Class Number Calculation of Special Number Fields

Takashi FUKUDA(Nihon Univ.)

2018.3.6 Séminaire de Théorie Algorithmique des Nombres

- TC (an interpreter of multiprecision C-language)
- Weber's class number problem
- Coates' conjecture
- An algorithm calculating p-class group of an abelian number field

1. TC and PARI

TC

- an interpreter of multiprecision C-language
- 'T' may be the first letter of 'Tiny' or 'Takashi'
- designed to be a platform implementing custom algorithms which are effective for special number fields
- my motto is

special algorithm for special number field

PARI

- implemented many algorithms for arbitrary number fields
- easy to use
- offers many functions which are easily called from C program
- for example, TC is compiled with PARI library

1.1. **What I have calculated using TC ?.**

2-part of the class number of abelian number fields of degree 512

- Fukuda-Komatsu, "On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$, Math. Comp. 78 (267), 1797–1808 (2009)
- Fukuda, "Greenberg conjecture for the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$, Interdiscip. Inform. Sci. 16 (1), 21–32 (2010)
- Fukuda-Komatsu, "On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$ II, Funct. Approx. Comment. Math. 51.1, 167–179 (2014)
- Fukuda-Komatsu-Ozaki-Tsuji, "On the Iwasawa λ-invariant of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}(\sqrt{p})$ III, Funct. Approx. Comment. Math. 54.1, 7–17 (2016)

3-part of the class number of non-abelian number fields of degree 486

- Fukuda-Komatsu, "Non-cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields", Experimental Math. 11 (4), 469–475 (2002)
- Fukuda-Komatsu, "Class number calculation using Siegel functions", LMS J. Comput. Math. 17, 295–302 (2014)

Examples.

$\mathbb{B}_n = \mathbb{Q}(\zeta_{2^{n+2}}) \cap \mathbb{R} : G(\mathbb{B}_n/\mathbb{Q}) \cong \mathbb{Z}/2^n\mathbb{Z}$

$k = \mathbb{Q}(\sqrt{m}) \ \ (m > 0), \ \ k_n = k\mathbb{B}_n : G(k_n/\mathbb{Q}) \cong Z/2\mathbb{Z} \times Z/2^n\mathbb{Z}$

$$2^{e_n} \mid\mid h(k_n)$$

Theorem 1 (Iwasawa)**.** $\exists\, \lambda,\ \mu,\ \nu \in \mathbb{Z}\ (\lambda, \mu \geq 0)$ *s.t.*

$$e_n = \mu\, 2^n + \lambda n + \nu \quad (n >> 0)$$

Conjecture 1.1 (Greenberg)**.** $\lambda = \mu = 0$

Criterion 1. $\exists\, n \geq 0$ *s.t.* $e_n = e_{n+1} \Longrightarrow e_n = e_m$ *for all* $m \geq n$

1.2. **How to compute e_n.**

E_n : the unit group of k_n

C_n : the cyclotomic unit group of k_n

$$C_n = \langle -1, \eta_1, \eta_2, \cdots, \eta_r \rangle, \quad r = 2^{n+1} - 1$$

Theorem 2 (Sinnott)**.** $(E_n : C_n) = 2^{e_n} \cdot 2^r \cdot q,\ q$ *: odd*

We try to find $e_i = 0, 1$ $(1 \leq i \leq r)$ s.t.

$$\sqrt{\eta_1^{e_1} \eta_2^{e_2} \cdots \eta_r^{e_r}} \in k_n .$$

Owing to a nice algorithm of Phost-Zassenhaus, this is done in $O(r^2)$-times not in $O(2^r)$-times.

Table of e_n

m	0	1	2	3	4	5	6	7	8
1201	0	2	3	4	5	6	7	8	9
3217	0	1	2	3	4	5	6	7	8
4481	0	2	4	6	7	8	9	10	11
12161	0	1	2	3	4	5	6	7	8
13841	0	2	4	5	6	7	8	9	10
15809	0	2	3	4	5	6	7	8	9
32639	2	4	8	16	32	34	34	*	*
50059	2	3	6	8	10	11	11	*	*
58323	4	7	8	9	10	11	12	12	*

- For this calculation, I used `factor()` of PARI library to factor a polynomial of degree 1024 with integer coefficients of 10000 digits.
- `factor()` is very excellent and factors those polynomals within a hour.

2. Weber's class number problem

$\mathbb{B}_n = \mathbb{Q}(\zeta_{2^{n+2}}) \cap \mathbb{R} : G(\mathbb{B}_n/\mathbb{Q}) \cong \mathbb{Z}/2^n\mathbb{Z}$

Theorem 3 (Weber, 1886)**.** *$h(\mathbb{B}_n)$ is odd for all $n \geq 0$*

Weber was interested in $h(\mathbb{B}_n)$. Note that $h(\mathbb{B}_n) \mid h(\mathbb{B}_{n+1})$.

<u>Weber 1896</u> $h(\mathbb{B}_3) = 1$

<u>Cohn 1960, Bauer 1969, Masley 1978</u> $h(\mathbb{B}_4) = 1$

<u>van der Linden 1982</u> $h(\mathbb{B}_5) = 1$

<u>Miller 2014</u> $h(\mathbb{B}_6) = 1$

Conjecture 2.1. *$h(\mathbb{B}_n) = 1$ for all $n \geq 1$.*

The whole class number $h(\mathbb{B}_n)$ is difficult to compute. So we are interested in an odd prime part of $h(\mathbb{B}_n)$. Put $h_n = h(\mathbb{B}_n)$.

Theorem 4 (Horie 2002,2005,2007)**.**
ℓ : a prime number with $\ell \equiv 3, 5 \pmod 8 \Longrightarrow \ell \nmid h_n$ for all $n \geq 1$.

Theorem 5 (Horie, Fukuda, Komatsu)**.**
ℓ : a prime number with $\ell \not\equiv \pm 1 \pmod{32} \Longrightarrow \ell \nmid h_n$ for all $n \geq 1$.

Theorem 6 (Fukuda-Komatsu 2009)**.** *Let ℓ be an odd prime number and define $c \in \mathbb{Z}$ by*

$$\begin{cases} 2^c \,||\, \ell - 1 & \text{if } \ell \equiv 1 \pmod 4, \\ 2^c \,||\, \ell^2 - 1 & \text{if } \ell \equiv 3 \pmod 4. \end{cases}$$

Put

$$m_\ell = 2c + \left[\frac{1}{2}\log_2(\ell - 1)\right] - 1\,.$$

If $\ell \nmid h_{m_\ell}$, then $\ell \nmid h_n$ for all $n \geq 1$.

ℓ	31	257	8191	65537	738197503
c	6	8	14	16	27
m_ℓ	13	19	33	39	67

Example 2.1. If we verify $738197503 \not| h_{67}$, we can assert that $738197503 \not| h_n$ $(n \geq 1)$.

Corollary 7. $\ell < 10^9 \Longrightarrow \ell \not| h_n$ $(n \geq 1)$.

2.1. How to verify $\ell \not| h_{m_\ell}$.

$\Delta_n = G(\mathbb{B}_n/\mathbb{Q}) \cong \mathbb{Z}/2^n\mathbb{Z}$
A_n : ℓ-part of the ideal class group of $\mathbb{B}_n$
$\chi : \Delta_n \longrightarrow \overline{\mathbb{Q}_\ell}$: character

$$e_\chi = \frac{1}{|\Delta_n|}\sum_{\sigma\in\Delta_n}\mathrm{Tr}(\chi(\sigma^{-1}))\sigma \in \mathbb{Z}_\ell[\Delta_n]$$

$$A_n = \bigoplus_\chi A_{n,\chi}, \quad A_{n,\chi} = A_n^{e_\chi}$$

χ runs over all representatives of $\mathbb{Q}_\ell$-conjugacy classes of irreducible characters of Δ_n.

$$B_k \leftrightarrow \mathrm{Ker}\chi \Longrightarrow A_{n,\chi} \cong A_{k,\chi}$$

We assume that χ is injective.

$\mathbb{B}_n = \mathbb{Q}(\zeta_{n+2} + \zeta_{n+2}^{-1})$, $\zeta_n = \exp(2\pi\sqrt{-1}/2^n)$. We use the element

$$\xi_n = (\zeta_{n+2} - 1)(\zeta_{n+2}^{-1} - 1) = 2 - \zeta_{n+2} - \zeta_{n+2}^{-1} \in \mathbb{B}_n$$

$e_{\chi,\ell^k} \in \mathbb{Z}[\Delta_n]$ s.t. $e_{\chi,\ell^k} \equiv e_\chi \pmod{\ell^k}$

Lemma 2.1 (Gras, Gillard, Greenberg, Mazur, Wiles)**.**

$$\sqrt[\ell^k]{\xi_n^{e_{\chi,\ell^k}}} \in \mathbb{B}_n, \quad \sqrt[\ell^{k+1}]{\xi_n^{e_{\chi,\ell^{k+1}}}} \notin \mathbb{B}_n \implies |A_{n,\chi}| = \ell^{k[\mathbb{Z}_\ell[\chi(\Delta_n)]:\mathbb{Z}_\ell]}$$

Corollary 8.

$$\sqrt[\ell]{\xi_n^{e_{\chi,\ell}}} \notin \mathbb{B}_n \implies |A_{n,\chi}| = 1$$

Corollary 9. $\exists\, p$ *: prime number with* $p \equiv 1 \pmod{2^{n+2}\ell}$ *s.t.*

$$(\xi_n^{e_{\chi,\ell}})^{\frac{p-1}{\ell}} \not\equiv 1 \pmod{\mathfrak{p}} \quad \textit{for some prime } \mathfrak{p} \textit{ of } \mathbb{B}_n \textit{ over } p$$
$$\implies |A_{n,\chi}| = 1$$

We may assume $e_\chi \in \mathbb{F}_\ell$.
$\eta_n \in \overline{\mathbb{F}}_\ell$: primitive 2^n-th root of 1, $K = \mathbb{F}_\ell(\eta_n)$
$\Delta_n = \langle\, \rho\, \rangle$, $(\zeta_{n+2} + \zeta_{n+2}^{-1})^\rho = \zeta_{n+2}^5 + \zeta_{n+2}^{-5}$

$\widehat{\Delta}_n = \langle\, \chi \,\rangle,\ \chi : \Delta \longrightarrow \overline{\mathbb{F}}_\ell^\times,\ \chi(\rho) = \eta_n^{-1}$
inj. char. of Δ_n is of a form χ^j $(j : odd)$

$$e_{\chi^j} = \frac{1}{2^n} \sum_{i=0}^{2^n-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{ij})\rho^i \in \mathbb{F}_\ell[\Delta_n]$$

p : a prime number s.t. $p \equiv 1 \pmod{2^{n+2}\ell}$
g_p : a primitive root of p.
$\exists\, \mathfrak{p}$: a prime ideal of $\mathbb{B}_n$ lying over p s.t.

$$\zeta_{n+2} + \zeta_{n+2}^{-1} \equiv g_p^{\frac{p-1}{2^{n+2}}} + g_p^{-\frac{p-1}{2^{n+2}}} \pmod{\mathfrak{p}}$$

If $e_{\chi^j} = \sum_i a_{ij}\rho^i$, then

$$
\begin{aligned}
\xi_n^{e_{\chi^j}} &= \prod_{i=0}^{2^n-1} \left(2 - \zeta_{n+2} - \zeta_{n+2}^{-1} \right)^{a_{ij}\rho^i} \\
&= \prod_{i=0}^{2^n-1} \left(2 - \zeta_{n+2}^{5^i} - \zeta_{n+2}^{-5^i} \right)^{a_{ij}} \\
&\equiv \underbrace{\prod_{i=0}^{2^n-1} \left(2 - g_p^{\frac{p-1}{2^{n+2}}5^i} - g_p^{-\frac{p-1}{2^{n+2}}5^i} \right)^{a_{ij}}}_{\text{calculate mod } p} \pmod{\mathfrak{p}}
\end{aligned}
$$

This is $O(2^n)$ complexity and hard to compute for large n.

But we can reduce the amount of computation.

We assmue that $\ell \equiv 1 \pmod 4$, $2^s \,||\, \ell - 1$, $n \geq s+1$ and explain how to reduce. We can prove

$$
\begin{aligned}
e_{\chi^j} &= \frac{1}{2^n} \sum_{i=0}^{2^n-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{ij})\rho^i \\
&= \frac{1}{2^n} \sum_{i=0}^{2^s-1} \mathrm{Tr}_{K/\mathbb{F}_\ell}(\eta_n^{2^{n-s}ij})\rho^{2^{n-s}i} \\
&= \frac{1}{2^s} \sum_{i=0}^{2^s-1} \eta_s^{ij}\, \rho^{2^{n-s}i}
\end{aligned}
$$

$X = \{\, j \in \mathbb{Z} \mid 1 \leq j \leq 2^s - 1 :$ odd $\}$, then

$\{\, \chi^j \mid j \in X \,\}$: representatives of $\mathbb{F}_\ell$-conjugacy classes of injective characters of Δ_n

$\xi_n^{e_{\chi^j}}$ $(j \in X)$ is computable in $O(4^s)$ times not in $O(4^n)$

$X = \{\, j \in \mathbb{Z} \mid 1 \le j \le 2^s - 1 : \text{ odd } \}$
$b,\ z_1,\ z_2,\ a_{ij} \in \mathbb{Z}$ s.t.

$$\begin{aligned} b &= 5^{2^{n-s}} \\ z_1 &\equiv g_p^{\frac{p-1}{2^{n+2}}} \equiv z_2^{-1} \pmod p \\ a_{ij} &\equiv g_\ell^{\frac{\ell-1}{2^n} ij} \pmod \ell \end{aligned}$$

Criterion 2. *Assume that for any $j \in X$, there exists a prime number p which satisfies $p \equiv 1 \pmod{2^{n+2}\ell}$ and*

$$\left(\prod_{i=0}^{2^s-1} (2 - z_1^{b^i} - z_2^{b^i})^{a_{ij}} \right)^{\frac{p-1}{\ell}} \not\equiv 1 \pmod p\,.$$

Then,

$$\ell \nmid \frac{h_n}{h_{n-1}}\,.$$

$$\ell \nmid \frac{h_1}{h_0},\ \ell \nmid \frac{h_2}{h_1},\ \cdots, \ell \nmid \frac{h_n}{h_{n-1}} \implies \ell \nmid h_n$$

2.2. **logarithmic version.**

Criterion 2 is simple but need a very long time for $\ell = 65537 = 2^{16} + 1$. So we consider a logarithmic version.

$$\nu_p : \mathbb{F}_p^\times \longrightarrow \mathbb{Z}/(p-1)\mathbb{Z} \quad \text{by} \quad x = g_p^{\nu_p(x)}$$

For $\ell = 65537$ and $n = 39$, $p \simeq 10^{18}$.

$\nu_p(x)$ is difficult to compute in gegenal. But $\nu_p(x)$ mod ℓ is enough for our purpose and we are able to find $i \in \mathbb{Z}$ with $\nu_p(x) = i + j\ell$ by

$$x^{\frac{p-1}{\ell}} = \left(g_p^{i+j\ell}\right)^{\frac{p-1}{\ell}} = \left(g_p^{\frac{p-1}{\ell}}\right)^i$$

in a resonable time. Hence we can compute

$$x_i \equiv \nu_p(2 - z_1^{b^i} - z_2^{b^i}) \pmod{\ell}.$$

Criterion 3. *Assume that for any $j \in X$, there exists a prime number p which satisfies $p \equiv 1 \pmod{2^{n+2}\ell}$ and*

$$\sum_{i=0}^{2^s-1} a_{ij} x_i \not\equiv 0 \pmod{\ell}$$

Then,

$$\ell \not| \frac{h_n}{h_{n-1}}\,.$$

Criterion 3 is faster than Criterion 2 in spite of a overhead computing x_i. But it is still an $O(4^s)$ algorithm and difficult to handle $\ell = 738197503$ because

$$2^{26} \;\; || \;\; \ell + 1\,.$$

2.3. **using FFT.**

We continuously assume that $\ell \equiv 1 \pmod 4$ and $n \geq s+1$. Then $a_{ij} = \eta_s^{ij}$. By putting $j = 2r+1$ and using a trick $2ri = r^2 + i^2 - (r-i)^2$, we have

$$\sum_i a_{ij} x_i \;=\; \sum_i \eta_s^{i(2r+1)} x_i = \eta_s^{r^2} \sum_i \eta_s^{-(r-i)^2} \eta_s^{i(i+1)} x_i$$

This is a cyclic convolution of $u_i = \eta_s^{-i^2}$ and $v_i = \eta_s^{i(i+1)} x_i$. Hence we can compute $\xi_n^{e_{\chi^j}}$ $(j \in X)$ in $O(s2^s)$ time.

In this manner, we established the following.

Theorem 10. $\ell < 10^9 \Longrightarrow \ell \nmid h_n$ *for all* $n \geq 1$.

3. Coates' conjecture

It is natural to consider an odd prime analogue to $\mathbb{B}_n$. Now we put

$$\mathbb{B}_{p,n} = \begin{cases} \mathbb{Q}(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}) & p = 2\,, \\ \text{the subfield of } \mathbb{Q}(\zeta_{p^{n+1}}) \text{ with degree } p^n & p \geq 3\,. \end{cases}$$

Conjecture 3.1. *$h(\mathbb{B}_{p,n}) = 1$ for all p and n.*

There are no known counter-examples.

John Coates considered

$$\overline{\mathbb{Q}} = \prod_{p,n} \mathbb{B}_{p,n}\,.$$

Every subfield of $\overline{\mathbb{Q}}$ of finite degree over $\mathbb{Q}$ is uniquely determined by it degree. Namely, for $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, we put

$$\mathbb{Q}(n) = \mathbb{B}_{p_1,e_1}\mathbb{B}_{p_2,e_2}\cdots\mathbb{B}_{p_r,e_r}\,, \quad h(n) = h(\mathbb{Q}(n))\,.$$

Conjecture 3.2 (Coates, original version). *$h(n) = 1$ for all $n \geq 1$.*

Horie 2001
$31 \mid h(2 \cdot 31)$, $73 \mid h(3 \cdot 73)$

Fukuda, Komatsu 2011
$31 \mid h(2 \cdot 31)$, $1546463 \mid h(2 \cdot 1546463)$, $73 \mid h(3 \cdot 73)$

Fukuda, Komatsu, Morisawa 2011
$18433 \mid h(2^8 \cdot 18433)$, $114689 \mid h(2^{10} \cdot 114689)$,
$487 \mid h(3^4 \cdot 487)$, $238627 \mid h(3^4 \cdot 238627)$,
$2251 \mid h(5^2 \cdot 2251)$

Fukuda 2011
$107 \mid h(2 \cdot 53)$

Conjecture 3.3 (Coates, final version). *$h(n)$ is bounded for all $n \geq 1$.*

4. An algorithm computing p-class group of an abelian number field

Algorithm of Buchman

- applicable to arbitrary number field F
- compute the whole class group C_F
- need a parallel computation of C_F and E_F
- sometimes need GRH

Algorithm of Aoki-Fukuda(LNCS vol.4076, 56–71, 2006)

- applicable to abelian number field F
- compute p-part of C_F
- don't need to compute E_F
- don't need GRH

p : odd prime number
F : abelian extension of $\mathbb{Q}$ with $p \nmid [F:\mathbb{Q}]$
A_F : p-part of the ideal class group of F, $\Delta = G(F/\mathbb{Q})$
$\chi : \Delta \longrightarrow \overline{\mathbb{Q}_p}^{\times}$: a character

$$
\begin{aligned}
e_\chi &= \frac{1}{|\Delta|}\sum_{\sigma\in\Delta}\mathrm{Tr}(\chi^{-1}(\sigma))\sigma \ \in\ \mathbb{Z}_p[\Delta], \\
A_F &= \bigoplus_{\chi} A_{F,\chi}, \quad A_{F,\chi} = A_F^{e_\chi} \\
A_{F,\chi} &\cong A_{K,\chi} \quad \text{if} \quad K = F^{\mathrm{Ker}\,\chi}
\end{aligned}
$$

We assume $\chi(\neq \omega, 1)$ is injective and try to establish an algorithm computing $A_{K,\chi}$. We also assume χ is even because odd case is easier.
Let $N = \mathrm{cond}(\chi) = \mathrm{cond}(K)$. Then,

$$
N = p^{\mathrm{ord}_p(N)} N_0, \quad p \nmid N_0, \quad \mathrm{ord}_p(N) \leq 1
$$

For each $n \in \mathbb{N}$, we define a cyclotomic unit $\xi_{K,n} \in K(\zeta_n)$ by

$$\xi_{K,n} = N_{\mathbb{Q}(\zeta_{Nn})/K(\zeta_n)}(\zeta_{Nn} - 1),$$

where $\zeta_n = \exp(2\pi\sqrt{-1}/n)$. We abbreviate $\xi_K = \xi_{K,1}$.

The order of $A_{K,\chi}$ is handled as follows.

$$\begin{aligned} E_{K,\chi} &= (E_K \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi \cong \mathcal{O}_\chi \quad \text{as } \mathcal{O}_\chi = \mathbb{Z}_p[\chi(\Delta)]\text{-module} \\ C_{K,\chi} &= \langle\, \xi_K^{e_\chi} \,\rangle \subset E_{K,\chi} \\ |\, A_{K,\chi} \,| &= |\, E_{K,\chi}/C_{K,\chi} \,| \end{aligned}$$

Namely, if d_0 is the maximal power of p satisfying $\xi_K^{e_\chi} \in E_{K,\chi}^{d_0}$, then

$$|\, A_{K,\chi} \,| = d_0^{[\mathcal{O}_\chi : \mathbb{Z}_p]}\,.$$

The exact value of d_0 is difficult to compute for a large number field. But we can get an upper bound d of d_0 as in the following way.

Lemma 4.1. *Let $\chi(\neq \mathbf{1})$ be an even character. If there exists a prime number ℓ which is congruent to 1 modulo p^{n+1} and totally decomposed in K and satisfies*

$$({\xi_K}^{e_{\chi,p^{n+1}}})^{\frac{\ell-1}{p^{n+1}}} \not\equiv 1 \pmod{\mathcal{L}} \tag{1}$$

for some prime ideal $\mathcal{L}$ of K lying above ℓ, then we have $|A_{K,\chi}| \leq p^{n[\mathcal{O}_\chi:\mathbb{Z}_p]}$.

So we fix d s.t.

$$d_0 \leq d$$

and argue with d.

Remark . We must take $d = d_0$. If $d_0 < d$, then our algorithm does not work. Namely, we choose d as a candidate of d_0. We can not prove $d = d_0$ at present but prove $d = d_0$ finally.

We use two auxiliary prime numbers ℓ and ℓ^*.

L is a finite set of prime numbers ℓ which satisfy

$$\begin{aligned} \ell &\equiv 1 \pmod{d^2} \\ \chi(\ell) &= 1 \\ ({\xi_K}^{e_{\chi,dp}})^{\frac{\ell-1}{dp}} &\not\equiv 1 \pmod{\mathcal{L}} \quad \exists\, \mathcal{L}: \text{ prime of } K \text{ lying above } \ell \\ ({\xi_K}^{e_{\chi,d}})^{\frac{\ell-1}{d}} &\equiv 1 \pmod{\mathcal{L}} \quad \forall\, \mathcal{L}: \text{ prime of } K \text{ lying above } \ell \end{aligned}$$

L^* is a finite set of prime numbers ℓ^* satisfying

$$\ell^* \equiv 1 \pmod{d^2 N_0 \ell} \quad \forall\, \ell \in L$$

We try to choose L so that its elements generate $A_{K,\chi}$ and use L^* to guarantee that primes in L actually generate $A_{K,\chi}$.

$$
\begin{aligned}
J_{L^*} &= \prod_{\mathcal{L}^*|\ell^*,\, \ell^* \in L^*} (\mathcal{O}_{K(\mu_r)}/\mathcal{L}^*)^\times,\ r = \prod_{\ell \in L} \ell \\
\overline{E}_K &= \langle (\varepsilon^\sigma \bmod \mathcal{L}^*)_{\mathcal{L}^*} \in J_{L^*} \mid \sigma \in \Delta \rangle_{\mathbb{Z}} \subset J_{L^*} \\
& \quad (E_K/{E_K}^d)_\chi \quad \left(\cong \mathcal{O}_\chi/d\right) \quad = \langle\, \varepsilon \,\rangle \quad \text{as } \mathcal{O}_\chi\text{-module} \\
& \quad J_{L^*}/(J_{L^*})^d \overline{E}_K \quad \text{is determined independent of } \varepsilon \\
W_{L^*,\chi} &\subset (K(\mu_r)^\times / {K(\mu_r)^\times}^d E_K)_\chi : \mathcal{O}_\chi\text{-submodule} \\
& \quad \text{generated by all elements prime to } \ \forall\, \ell^* \in L^* \\
D^* &: W_{L^*,\chi} \to J_{L^*}/(J_{L^*})^d \overline{E}_K \quad \text{the diagonal map} \\
D_\ell &= \sum_{i=0}^{\ell-2} i {\sigma_\ell}^i, \quad G(K(\mu_\ell)/K) = \langle\, \sigma_\ell \,\rangle
\end{aligned}
$$

$$\mathcal{M}_{L,L^*} \;=\; D^*\big(\langle \xi_{K,\ell}{}^{D_\ell e_\chi} \bmod K(\mu_r)^{\times d} E_K \mid \ell \in L\rangle_{\mathcal{O}_\chi}\big)$$
$$\mathcal{O}_\chi\text{-submodule of } J_{L^*}/(J_{L^*})^d \overline{E}_K$$

Now we state our theorems. Theorem 12 enables us to determine the structure of $A_{K,\chi}$ via $\mathcal{M}_{L,L^*}$ and Theorem 11 guarantees that there always exist L and L^* for which Theorem 12 holds if we take $d = d_0$, where d_0 be the power of p such that $|A_{K,\chi}| = d_0{}^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$ as before.

Theorem 11. *For $d = d_0$, there exist finite sets L and L^* of rational primes satisfying $|\mathcal{M}_{L,L^*}| = d_0{}^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$.*

Theorem 12. *If we have $|\mathcal{M}_{L,L^*}| = d^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$ for some L and L^*, then we have*

$$A_{K,\chi} \cong \mathcal{M}_{L,L^*} \quad \textit{as} \quad \mathbb{Z}_p\textit{-module.}$$

4.1. **How to compute $\mathcal{M}_{L,L^*}$.**

$$\mathcal{M}_{L,L^*} \subset J_{L^*}/(J_{L^*})^d \overline{E}_K$$

The problem is how to compute $\overline{E}_K$. We can avoid this difficulty by requesting further condition on L^*:

$$({\xi_K}^{e_{\chi,d^2}})^{\frac{\ell^*-1}{d^2}} \equiv 1 \pmod{\mathcal{L}^*} \quad \forall\, \mathcal{L}^* \mid \ell^* \;\; \forall\, \ell^* \in L^* \tag{2}$$

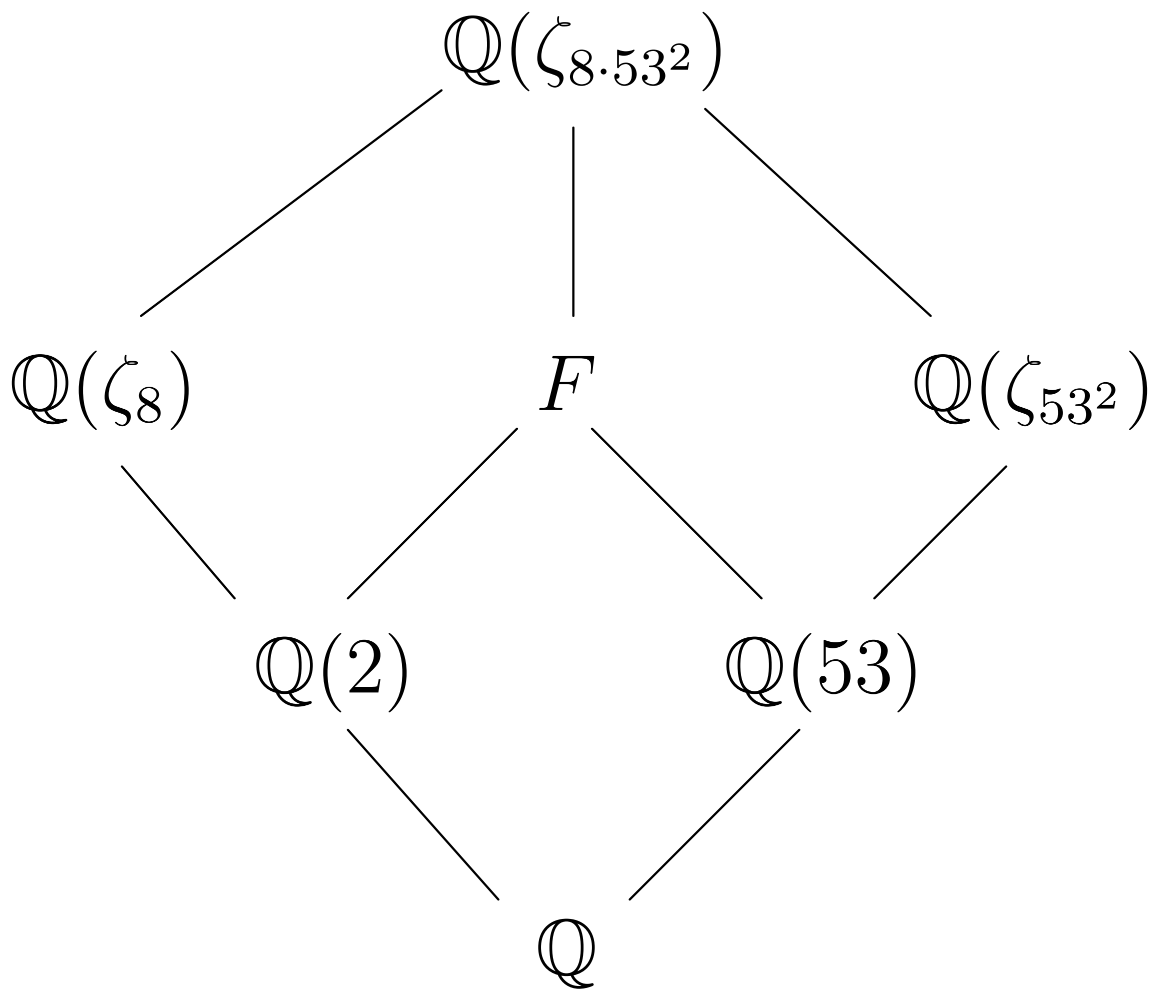
Once one assume (2), one can easily compute $\mathcal{M}_{L,L^*}$ because

$$J_{L^*}/(J_{L^*})^d \overline{E}_K = J_{L^*}/(J_{L^*})^d \,.$$

Though the condition (2) seems highly technical, we succeeded in finding such ℓ^* in all practical calculations.

4.2. **Example.**

$$F \quad = \quad \mathbb{Q}(2 \cdot 53) = \mathbb{Q}(2)\,\mathbb{Q}(53)$$



$$X^{106} - 2862X^{104} + 1802X^{103} + 3900588X^{102} - 4638030X^{101} - 3373404155X^{100} + 5673896238X^{99} + 2081752275142X^{98}$$

$$- 4398128806988X^{97} - 977389100655721X^{96} + 2429859905389614X^{95} + 363549526140245392X^{94} - 1020429095666186350X^{93}$$

$$- 1101582219163107344 99X^{92} + 33925382228782136539 2X^{91} + 277492733035243591775 46X^{90} - 918224444402959941502 02X^{89}$$

$$- 5901624396051283040531182X^{88} + 20648869148949768841422056X^{87} + 107256506501063279849013 7398X^{86}$$

$$- 3918025859734189865774597880X^{85} - 16819195482346545247041742 4101X^{84} + 634876013490169421241504567932X^{83}$$

$\dots$

$\dots$

$\dots$

$$+ 4091791858828931257406254423165568805963826731183334402901983050124564 17X^{22}$$

$$- 5634640363814502278258169059398756657589745585827977013028693295155450 36X^{21}$$

$$- 1098500808659915500363398446632788427641194291293271720887409532042327 240X^{20}$$

$$+ 1330937269294442853362274642592676639158500801347535748664825989940987 158X^{19}$$

$$+ 2390216386565429830832065403321260382451335471219125611212694324435855 385X^{18}$$

$$- 2476302782967875107628308770537976626480322020625317565946134266465532 534X^{17}$$

$$- 4130356405885465870450941317206409094663802779323967824069447876400458 200X^{16}$$

$$+ 3508812253030802132953099212239152646443245476982586655464367742184134 552X^{15}$$

$$+\,5525906619615158308101022286522139931080968985209686399477177696895914934X^{14}$$

$$-\,3600993328850310057543450856734743728293258338042761420245092855453342806X^{13}$$

$$-\,5539550340860037020893964065034522942356733061593745116235808870022102588X^{12}$$

$$+\,2454230555629935084008384601129581977809193353518819983625611714330648950X^{11}$$

$$+\,3979597896764893224663691699950013468200518473787145534147321670632797119X^{10}$$

$$-\,902631889558091660513183957709437279270637992855335218016143638760081454X^{9}$$

$$-\,1913089999533662203817388909792448015487554575413958363832353398976363622X^{8}$$

$$+\,200534929264482016076778005571766013799349739175163807868815600069140 16X^{7}$$

$$+\,539217384501017861944712996651790763390760513744093201418377608077772466X^{6}$$

$$+\,1067700837905541875402100208857185092288891385080060717638625828632550 54X^{5}$$

$$-\,600623222668498910863807509411419777873929518272608149841023947078188 80X^{4}$$

$$-\,267019205816760972010372226072572031488270985372637519583520997819822 04X^{3}$$

$$-\,30855751320714042243562305493888687680163408504011829619516438098499003X^{2}$$

$$+\,3168959176396600000775407897599455044433955335001046414174343217808 6X$$

$$+\,1428092422058835777117356135526788910255649117687929230233808985151 9$$

$f = \mathrm{cond}(F) = 8 \cdot 53^2,\ p = 107.$ We take $d = p$.
A_F : p-part of the ideal class group of F
$\Delta = G(F/\mathbb{Q}) = \langle\, \sigma \mid F \,\rangle,\ \sigma \in G(\mathbb{Q}(\zeta_f)/\mathbb{Q}),\ \zeta_f^{\sigma} = \zeta_f^{19717}$
$\chi : \Delta \longrightarrow \mathbb{Z}_p^{\times}$ s.t. $\chi(\sigma) = \eta^{-1},\ \eta \in \mathbb{Z}_p^{\times},\ \eta^{p-1} = 1,\ \eta \equiv 2 \pmod{p}$

$$\begin{aligned} e_{\chi^j} &= \frac{1}{|\Delta|}\sum_{\rho\in\Delta}\chi^{-j}(\rho)\rho = \frac{1}{|\Delta|}\sum_{i=0}^{105}\eta^{ij}\sigma^i \in \mathbb{Z}_p[\Delta] \\ A_{F,j} &= A_{F,\chi^j} = A_F^{e_\chi^j} \end{aligned}$$

$$\begin{aligned} j \neq 23 &\implies A_{F,j} = 0 \\ j = 23 &\implies |\,\mathcal{M}_{L,L^*}\,| = d \Longrightarrow A_{F,j} \cong \mathcal{M}_{L,L^*} \cong \mathbb{Z}/p\mathbb{Z} \end{aligned}$$

with $L = \{\,3087383137\,\},\ L^* = \{\,953193463154457763 3\,\}$.

Hence we have $A_F \cong \mathbb{Z}/107\mathbb{Z}$.

4.3. **Outline of our algorithm.**

Input	p, f and a subgroup H of $G = (\mathbb{Z}/f\mathbb{Z})^\times$
Output	informations about p-part of the ideal class group of the subfield F of $\mathbb{Q}(\zeta_f)$ corresponding to H
Step1	We run all the cyclic subfields K of F, namely all the subgroups H_1 of G s.t. $H \subset H_1 \subset G$, G/H_1 is cyclic, and estimate p-part of $h(F)$.
Step2	Using two sets of auxiliary prime numbers ℓ and ℓ^*, we prove that our estimate is correct and simultaneously determine the structure of p-part of $C(F)$.

Thank You !