Computing class groups

Fabrice ETIENNE

University of Bordeaux, IMB

2024

Sommaire

Introduction

Definition : class group of a number field

Let K be a number field. Denote by $I(K)$ the collection of all fractional ideals of K, and by $P(K)$ the collection of all principal ideals of K. Then, $P(K)$ is a subgroup of $I(K)$, and the class group $C(K)$ is the quotient $C(K) = \frac{I(K)}{P(K)}$

Introduction

Buchmann algorithm

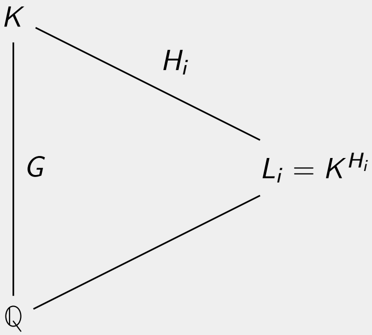
Given a number field K of degree n over $\mathbb{Q}$ and of discriminant $D(K)$, there is an algorithm to compute its class group (under the Riemann Hypothesis), in time

$$\mathcal{O}(e^{a\sqrt{ln|D(K)|lnln|D(K)|}})$$

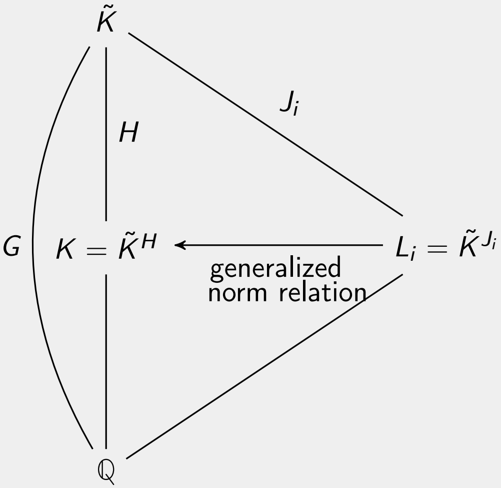
where a is small and the $\mathcal{O}$ constant depends on n.

Introduction

If $K/\mathbb{Q}$ is a Galois extension of Galois group G, and if G admits a norm relation with respect to some subgroups H_i, then we use Buchmann algorithm on the $L_i = K^{H_i}$, and we use the norm relation to find the class group of K.



Introduction



We use Buchmann algorithm here

Reference

<u>Reference :</u>

Jean-François Biasse, Claus Fieker, Tommy Hofmann and Aurel Page.
"Norm relations and computational problems in number fields".
In : Journal of the London Mathematical Society (2022).

Definitions

Let G be a finite group.

Definition : norm element

If H is a subgroup of G, we call **norm element** of H the element $N_H = \sum_{h \in H} h \in \mathbb{Z}[G]$.

Definition : norm relation

Let $\mathcal{H}$ be a set of subgroups of G, and R a commutative ring. A **norm relation** over R with respect to $\mathcal{H}$ is a relation in $R[G]$ of the form

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

$a_i, b_i \in R[G]$
$H_i \in \mathcal{H}, H_i \neq \{0\}$

Properties of norm relation

Let K/F be a Galois extension of number fields, of Galois group G.
We will consider relations of the form

$$(*) : d = \sum_{i=1}^{l} a_i N_{H_i} b_i$$

with $d \in \mathbb{N}^*, a_i, b_i \in \mathbb{Z}[G], H_i < G$.

Définition

The exponent of a $\mathbb{Z}$-module M is the smallest $e \in \mathbb{N}^*$ such that $\forall x \in M, e \cdot x = 0$

Properties of norm relation

Proposition

Let M be a $\mathbb{Z}[G]$-module. If G has a relation of the form $(*)$, then the exponent of the quotient $M/(\sum_{i=1}^{l} a_i M^{H_i})$ is finite and divides d.

Corollary

If G has a relation of the form $(*)$, then the exponent of the quotient
$\mathcal{O}_{K,S}^{\times}/(\mathcal{O}_{K^{H_1},S}^{\times})^{a_1}\cdots(\mathcal{O}_{K^{H_\ell},S}^{\times})^{a_\ell}$ is finite and divides d.

Definitions

Definition : Generalized norm relation

Let G be a finite group, H a subgroup of G, $\mathcal{J}$ a set a subgroups of G and R a commutative ring. A **generalized norm relation over** R **with respect to** H **and** $\mathcal{J}$ is an equality in $R[G]$ of the form

$$N_H = \sum_{i=1}^{l} a_i N_{J_i} b_i$$

where $a_i, b_i \in R[G]$, $H_i \in \mathcal{H}$, and $H_i \neq 1$.

Definitions

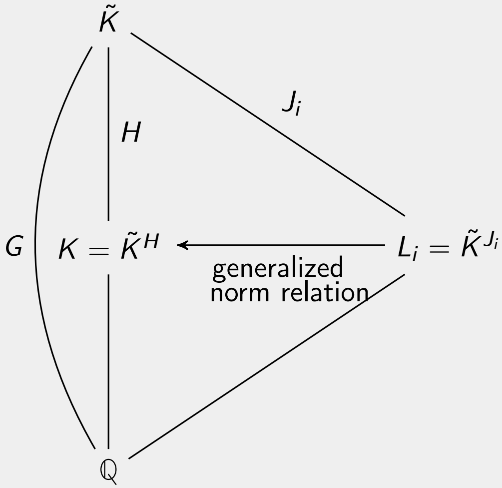
Definition :

If K is a number field, and $L_1, \cdots, L_\ell$ some other number fields. Let Ω a Galois extension of $\mathbb{Q}$ containing K and all the L_i, and let $\mathcal{G}$ its Galois group. We denote by $\mathcal{H}$ the subgroup of $\mathcal{G}$ fixing K, and by $\mathcal{Y}_i$ the ones fixing the L_i respectively. Then we say there is a generalized norm relation between K and the L_i if $\mathcal{G}$ admits a generalised norm relation over $\mathbb{Q}$ with respect to $\mathcal{H}$ and the $\mathcal{Y}_i$.

Properties of norm relations

$$\begin{tikzcd}
 & \Omega \arrow[dl, "\mathcal{N}"'] \arrow[dr, bend left, "\mathcal{Y}_i"] \arrow[ddl, bend left, "\mathcal{H}"] \arrow[dddl, bend left, "\mathcal{G}"] & \\
\tilde{K} \arrow[d, "H"'] \arrow[dd, bend right, "G"'] & & L_i \arrow[ddll, bend left] \\
K \arrow[d] & & \\
\mathbb{Q} & &
\end{tikzcd}$$

Computing class groups with generalized norm relations



We use Buchmann algorithm here

Computing class groups with generalized norm relations

Theorem :

Suppose there is a relation of the form $dN_H = \sum_i a_i N_{J_i} b_i$, with $d \in \mathbb{N}^*$ et $a_i, b_i \in \mathbb{Z}[G]$. Let M be a $\mathbb{Z}[G]$-module. Then the exponent of the quotient $M^H/(N_H \cdot (\sum_i a_i M^{J_i}))$ is finite and divides $|H|^2 d$.

Corollary :

Denote $\alpha_i = N_H(a_i)$ for all i. Then the exponent of the quotient $\mathcal{O}^\times_{K^H,S}/((\mathcal{O}^\times_{K^{J_1},S})^{\alpha_1} \cdots (\mathcal{O}^\times_{K^{J_\ell},S})^{\alpha_l})$.

Compositum

Let L, M be number fields

Definition : Compositum

A **compositum** of L and M is a triple (C, ι_L, ι_M) where C is a number field, $\iota_L : L \to C$ and $\iota_M : M \to C$ are morphisms of $\mathbb{Q}$-algebras, and C is generated by $\iota_L(L)$ and $\iota_M(M)$.

Theorem

There is an injective morphism
$\Phi : \mathbb{Z}[\mathrm{Compos}(K, L)] \to \mathrm{Hom}_{R[G]}(R[\mathrm{Hom}(L, \mathbb{C})], R[\mathrm{Hom}(K, \mathbb{C})])$.

A characterization with compositums

Proposition

If $L_1, \cdots, L_\ell$ are number fields, and $\beta_1, \cdots, \beta_\ell$ such that $L_i = \mathbb{Q}(\beta_i)$, then $K = \mathbb{Q}(\alpha)$ admits a generalized norm relation with respect to $L_1, \cdots, L_\ell$, if and only if there is a relation of the form

$$\alpha = \sum_{i=1}^{\ell} \sum_{C \in \mathrm{Compos}(K, L_i)} a_{i,C} C \cdot \beta_i$$

Looking for generalized norm relations

Algorithm

input : A number field $K = \tilde{K}^H$ and a family $L_i = \tilde{K}^{J_i}$ of number fields.

output : True if and only if there is a generalized norm relation, and if so, the coefficients of the relation.

- For all i, list all compositums of K and L_i.
- For all i, and for all $\sigma \in \mathrm{Hom}(L_i, \mathbb{C})$ and for all compositum C,compute $C \cdot \sigma \in \mathbb{Q}[\mathrm{Hom}(K, \mathbb{C})]$.
- We are left with a linear algebra problem of polynomial dimension.

Computing the class group

Step 1 :

Compute the class group of every subfield $K_j = \tilde{K}^{J_j}$, using **bnfinit** and **bnfunits**.

Step 2 :

Compute all compositums of K and K_j for all j.

Computing the class group

Step 3 :

For each K_j, compute S_j a set of prime ideals that generates the coprime to d-part of the class group.

Step 4 :

Compute the matrix of an application $\Phi : \sum K_j^{n_j} \to K$, that sends all the ideals above all the primes in S_j to their image by every compositum.

Step 5 :

Compute all the valuations of the S_j-units of all the K_j in every prime ideal in S_j. Then apply the matrix of the application Φ and take the Smith Normal Form.

Exemple

Theorem

If $p > 2$ is a prime number, let $G = GL_2(\mathbb{F}_p)$, $H \simeq C_p < G$, then G admits a generalized norm relation over $\mathbb{Q}$ with respect to H and a set of subgroups $\{J_1, \cdots, J_\ell\}$ whose index in G are smaller or equal to $p^2 - 1$.

Any questions ?

Thank you !