, places above v are totally split in L/K, and in particular are **unramified** in this extension.

Totally split primes

Special case of Geometric Krasner's Lemma:
Assume that the inverse image of P_0 by ϕ consists only of k-rational points, so that $L_0 = k$.

Then, if P is v-adically close enough from P_0, places above v are totally split in L/K, and in particular are **unramified** in this extension.

There is no reason why this should happen, but...

Twisting Galois covers

Consider a Galois cover $\phi : D \to C$ with group Γ, and a rational point $P_0 \in C(k)$.

It is possible to twist (by some Galois cocycle $\sigma : \mathrm{Gal}(\overline{k}/k) \to \Gamma$) the cover ϕ in such a way that the inverse image of P_0 by the twisted cover ϕ^σ consists only of k-rational points.

If Γ is commutative, then ϕ^σ is again a Galois cover with group Γ.

So, if we choose some $P_0 \in C(k)$, we may now assume that our cover $\phi : D \to C$ has this property with respect to P_0.

Needed properties of $t : C \to \mathbb{P}^1$

Reminder: the points $P \in C(\overline{k})$ we consider are obtained as $P_\alpha := t^{-1}(\alpha)$ for some $\alpha \in \mathbb{P}^1(k)$.

Needed properties of $t : C \to \mathbb{P}^1$

Reminder: the points $P \in C(\overline{k})$ we consider are obtained as $P_\alpha := t^{-1}(\alpha)$ for some $\alpha \in \mathbb{P}^1(k)$.

Question: how is it possible to ensure that P_α is v-adically close enough from some fixed P_0?

Needed properties of $t : C \to \mathbb{P}^1$

Reminder: the points $P \in C(\overline{k})$ we consider are obtained as $P_\alpha := t^{-1}(\alpha)$ for some $\alpha \in \mathbb{P}^1(k)$.

Question: how is it possible to ensure that P_α is v-adically close enough from some fixed P_0?

Idea: if t is totally ramified at P_0, then when α is close enough from $t(P_0)$, the point P_α is close enough from P_0.

Needed properties of $t : C \to \mathbb{P}^1$

Reminder: the points $P \in C(\overline{k})$ we consider are obtained as $P_\alpha := t^{-1}(\alpha)$ for some $\alpha \in \mathbb{P}^1(k)$.

Question: how is it possible to ensure that P_α is v-adically close enough from some fixed P_0?

Idea: if t is totally ramified at P_0, then when α is close enough from $t(P_0)$, the point P_α is close enough from P_0.

(This idea looks really stupid, but we don't have a better one for the moment.)

Theorem (Bilu-G. 2016)

Consider:

- *a smooth, projective, geometrically irreducible curve C defined over a number field k;*
- *a geometrically irreducible Galois cover $D \to C$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^r$.*

Theorem (Bilu-G. 2016)

Consider:

- *a smooth, projective, geometrically irreducible curve C defined over a number field k;*
- *a geometrically irreducible Galois cover $D \to C$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^r$.*

Assume that C admits a finite morphism $t : C \to \mathbb{P}^1$ of degree d, totally ramified at some k-rational point of C.

Theorem (Bilu-G. 2016)

Consider:

- *a smooth, projective, geometrically irreducible curve C defined over a number field k;*
- *a geometrically irreducible Galois cover $D \to C$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^r$.*

Assume that C admits a finite morphism $t : C \to \mathbb{P}^1$ of degree d, totally ramified at some k-rational point of C.

Then there exists infinitely many number fields K with $[K : k] = d$ such that

$$\mathrm{rank}_n \mathrm{Cl}(K) \geq r + \mathrm{rank}_n \mathrm{Cl}(k).$$

Quantitative version

Let m be the (smallest) degree of a rational function x such that $k(C) = k(t, x)$. We measure the size of $\mathrm{Disc}(K/k)$ by putting

$$\mathcal{D}(K/k) := \left|\mathcal{N}_{k/\mathbb{Q}} \mathrm{Disc}(K/k)\right|^{1/[k:\mathbb{Q}]}.$$

Quantitative version

Let m be the (smallest) degree of a rational function x such that $k(C) = k(t, x)$. We measure the size of $\mathrm{Disc}(K/k)$ by putting

$$\mathcal{D}(K/k) := \left|\mathcal{N}_{k/\mathbb{Q}} \mathrm{Disc}(K/k)\right|^{1/[k:\mathbb{Q}]}.$$

Using a quantitative version of Hilbert's irreducibility theorem due to Dvornicich and Zannier, we prove the following:

Quantitative version

Let m be the (smallest) degree of a rational function x such that $k(C) = k(t, x)$. We measure the size of $\mathrm{Disc}(K/k)$ by putting

$$\mathcal{D}(K/k) := \left|\mathcal{N}_{k/\mathbb{Q}} \mathrm{Disc}(K/k)\right|^{1/[k:\mathbb{Q}]}.$$

Using a quantitative version of Hilbert's irreducibility theorem due to Dvornicich and Zannier, we prove the following:

For all sufficiently large $X > 0$, the number of isomorphism classes of fields K as above, and such that $\mathcal{D}(K/k) \leq X$, is at least

$$cX^{[k:\mathbb{Q}]/2m(d-1)}/\log X$$

where $c > 0$ is some constant depending on C, t, x and k.

A cyclotomic example, via Fermat curves

Let $p \geq 3$ be a prime, and let d be an integer such that $2 \leq d \leq p - 1$.

Let C be the smooth projective curve defined by the affine equation

$$y^p = x^{d-1}(1-x)$$

(This is a quotient of the Fermat curve).

A cyclotomic example, via Fermat curves

Let $p \geq 3$ be a prime, and let d be an integer such that $2 \leq d \leq p-1$.

Let C be the smooth projective curve defined by the affine equation

$$y^p = x^{d-1}(1-x)$$

(This is a quotient of the Fermat curve).

Because p and d are coprime, the curve C has a unique point at infinity, and the coordinate map $y : C \to \mathbb{P}^1$ is totally ramified at this point, with degree d.

Greenberg's result

Let $\mathbb{Q}(\zeta_p)$ be the p-th cyclotomic field.

Greenberg's result

Let $\mathbb{Q}(\zeta_p)$ be the p-th cyclotomic field.

Theorem (Greenberg, 1981)

Let $J(C)$ be the Jacobian of C. Then $J(C)(\mathbb{Q}(\zeta_p))$ contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$.

Greenberg's result

Let $\mathbb{Q}(\zeta_p)$ be the p-th cyclotomic field.

Theorem (Greenberg, 1981)

Let $J(C)$ be the Jacobian of C. Then $J(C)(\mathbb{Q}(\zeta_p))$ contains a subgroup isomorphic to $(\mathbb{Z}/p\mathbb{Z})^3$.

This subgroup allows us, via Kummer theory, to construct a Galois cover of C with group $(\mathbb{Z}/p\mathbb{Z})^3$, defined over the field $\mathbb{Q}(\zeta_p)$.

A real life example!

Theorem

Let $p \geq 3$ *be a prime, and let* d *be an integer such that* $2 \leq d \leq p-1$*. Then there exist infinitely many extensions* $K/\mathbb{Q}(\zeta_p)$ *with* $[K:\mathbb{Q}(\zeta_p)] = d$ *such that*

$$\operatorname{rank}_p \mathrm{Cl}(K) \geq 3 + \operatorname{rank}_p \mathrm{Cl}(\mathbb{Q}(\zeta_p)).$$

More precisely, for sufficiently large positive X*, the number of such* K *with* $\mathcal{D}(K/\mathbb{Q}(\zeta_p)) \leq X$ *is at least* $cX^{(p-1)/2p(d-1)}/\log X$*, where* c *only depends on* p*.*

A real life example!

Theorem

Let $p \geq 3$ be a prime, and let d be an integer such that $2 \leq d \leq p-1$. Then there exist infinitely many extensions $K/\mathbb{Q}(\zeta_p)$ with $[K : \mathbb{Q}(\zeta_p)] = d$ such that

$$\operatorname{rank}_p \operatorname{Cl}(K) \geq 3 + \operatorname{rank}_p \operatorname{Cl}(\mathbb{Q}(\zeta_p)).$$

More precisely, for sufficiently large positive X, the number of such K with $\mathcal{D}(K/\mathbb{Q}(\zeta_p)) \leq X$ is at least $cX^{(p-1)/2p(d-1)}/\log X$, where c only depends on p.

Example: there exist infinitely many quadratic extensions $K/\mathbb{Q}(\zeta_{37})$ such that $\operatorname{rank}_{37} \operatorname{Cl}(K) \geq 4$.

Thank you for your attention!