Computing class groups using norm relations

A. Page
joint work with J.-F. Biasse, C. Fieker and T. Hofmann

COUNT conference, CIRM, Luminy
Inria / Université de Bordeaux

03/03/2023

Computing class groups

Goal : given a number field K, compute $\mathrm{Cl}(K)$.

Notation : absolute value of discriminant Δ_K, degree n.

Assuming GRH :

- Heuristic : $\exp(\tilde{\mathcal{O}}(\log \Delta_K)^\alpha)$ for $1/3 \leq \alpha \leq 2/3$.
- Practice : impossible for $n > 150$.

Unconditionally : $\tilde{\mathcal{O}}(\Delta_K^{1/2})$.

New examples : under GRH

- $K = \mathbb{Q}(\zeta_{6552})$
- $n = 1728$
- $\Delta_K = 2^{3456} \cdot 3^{2592} \cdot 7^{1440} \cdot 13^{1584} \approx 10^{5258}$
- $(\log \Delta_K)^2 \approx 10^8$

$\mathrm{Cl}(K)$ computed in 4.2 hours on a laptop.

- $\mathrm{rk}_2\,\mathrm{Cl}(K) = 112$
- $\mathrm{rk}_3\,\mathrm{Cl}(K) = 101$
- $h^+_{6552} = 70695077806080 = 2^{24} \cdot 3^3 \cdot 5 \cdot 7^4 \cdot 13 \approx 7 \cdot 10^{13}$

New examples : unconditionally

- $K = \mathbb{Q}(\zeta_{2520})$
- $n = 576$
- $\Delta_K = 2^{1152} \cdot 3^{864} \cdot 5^{432} \cdot 7^{480} \approx 10^{1466}$
- Minkowski bound $\approx 10^{515}$

$\mathrm{Cl}(K)$ computed in 44 hours with a single core.

- $\mathrm{rk}_2 \, \mathrm{Cl}(K) = 38$
- $\mathrm{rk}_3 \, \mathrm{Cl}(K) = 15$
- $h^+_{2520} = 208 = 2^4 \cdot 13$

Buchmann's algorithm

Algorithm :

- Choose S set of primes generating $\mathrm{Cl}(K)$ (GRH).
- Find S-units $R \subset \mathbb{Z}_{K,S}^{\times}$.
- Compute $C = \mathbb{Z}^S / \langle R \rangle$ and $U = \ker(\langle R \rangle \to \mathbb{Z}^S)$.
- Check if $\langle R \rangle = \mathbb{Z}_{K,S}^{\times}$ using class number formula.
- Output C.

Using automorphisms

Question : assume K has a nontrivial group G of automorphisms. Can we use this to compute $\mathrm{Cl}(K)$ faster ?

- Use action of G to get extra relations for free.
- Use structure of module over the group ring for faster linear algebra ?
- By Galois theory, K has many subfields.

Norm relations

For $H \leq G$, define the *norm element*

$$N_H = \sum_{h \in H} h \in \mathbb{Z}[G].$$

Wada, Bauch–Bernstein–de Valence–Lange–van Vredendaal, Biasse–van Vredendaal : $G = C_2 \times C_2 = \langle \sigma, \tau \rangle$.

$$2 = N_{\langle \sigma \rangle} + N_{\langle \sigma \rangle} - \sigma N_{\langle \sigma\tau \rangle}.$$

Parry, Lesavourey–Plantard–Susilo : $G = C_3 \times C_3 = \langle u, v \rangle$.

$$3 = N_{\langle u \rangle} + N_{\langle v \rangle} + N_{\langle uv \rangle} - (u + uv) N_{\langle u^2 v \rangle}.$$

Norm relations

Definition : *norm relation* with *denominator d*

$$d = \sum_{i=1}^{k} a_i N_{H_i} b_i$$

with $a_i, b_i \in \mathbb{Z}[G]$ and $d \in \mathbb{Z}_{>0}$.

Proposition : Let M be a $\mathbb{Z}[G]$-module. Then the exponent of

$$M/\langle M^{H_1}, \ldots, M^{H_k} \rangle_{\mathbb{Z}[G]}$$

is finite and divides d.

Proof : Let $m \in M$. Then

$$dm = \sum_i a_i N_{H_i} b_i m \in \sum_i a_i M^{H_i}.$$

S-units

Apply to M the S-units of K :
The S-units of the subfields $K_i = K^{H_i}$ generate a $\mathbb{Z}[G]$-submodule of finite index in the S-units of K.

Algorithm (S-units with a norm relation) :

- For each subfield $K_i = K^{H_i}$, compute S-unit group $\mathbb{Z}_{K_i,S}^\times$.
- Compute $\mathbb{Z}[G]$-module generated by all $\mathbb{Z}_{K_i,S}^\times$.
- Extract all possible d-th powers to obtain $\mathbb{Z}_{K,S}^\times$.
- Output $\mathbb{Z}_{K,S}^\times$.

Saturation

Problem : from $R \subset K^\times$, compute $R' = \{x \in K^\times \text{ s.t. } x^d \in R\}$.

Saturation algorithm (Pohst–Zassenhaus, rediscovered many times) :

- Use reduction modulo primes to detect powers.
- Compute d-th roots.
- Terminate or add more primes.

Biasse–Fieker–Hofmann–P. : under GRH, polynomial bound on the set of primes required.

Denominators of norm relations

Can we control the denominator d ?

Theorem (Biasse–Fieker–Hofmann–P.)

If G admits a norm relation using certain subgroups, then it also admits one with d dividing $|G|^3$ and using the same subgroups.

Proof sketch : There is a representation-theoretic interpretation of existence of a norm relation. Rewrite it in terms of idempotents, and estimate the denominators of the idempotents.

Reduction to the subfields

Theorem (Biasse–Fieker–Hofmann–P.)

Assume GRH. Let G admitting a norm relation. The computation of the group of S-units reduces in deterministic polynomial time from any K with an action of G to the corresponding subfields.

Existence of norm relations

When do such relations exist ?

Theorem (Biasse–Fieker–Hofmann–P., Wolf)

A finite group G admits a norm relation if and only if G contains

- *a non-cyclic subgroup of order pq (p,q, primes not necessarily distinct), or*
- *a subgroup isomorphic to* $\mathrm{SL}_2(\mathbb{F}_p)$ *where* $p = 2^{2^k} + 1$ *is a Fermat prime with* $k > 1$*.*

Also : criterion to test existence with specific subgroups, more precise information in the abelian case.

Back to the example

- $K = \mathbb{Q}(\zeta_{6552})$
- $n = 1728$
- Galois group $G \cong C_{12} \times C_6^2 \times C_2^2$
- Relation with $d = 1$ reducing to 62 subfields of degree ≤ 192.
- Relations with d a power of 2 or 3 reducing to 672 subfields of degree ≤ 12.

Implementations

- Implementation in Julia (Nemo/Hecke) : general case.
- Implementation in gp : requires K to be Galois over $\mathbb{Q}$, only uses relations coming from abelian subgroups, only computes the class group, possible infinite loop, but faster.
- Implementation in libpari : general case, TODO !

Questions ?

Thank you !

Remember :

- Notion of "norm relation" in G.
- Recover M from the M^{H_i}.
- Existence if G is "far from cyclic".