Computing Logarithmic Class Groups

José Ibrahim Villanueva Gutiérrez

Atelier PARI/GP 2017

11th January 2017

université de BORDEAUX

CONACYT
Consejo Nacional de Ciencia y Tecnología

Introduction

- This talk is about the algorithms to compute
  - Logarithmic class group: `bnflog`
  - Logarithmic ramification index and logarithmic inertia degree: `bnflogef`
- For each of these topics we will
  - Briefly recall the definitions and the context
  - Summarize the progress made in previous computational work
  - Highlight the main steps towards the new algorithm made by **Karim Belabas** and **Jean-François Jaulent**.
- During the talk, I will present some examples of
  - already implemented stuff
  - future work.

The class group and the group of units

- Let K be a number field, and fix ℓ a prime number.
- Let $(v_{\mathfrak{p}})_{\mathfrak{p}}$ be the family of classic valuations.
- A principal fractional ideal can be expressed as

$$(x) = \prod_{\mathfrak{p} \in \mathrm{Pl}_K^0} \mathfrak{p}^{v_{\mathfrak{p}}(x)} \quad \text{with } x \in K^\times.$$

- We have the following exact sequence

$$1 \longrightarrow E_K \longrightarrow K^\times \xrightarrow{div} I_K = \bigoplus_{\mathfrak{p} \in \mathrm{Pl}_{K^0}} \mathbb{Z}\mathfrak{p} \longrightarrow C_K \longrightarrow 1.$$

- If we tensor by $\mathbb{Z}_\ell$

$$1 \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} E_K \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times \xrightarrow{div} \bigoplus_{\mathfrak{p} \in \mathrm{Pl}_{K^0}} \mathbb{Z}_\ell \mathfrak{p} \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} C_K \longrightarrow 1.$$

Logarithmic valuations

- We define ℓ-adic logarithmic valuations as the morphisms

$$\widetilde{v}_{\mathfrak{p}} : K_{\mathfrak{p}}^{\times} \longrightarrow \mathbb{Z}_{\ell},$$

such that

$$\widetilde{v}_{\mathfrak{p}}(x) = \begin{cases} v_{\mathfrak{p}}(x) & \text{if } \mathfrak{p} \nmid \ell, \\ -\frac{\mathrm{Log}_{\ell}(N_{K_{\mathfrak{p}}/\mathbb{Q}_{\ell}}(x))}{\deg \mathfrak{p}} & \text{if } \mathfrak{p} | \ell. \end{cases}$$

- The term $\deg \mathfrak{p}$ is chosen to normalize.

Logarithmic Classes of arbitrary degree

- We replace the classical valuations $(v_{\mathfrak{p}})_{\mathfrak{p}}$ by the logarithmic valuations $(\widetilde{v}_{\mathfrak{p}})_{\mathfrak{p}}$:

$$1 \longrightarrow \widetilde{\mathcal{E}}_K \longrightarrow \mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times \xrightarrow{\widetilde{div}} \bigoplus_{\mathfrak{p} \in \mathrm{Pl}_K^0} \mathbb{Z}_\ell \mathfrak{p} \longrightarrow \widetilde{\mathcal{C}\ell}_K^* \longrightarrow 1.$$

- The image of $\mathbb{Z}_\ell \otimes_{\mathbb{Z}} K^\times$ is the subgroup $\mathcal{P}_K$ of **logarithmic principal divisors**.
- If we define the **degree** of a logarithmic divisor $\mathfrak{d} = \sum_{\mathfrak{p}} \alpha_{\mathfrak{p}} \mathfrak{p}$ additively

$$\deg\left(\sum_{\mathfrak{p}} \alpha_{\mathfrak{p}} \mathfrak{p}\right) = \sum_{\mathfrak{p}} \alpha_{\mathfrak{p}} \deg \mathfrak{p},$$

it turns out that the elements of $\mathcal{P}_K$ have degree 0.

- The **logarithmic class group of arbitrary degree**

$$\widetilde{\mathcal{C}\ell}_K^* = \bigoplus_{\mathfrak{p} \in \mathrm{Pl}_{K0}} \mathbb{Z}_\ell \mathfrak{p} / \mathcal{P}_K$$

has as subgroup the **logarithmic class group**

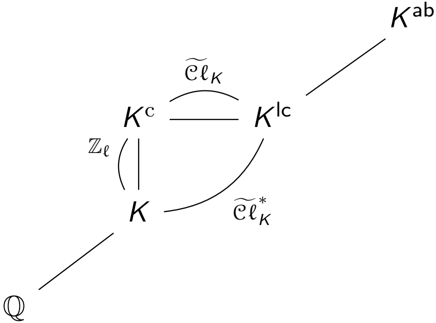
$$\widetilde{\mathcal{C}\ell}_K,$$

formed by the classes of degree 0.

Galois interpretation

- Every number field has an infinite Galois extension K^{c} such that $\mathrm{Gal}(K^{\mathrm{c}}/K) \simeq \mathbb{Z}_\ell$, the $\mathbb{Z}_\ell$-**cyclotomic extension** of K.
- Indeed $K^{\mathrm{c}} = K\mathbb{Q}^{\mathrm{c}}$.
- The maximal abelian ℓ-extension over K that splits completely over K^{c} is called the **locally ℓ-cyclotomic extension** and denoted K^{lc}.
- Gross-Kuz'min Conjecture:
  The Galois group $\mathrm{Gal}(K^{\mathrm{lc}}/K)$ is a $\mathbb{Z}_\ell$-module of rank 1.
- The **logarithmic class group** is defined as

$$\widetilde{\mathcal{C}\ell}_K = \mathrm{Gal}(K^{\mathrm{lc}}/K^{\mathrm{c}}).$$


K^{ab}
$\widetilde{\mathcal{C}\ell}_K$
K^c
K^{lc}
$\mathbb{Z}_\ell$
K
$\widetilde{\mathcal{C}\ell}_K^*$
$\mathbb{Q}$

History

- F. Diaz y Diaz & F. Soriano, *Approche algorithmique du groupe des classes logarithmiques* (1999).
  - Compute for the first time the logarithmic class group assuming $K/\mathbb{Q}$ is Galois.
- F. Diaz y Diaz, J-F. Jaulent, S. Pauli, M. Pohst & F. Soriano, *A new algorithm for the computation of logarithmic ℓ-class groups of number fields* (2005).
  - Remove the Galois assumption.
  - For $\widetilde{\mathcal{C}\ell}_K$ uses the exact sequence

$$0 \to \widetilde{\mathcal{C}\ell}_K(\ell) \to \widetilde{\mathcal{C}\ell}_K \xrightarrow{\theta} C\ell' \to \operatorname{coker}\theta \to 0$$

- K. Belabas & J-F. Jaulent, *The logarithmic class group package in PARI/GP.*
  - Simplify.
  - Short exact sequence

$$0 \to \widetilde{\mathcal{C}\ell}^*_K(\ell) \to \widetilde{\mathcal{C}\ell}^*_K \xrightarrow{\theta} C\ell' \to 0$$

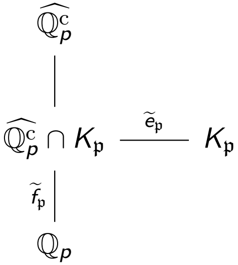
Logarithmic inertia and logarithmic ramification

- Let $\mathfrak{p} \in \mathrm{Pl}_K^0$ be a place above $p \in \mathbb{Z}$.
- Let $\widehat{\mathbb{Q}_p^c}$ be the cyclotomic $\widehat{\mathbb{Z}}$-extension of $\mathbb{Q}_p$.
- The **logarithmic inertia degree** is defined as

$$\widetilde{f}_\mathfrak{p} = [K_\mathfrak{p} \cap \widehat{\mathbb{Q}_p^c} : \mathbb{Q}_p].$$

- The **logarithmic ramification index** by

$$\widetilde{e}_\mathfrak{p} = [K_\mathfrak{p} : K_\mathfrak{p} \cap \widehat{\mathbb{Q}_p^c}].$$



Properties

- We have the following multiplicative relations:

$$n_{\mathfrak{p}} = [K_{\mathfrak{p}} : \mathbb{Q}_p] = e_{\mathfrak{p}} f_{\mathfrak{p}} = \widetilde{e}_{\mathfrak{p}} \widetilde{f}_{\mathfrak{p}}.$$

- Furthermore, $v_q(e_{\mathfrak{p}}) = v_q(\widetilde{e}_{\mathfrak{p}})$ for all $q \neq p$.
- The logarithmic ramification index $\widetilde{e}_{\mathfrak{p}}$ and $[h_{\mathfrak{p}}(K_{\mathfrak{p}}^{\times}) : \mathbb{Z}_p]$ have the same valuation at p where

$$h_{\mathfrak{p}}(\alpha) = \frac{\mathrm{Log}_p \, N_{K_{\mathfrak{p}}/\mathbb{Q}_p}(\alpha)}{2 \cdot p \cdot n_{\mathfrak{p}}}.$$

- $v_p(\widetilde{f}_{\mathfrak{p}}) \leqslant v_p(e_{\mathfrak{p}})$, so if $v_p(e_{\mathfrak{p}}) = 0$, then

$$\widetilde{e}_{\mathfrak{p}} = e_{\mathfrak{p}} p^{v_p(f_{\mathfrak{p}})} \quad \text{and} \quad \widetilde{f}_{\mathfrak{p}} = f_{\mathfrak{p}} p^{-v_p(f_{\mathfrak{p}})}.$$

Algorithm

Computing $\widetilde{e_\mathfrak{p}}$ and $\widetilde{f_\mathfrak{p}}$

- **Input** A prime ideal $\mathfrak{p}$ of K (hence maximal), $e_\mathfrak{p}$ and $f_\mathfrak{p}$.
- **Output** $\widetilde{e_\mathfrak{p}}$ and $\widetilde{f_\mathfrak{p}}$

1. If $v_p(e_\mathfrak{p}) = 0$ set $\widetilde{e_\mathfrak{p}} \leftarrow e_\mathfrak{p} p^{v_p(f_\mathfrak{p})}$ and $\widetilde{f_\mathfrak{p}} \leftarrow f_\mathfrak{p} p^{-v_p(f_\mathfrak{p})}$.
2. Set $g_0 \leftarrow \pi$. Compute generators $g_1, \ldots, g_s$ of $(1+\mathfrak{p})$ (recall $K_\mathfrak{p}^\times = \mathfrak{p}^\mathbb{Z} \times \mu_\mathfrak{p} \times (1+\mathfrak{p})$).
3. Let $v \leftarrow \min_i v_\mathfrak{p}\left(\mathrm{Log}_\mathfrak{p} N_{K_\mathfrak{p}/\mathbb{Q}_p}(g_i)\right)$.
4. Let $v \leftarrow v - v_p(2 \cdot p \cdot n_\mathfrak{p})$. Set $\widetilde{e_\mathfrak{p}} \leftarrow e_\mathfrak{p} p^{-v}$ and $\widetilde{f_\mathfrak{p}} \leftarrow f_\mathfrak{p} p^{v}$.

The additive morphism $deg(\mathfrak{p})$

- The **logarithmic degree** is defined in the following way

$$\deg \mathfrak{p} = \widetilde{f}_{\mathfrak{p}} \deg p \quad \text{where} \quad \deg p = \begin{cases} \mathrm{Log}_\ell(p) & \text{if } p \neq \ell \\ \mathrm{Log}_\ell(1+\ell) & \text{if } p = \ell \\ \mathrm{Log}_\ell(1+4) & \text{if } p = \ell = 2 \end{cases}$$

- The function `bnflog` takes as usual a number field structure, a prime number and a logarithmic divisor. It returns the $\exp(\deg \mathfrak{p})$, hence a natural number.
-
```
? bnflogdegree(bnfinit(x),3,3)
%2 = 4
```

Behind the algorithm of the logarithmic class group

- We have the following short exact sequences:

$$0 \to \widetilde{\mathcal{C}\ell}_K^*(\ell) \to \widetilde{\mathcal{C}\ell}_K^* \xrightarrow{\theta} C\ell' \to 0$$

  and

$$0 \to C\ell(\ell) \to C\ell \to C\ell' \to 0$$

- We can compute relations and generators for $C\ell'$. H. Cohen, F. Diaz y Diaz and M. Olivier; *Algorithmic Methods for Finitely Generated Abelian Groups* (2001).
- The group $\widetilde{\mathcal{C}\ell}_K^*(\ell)$ has generators given by the classes of the places $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_s\}$ above ℓ and generators derived from $\widetilde{div}(u_j) = 0$, where u_j is a generator of the S-units ($\mathbb{Z}_\ell$-module of rank $r + c + s - 1$).
- If $\widetilde{\mathcal{C}\ell}_K^*(\ell)$ is given by the ℓ-adic SNF of the matrix

$$M = (\widetilde{v}_{\mathfrak{p}_i}(u_j)),$$

  the Kuz'min-Gross conjecture holds for the prime ℓ and the field K.
- We now can describe $\widetilde{\mathcal{C}\ell}_K^*$ by generators and relations.

Examples

- Logarithmic class group for several ℓ

```
? K=bnfinit(x^2-2017,1);
? K.cyc
%1 = []
? forprime(l=2,10000000,
      if(bnflog(K,l),print(l,"Clog="bnflog(K,l)[1])))
```

- Logarithmic ramification and logarithmic inertia degree

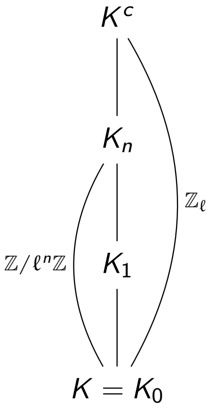
```
? T=x^6-3*x^5+5*x^3-3*x+1;
? F=nfinit(T);
? P2=idealprimedec(F,2)[1];
? [P2.e,P2.f]
%9 = [3, 2]
? bnflogef(F,P2)
%10 = [6, 1]
```

Computing $\widetilde{\mathcal{C}\ell}_K$ in the first layers of the $\mathbb{Z}_\ell$-cyclotomic extension

- Let K be a quadratic number field and $\ell = 3$.
- Compute $\widetilde{\mathcal{C}\ell}$ for the first layers of the cyclotomic $\mathbb{Z}_\ell$-extension K^c of K.
- We know that there exists $\widetilde{\mu}, \widetilde{\lambda} \in \mathbb{N}$ and $\widetilde{\nu} \in \mathbb{Z}$ such that

$$|\widetilde{\mathcal{C}\ell}_n| = \ell^{\widetilde{\mu}\ell^n + \widetilde{\lambda}n + \widetilde{\nu}}$$

  for n big enough.
- Compare these logarithmic invariants experimentally with the classical Iwasawa invariants (μ, λ, ν).



```
? d=3739; l=3; K=bnfinit(x^2-d,1);
? bnflog(K,l)
%14 = [[9], [3], [3]]
? pr=idealprimedec(K,l);
? vector(#pr,i,bnflogef(K,pr[i]))
%16 = [[1, 1], [1, 1]]
? T=polcompositum(K.pol,polsubcyclo(9,3))[1];
? K1=bnfinit(nfinit([T.pol,10^5]),1);
? bnflog(K1,l)
%19 = [[27], [3], [9]]
? pr=idealprimedec(K1,l);
? vector(#pr,i,bnflogef(K1,pr[i]))
%21 = [[1, 3], [1, 3]]
? T=polcompositum(K.pol,polsubcyclo(27,9))[1];
? K2=bnfinit(nfinit([T.pol,10^5]),1);
? bnflog(K2,3)
%24 = [[81], [3], [27]]
? pr=idealprimedec(K2,l);
? vector(#pr,i,bnflogef(K2,pr[i]))
%26 = [[1, 9], [1, 9]]
```

Future

- Recover generators of $\widetilde{\mathcal{C}\ell}_K$ to study the behaviour when we take the logarithmic extension morphism $\widetilde{i}_{L/K}$.
- Compute the structure and give generators for the logarithmic group of units $\widetilde{\mathcal{E}}_K$.
- Compute $\widetilde{\mathcal{C}\ell}_{K_n}$ for the first layers of $\mathbb{Z}_\ell$-anticyclotomic extensions.