Norm relations and class group computations

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

25 February 2022
Séminaire Afrimath

Inria Bordeaux / IMB

Computing class groups

Goal: given a number field K, compute the class group Cl_K.

Buchmann's algorithm:

1. Choose S set of primes generating Cl_K (GRH).
2. Find S-units $R \subset \mathbb{Z}_{K,S}^{\times} = \{x \in K^{\times} \mid v_{\mathfrak{p}}(x) = 0 \text{ for all } \mathfrak{p} \notin S\}$.
3. Compute $C = \mathbb{Z}^S / \langle R \rangle$ and $U = \ker(\langle R \rangle \to \mathbb{Z}^S)$.
4. Check if $\langle R \rangle = \mathbb{Z}_{K,S}^{\times}$ using class number formula.
5. Output C.

Can be used up to degree ~ 150 (painfully), maybe ~ 200.

Main problem: Step 2, how do you construct S-units?

Example of new computation

Let $K = \mathbb{Q}(\zeta_m)$ with $m = 6552 = 2^3 \cdot 3^2 \cdot 7 \cdot 13$.

We have

- $[K : \mathbb{Q}] = 1728 = 2^6 \cdot 3^3$;
- $\Delta_K = 2^{3456} \cdot 3^{2592} \cdot 7^{1440} \cdot 13^{1584} \approx 10^{5258}$.

4h computation on a laptop:

- $\mathrm{Cl}_K \cong (\ldots$ too large to display $\ldots)$;
- $\dim_{\mathbb{F}_2} \mathrm{Cl}_K = 112$;
- $\dim_{\mathbb{F}_3} \mathrm{Cl}_K = 101$;
- $h_m^+ = 70695077806080 = 2^{24} \cdot 3^3 \cdot 5 \cdot 7^4 \cdot 13$.

What is special about K?

- $\mathrm{Gal}(K/\mathbb{Q}) \cong C_{12} \times C_6^2 \times C_2^2$;
- "many" subfields.

Plan

Question: How do you get information about K from its subfields?

1. Brauer relations
2. Norm relations
3. Algorithms

Brauer relations

Notations

Let G be a finite group.
Group algebra $\mathbb{Q}[G]$: set of formal sums

$$x = \sum_{g \in G} x_g g \quad x_g \in \mathbb{Q}$$

with multiplication induced from G, $\mathbb{Z}[G] = \{x \in \mathbb{Q}[G] \mid x_g \in \mathbb{Z}\}$.

$\mathbb{Z}[G]$ (resp. $\mathbb{Q}[G]$)-**module** M:
abelian group (resp. $\mathbb{Q}$-vector space) M + linear action of G.

Let $H \leq G$ be a subgroup.
Fixed points $M^H = \{m \in M \mid hm = m \text{ for all } h \in H\}$.
$\mathbb{Q}[G/H] =$ **permutation module** of G/H: $\mathbb{Q}$-basis $\{gH\}$,
G-action by permuting the cosets.

Example

Let $G = C_4 = \langle \sigma \rangle$.

We have

$$\mathbb{Q}[G] = \mathbb{Q} \oplus \mathbb{Q}\sigma \oplus \mathbb{Q}\sigma^2 \oplus \mathbb{Q}\sigma^3.$$

Multiplication:

$$(1 + \sigma^2)(2 - \sigma^3) = 2 + 2\sigma^2 - \sigma^3 - \sigma^5 = 2 - \sigma + 2\sigma^2 - \sigma^3.$$

Let $H = \langle \sigma^2 \rangle$. We have

$$\mathbb{Q}[G/H] = \mathbb{Q}H \oplus \mathbb{Q}\sigma H.$$

Multiplication by σ: $H \mapsto \sigma H$ and $\sigma H \mapsto \sigma^2 H = H$, therefore represented by the matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Brauer relations

Definition

A formal sum

$$\Theta = \sum_i a_i H_i \quad a_i \in \mathbb{Z}$$

is a **Brauer relation** if

$$\bigoplus_{a_i>0} \mathbb{Q}[G/H_i]^{a_i} \cong \bigoplus_{a_i<0} \mathbb{Q}[G/H_i]^{-a_i}.$$

("$\bigoplus_i \mathbb{Q}[G/H_i]^{a_i} \cong 0$")

Brauer relations: example

Let $G = C_2 \times C_2 = \langle \sigma, \tau \rangle$.

- Let $\chi \colon G \to \{\pm 1\}$ be nontrivial. We have $C = \ker \chi \cong C_2$ and $\mathbb{Q}[G/C] \cong \mathbf{1} \oplus \chi$;
- $\mathbb{Q}[G/G] \cong \mathbf{1}$;
- $\mathbb{Q}[G/1] \cong \bigoplus_\chi \chi \cong \mathbf{1} \oplus \bigoplus_{\chi \neq \mathbf{1}} \chi$;

We get

$$\bigoplus_{\chi \neq 1} \mathbb{Q}[G/\ker \chi] \cong \mathbb{Q}[G/1] \oplus \mathbb{Q}[G/G]^2.$$

Therefore

$$\Theta = 2G + 1 - \langle \sigma \rangle - \langle \tau \rangle - \langle \sigma\tau \rangle$$

is a Brauer relation.

Zeta function relations

Theorem (Brauer, Kuroda)

$\Theta = \sum_i a_i H_i$ *Brauer relation for* $G = \mathrm{Gal}(K/F)$. *Then*

$$\prod_i \zeta_{K^{H_i}}(s)^{a_i} = 1.$$

Proof.

Artin L-functions satisfy

- $L(\bigoplus_i M_i, s) = \prod_i L(M_i, s)$, and
- $L(\mathbb{Q}[G/H], s) = \zeta_{K^H}(s)$.

Class number and regulator relations

Corollary

$\Theta = \sum_i a_i H_i$ *Brauer relation for* $G = \mathrm{Gal}(K/F)$. *Then*

$$\prod_i \left(\frac{h_{K^{H_i}} \mathrm{Reg}_{K^{H_i}}}{w_{K^{H_i}}} \right)^{a_i} = 1.$$

Proof.

Analytic class number formula. □

Question: Can you separate h, Reg, w?
No in general.

Class group relations

However,

Theorem (Boltje)

$\Theta = \sum_i a_i H_i$ Brauer relation for $G = \mathrm{Gal}(K/F)$, and let p be a prime not dividing $|G|$. Then

$$\bigoplus_{a_i>0} (\mathrm{Cl}_{K^{H_i}} \otimes \mathbb{Z}_p)^{a_i} \cong \bigoplus_{a_i<0} (\mathrm{Cl}_{K^{H_i}} \otimes \mathbb{Z}_p)^{-a_i}.$$

Question: What do you do for p dividing $|G|$?

Norm relations

Motivation

Notation: For $H \leq G$ a subgroup, write $N_H = \sum_{h \in H} h \in \mathbb{Z}[G]$.

Bauch – Bernstein – de Valence – Lange – van Vredendaal, Biasse – van Vredendaal : fast algorithm for **multiquadratic fields** $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_k})$.

These works feature the following relation due to Wada:
Let $G = C_2 \times C_2 = \langle \sigma, \tau \rangle$.
We have

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

Norm relations

Definition

A **norm relation** is an equality of the form

$$\mathcal{R}\colon 1 = \sum_{i=1}^{k} a_i N_{H_i} b_i \quad a_i, b_i \in \mathbb{Q}[G],\ 1 \neq H_i \subset G.$$

We can also write it as

$$\mathcal{R}\colon d = \sum_{i=1}^{k} a_i' N_{H_i} b_i' \quad d \in \mathbb{Z}_{>0},\ a_i', b_i' \in \mathbb{Z}[G]$$

with d minimal, called the **denominator** of $\mathcal{R}$.

Norm relation example

Example

Let $G = C_p \times C_p$ with p prime.

$$p = \sum_{C_p \cong C \leq G} N_C - N_G.$$

Example

Let $G = C_p \rtimes C_q$ nonabelian with $q \mid p - 1$ primes.

$$p = N_{C_p} + \sum_{C_q \cong C \leq G} N_C - N_G.$$

Consequence of a norm relation

Proposition

Let M be a $\mathbb{Z}[G]$-module and $\mathcal{R}$: $d = \sum_i a_i N_{H_i} b_i$ a norm relation. Then $M/\sum_i a_i M^{H_i}$ has exponent dividing d.

Proof.

Let $x \in M$. Then $dx = \sum_i a_i \underbrace{N_{H_i} b_i x}_{\in M^{H_i}}$. □

Corollary

$G = \mathrm{Gal}(K/F)$, S a G-stable set of primes, $M = \mathbb{Z}_{K,S}^{\times}$.
Let N be the $\mathbb{Z}[G]$-submodule of M generated by the $\mathbb{Z}_{K^{H_i},S}^{\times}$.
Then M/N has exponent dividing d.

Existence of a norm relation

Question: When do such relations exist?

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

G admits a norm relation iff G contains

- *a noncyclic subgroup of order pq (p, q primes), or*
- *a subgroup isomorphic to* $\mathrm{SL}_2(\mathbb{F}_p)$ *for* $p = 2^{2^k} + 1 > 5$ *a Fermat prime.*

Algorithms

Saturation

Setup: $G = \mathrm{Gal}(K/F)$, G-stable S, norm relation $\mathcal{R}$ of denominator d. Assume we know the $\mathbb{Z}[G]$-submodule U of $\mathbb{Z}_{K,S}^{\times}$ generated by $\mathbb{Z}_{K^{H_i},S}^{\times}$.

Problem: Compute $\mathbb{Z}_{K,S}^{\times}$.

Easy case: if $d = 1$, $U = \mathbb{Z}_{K,S}^{\times}$ already!

Example

$G = C_6 \times C_6$.

- $\mathcal{R}_2 : 2 = \ldots$ coming from $C_2 \times C_2 \subset G$;
- $\mathcal{R}_3 : 3 = \ldots$ coming from $C_3 \times C_3 \subset G$.

$\Longrightarrow \mathcal{R}_3 - \mathcal{R}_2 : 1 = \ldots$ relation with denominator 1!

Saturation algorithm

General case: $d > 1$. We want to compute

$$V = \{x \in K^\times \mid x^d \in U\}.$$

Do not try every element of U/U^d and compute d-th roots!
Use several primes $\mathfrak{p}$ with $N\mathfrak{p} = 1 \bmod d$, the maps

$$U \to \mathbb{F}_\mathfrak{p}^\times \to (\mathbb{F}_\mathfrak{p}^\times)/(\mathbb{F}_\mathfrak{p}^\times)^d \cong \mathbb{Z}/d\mathbb{Z}$$

and linear algebra.

Problem (Grunwald – Wang): can fail to detect d-th powers.

$16 \in \mathbb{Q}^\times$ is an 8-th power modulo all p but is not an 8-th power.

But it "almost" works, and we prove a **bound under GRH** on the set of $\mathfrak{p}$.

Denominator bound

Question: Can the denominator d be too large?

Theorem (Biasse–Fieker–Hofmann–P.)

Let G be a finite group, and let $\mathcal{R}$ be a norm relation for G. Then there exists a norm relation with respect to the same set of subgroups, and such that the denominator divides $|G|^3$.

Main result

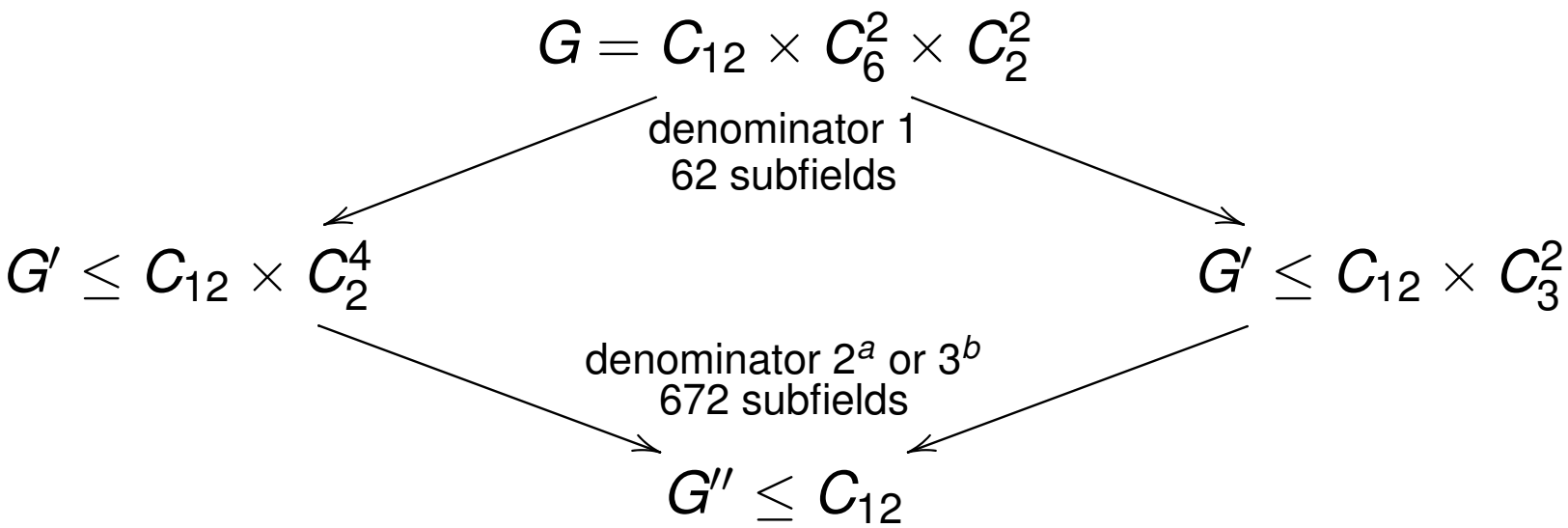
Putting everything together:

Theorem (Biasse–Fieker–Hofmann–P.)

Let $G = \mathrm{Gal}(K/F)$ admitting a norm relation, and let S be a G-stable set of primes.
Under GRH, the computation of $\mathbb{Z}_{K,S}^{\times}$ reduces in polynomial time to that of the $\mathbb{Z}_{K^{H_i},S}^{\times}$.

Initial example

$K = \mathbb{Q}(\zeta_{6552})$.



Implementations

- Implementation in Julia (Nemo/Hecke): general case.
- Implementation in GP (Pari/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.
  Code: `https://hal.inria.fr/hal-02961482`

Questions ?

Thank you!

https://arxiv.org/abs/2002.12332