Norm relations and class group computations

jw/ J.F. Biasse
C. Fieker
T. Hofmann.

Goal: faster class group computations in some number fields.

Example

$K = \mathbb{Q}(J_m)$ $\quad m = 6552 = 2^3 \cdot 3^2 \cdot 7 \cdot 13$

$\mathrm{disc}(K) = 2^{3456} \cdot 3^{2592} \cdot 7^{1440} \cdot 13^{1584} \approx 10^{5258}$

$Cl_K \cong \dots$ $\quad 12(\log|\Delta_K|)^2 \approx 1.8 \cdot 10^9$ $\sim 84 \cdot 10^6$ primes?

4h. laptop

$\dim_{\mathbb{F}_2}(Cl_K/2Cl_K) = 112$

$\dim_{\mathbb{F}_3}(Cl_K/3Cl_K) = 101$

$h_m^+ = 706350778060 80 = 2^{24} \cdot 3^3 \cdot 5 \cdot 7^4 \cdot 13$

Buchmann's algorithm:

S set of prime ideals that generate Cl_K

GRH $\Rightarrow \{\mathfrak{p} \mid N\mathfrak{p} \leq 12(\log|\Delta_K|)^2\}$ ok.

By searching at random (or storing...), find elements

$x \in \mathbb{Z}_{K,S}^\times = \{x \in K^\times \mid v_\mathfrak{p}(x) = 0 \ \forall \mathfrak{p} \notin S\}$

S-units

$$Cl_K \cong \mathbb{Z}^S / N_S(\mathbb{Z}_{K,S}^\times)$$

stop using analytic class number formula.

What is special about K?

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

How do you get information about K from its subfields?

I) Brauer relations

- G finite group.
  R ring (commutative)
  $R[G]$ group ring = formal sums $x = \sum_{g \in G} x_g g$ $x_g \in R$.
  $R[G]$-module M = finitely generated R-module M + R-linear action of G.
  $M^H = \{x \in M \mid hx = x \ \forall h \in H\}$ fixed points.
  $H \leq G$ ← subgroup
  $R[G/H]$ = permutation module of G/H
  R-basis $\{gH\}$, G-action by permutation of cosets.

Def A formal sum
$$\Theta = \sum_{i=1}^{k} a_i H_i \qquad a_i \in \mathbb{Z}$$
is a Brauer relation over R ($R = \mathbb{Q} \Leftrightarrow R = \mathbb{C}$ if ~~not stated~~ omitted) if
"$\bigoplus_{i=1}^{k} R[G/H_i]^{\oplus a_i} \cong 0$"
$$\bigoplus_{a_i \geq 0} R[G/H_i]^{\oplus a_i} \cong \bigoplus_{a_i < 0} R[G/H_i]^{-a_i}$$

Ex: $G = C_2 \times C_2 = \langle \sigma, \tau \rangle$ ← trivial module
$\chi : G \to \{\pm 1\}$ $\quad \mathbb{Q}[G/\ker\chi] \cong 1 \oplus \chi$
$C = \ker\chi$
$\mathbb{Q}[G/1] \cong 1 \oplus \bigoplus_{\chi} \chi \qquad \mathbb{Q}[G/G] = 1$
$\bigoplus_{\chi} \mathbb{Q}[G/\ker\chi] \cong \mathbb{Q}[G/1] \oplus \mathbb{Q}[G/G]^2$
$\Theta = 2G + 1 - \langle\sigma\rangle - \langle\tau\rangle - \langle\sigma\tau\rangle$

Ex: $G = S_3$ (may skip)
$\mathbb{Q}[G/C_3] \cong 1 \oplus \mathrm{sgn}$
$\mathbb{Q}[G/C_2] \cong 1 \oplus \mathrm{std}$
$\mathbb{Q}[G/1] \cong 1 \oplus \mathrm{sgn} \oplus \mathrm{std}^2$
$\Theta = 2G + 1 - C_3 - 2C_2$

Thm (Brauer–Kuroda) If K/F Galois group G,

If $\oplus$ is a Brauer relation, then

$$\prod_{i=1}^{k} J_{K^{H_i}}(s)^{a_i} = 1$$

$$\oplus = \sum_{i=1}^{k} a_i H_i$$

Proof Artin L-function

$$L(\mathbb{Q}[G/H], s) = J_{K^H}(s)$$

$$L\Big(\bigoplus_{i=1}^{k} \mathbb{Q}[G/H_i]^{a_i}\Big) = \prod_{i=1}^{k} L(\mathbb{Q}[G/H_i], s)$$

□

Cor

$$\prod_{i=1}^{k} \left(\frac{h_{K^{H_i}} \operatorname{Reg}_{K^{H_i}}}{w_{K^{H_i}}} \right)^{a_i} = 1$$

Proof Analytic class number formula. □

Call a Brauer relation **useful** if coefficient of $H=1$ is $\neq 0$.

Thm (Funakura)

G admits a useful Brauer relation iff G contains a non-cyclic subgroup of order pq, where p, q are primes (distinct or not).

Q: Can you separate h, Reg, w?

$$\prod_{i=1}^{k} h_{K^{H_i}}^{a_i} = 1, \quad \prod_{i=1}^{k} \operatorname{Reg}_{K^{H_i}}^{a_i} = 1, \quad \prod_{i=1}^{k} w_{K^{H_i}}^{a_i} = 1 \; ?$$ **NO** in general.

But

Thm (Boltje) If $\oplus = \sum a_i H_i$ is a Brauer relation over $\mathbb{Z}_p$ ($\Leftrightarrow \mathbb{F}_p$, $\Rightarrow \mathbb{Q}$, $\Leftarrow \mathbb{Z}_{(p)}$), $p \nmid |G|$, then

$$\bigoplus_{a_i \geq 0} \mathcal{C}l_{K^{H_i}}^{a_i} \otimes \mathbb{Z}_p \cong \bigoplus_{a_i < 0} \mathcal{C}l_{K^{H_i}}^{-a_i}$$

What do you do for $p \mid |G|$?

II) Norm relations

Bauch – Bernstein – de Valence – Lange – van Vredendaal
Biasse – van Vredendaal
} fast algorithm for multiquadratic fields

$H \leq G$

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

ex: $G = C_2 \times C_2 = \langle \sigma, \tau \rangle$

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

$= (1+\sigma) + (1+\tau) - \sigma(1+\sigma\tau)$

uses

Def A norm relation is an equality of the form

$\mathcal{R}: 1 = \sum_{i=1}^{k} a_i N_{H_i} b_i \qquad a_i, b_i \in \mathbb{Q}[G] \qquad H_i \leq G$

May write as

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

d denominator of $\mathcal{R}$.

ex: p prime, $G = C_p \times C_p$

$p = \sum_{\substack{C \leq G \\ |C| = p}} N_C - N_G$

ex: p prime, $q \mid p-1$, $G = C_p \times C_q$ nontrivial

$p = N_{C_p} + \sum_{\substack{C \leq G \\ |C| = q}} N_C - N_G$

Prop Let M be a $\mathbb{Z}[G]$-module. If $\mathcal{R}: d = \sum a_i N_{H_i} b_i$ is a norm relation then $M / \sum_{i=1}^{k} a_i M^{H_i}$ has exponent dividing d.

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

Corollary. If K/F has Galois group G, then and S is G-stable, then in $M = \mathcal{O}_{K,S}^\times$, the ~~subgroup~~ $\mathbb{Z}[G]$-submodule N generated by the $\mathcal{O}_{K^{H_i},S}^\times$ satisfies M/N has exponent dividing d.

partial converse:

Prop. K/F Galois group G, S G-stable.

(may skip)

Assume S contains a totally split prime.

If the $\mathbb{Z}[G]$-submodule of $\mathcal{O}_{K,S}^\times$ generated by the $\mathcal{O}_{K^{H_i},S}^\times$ has finite index, then $\exists$ norm relation.

Prop $\mathcal{H}$ set of nontrivial subgroups of G. TFAE

(may skip)

(i) $\exists$ norm relation with all $H_i \in \mathcal{H}$

(ii) $\forall$ simple $\mathbb{Q}[G]$-module M, $\exists H \in \mathcal{H}$ s.t. $M^H \neq 0$

(iii) $\exists \bigoplus_{i=1}^{k} \mathbb{Q}[G/H_i]^{a_i} \twoheadrightarrow \mathbb{Q}[G]$ surjection of $\mathbb{Q}[G]$-modules.

Thm ($\approx$ Wolf)

G admits a norm relation iff G contains a non-cyclic subgroup of order pq (p,q primes) or isomorphic to $SL_2(\mathbb{F}_p)$, $p \nmid 5$ Fermat prime.

Prop K/F Galois G, $\mathcal{R}$ relation denominator d.

(may skip)

$Cl_K \otimes \mathbb{Z}[\frac{1}{d}]$ is a direct summand of $\bigoplus_{i=1}^{k} Cl_{K^{H_i}} \otimes \mathbb{Z}[\frac{1}{d}]$

$Cl_K / Cl_K[d]$ is isomorphic to a subgroup of $\bigoplus_{i=1}^{k} Cl_{K^{H_i}}$.

III) Algorithms

K/F Galois group G, S G-stable, $\mathcal{R}$ relation denominator d.
Assume we know $U = \mathbb{Z}[G]$-submodule of $\mathbb{Z}_{K,S}^\times$ gene by $\mathbb{Z}_{K^{Hi},S}^\times$.

▶ if $d = 1$, nothing to do!

ex: $G = C_6 \times C_6$.

$\mathcal{R}_2 : 2 = \dots$ coming from $C_2 \times C_2 \leq G$
$\mathcal{R}_3 : 3 = \dots$ coming from $C_3 \times C_3 \leq G$
$\Rightarrow \mathcal{R}_3 - \mathcal{R}_2 : 1 = \dots$ denominator 1!

▶ $d \neq 1$:
Compute $V = \{x \in K^\times \mid x^d \in U\}$ (situation)?
DO NOT try every element of U/dU and compute d-th root.
Use $U \longrightarrow \mathbb{F}_\mathfrak{p}^\times \longrightarrow \mathbb{F}_\mathfrak{p}^\times/(\mathbb{F}_\mathfrak{p}^\times)^d \cong \mathbb{Z}/d\mathbb{Z}$ ($\mathfrak{p}$ residue degree 1, $N\mathfrak{p} \equiv 1 \bmod d$)
Problem (Gramwald-Wang): does not detect d-th powers
$16 \in \mathbb{Q}^\times$ 8-th power mod all $\mathfrak{p}$ but not 8-th power.
$X^8 - 16 = (X^2-2)(X^2+2)(X^2-2X+2)(X^2+2X+2)$
But almost works (if d is a prime power and $K(\mu_d)/K$ is cyclic)
GRH-bound on set of $\mathfrak{p}$: $C_0 = 18\, d^2 (2\log|\Delta_K| + 6n\log d + \log M_S)^2$

▶ d too large?

Thm. $\mathcal{H}$ set of subgroups of G. If $\exists$ relation wrt $\mathcal{H}$, then $\exists$ relation with denominator dividing $|G|^3$.

Thm Under GRH, $\exists$ poly time reduction from computation of $\mathbb{Z}_{K,S}^\times$ to that of $\mathbb{Z}_{K^{Hi},S}^\times$.

Ex: $K = \mathbb{Q}(\mathrm{J}_{6552})$