# A NEW ALGORITHM FOR COMPUTING $p$-CLASS GROUPS OF ABELIAN NUMBER FIELDS

青木美穂 AND 福田隆

## 1. Introduction

計算機の発達とともに代数体の様々な不変量を計算するアルゴリズムの研究が進み Computational Number Theory とでも呼ぶべき分野が発展しつつある．有限次代数体 $F$ の最も基本的な不変量であるイデアル類群 $Cl_F$ と単数群 $E_F$ を計算する十分実用になるアルゴリズムが多くの人により開発され，いくつかのソフトウェアパッケージに実装されている．しかしながら $F$ の判別式が大きくなると現実的な時間で計算を完了するために一般 Riemann 予想 (GRH) を仮定したり，類群だけを求めたい時にも類群と単数群を並行して計算しなければならない等，改良すべき点も残されている．

今回我々が提案するのは，$F$ が有限次アーベル体で $p$ が $F$ の次数 $[F:\mathbb{Q}]$ を割らない奇素数の時に，類群の $p$-part $Cl_F\{p\}$ を新しい原理に基づいて計算するアルゴリズムである．GRH は必要なく，基本単数を求めることなしに $Cl_F\{p\}$ を計算できる．

$A_F = Cl_F\{p\}$ とおくと，複素共役 $J$ の作用で $A_F$ は plus part と minus part の直和に分解できる．

$$A_F = A_F^+ \oplus A_F^-, \quad A_F^{\pm} = \{x \mid x \in A_F, Jx = \pm x\}.$$

我々の方針は $A_F^-$ と $A_F^+$ のよい性質をもつ annihilator を用いて $A_F^-$ 及び $A_F^+$ の生成元を具体的に記述しようというものである．$A_F^-$ については古典的な Stickelberger 元がよい性質をもつ annihilator として知られており，Gauss 和を使って $A_F^-$ の生成元を記述できる．$A_F^+$ については近年の Kolyvagin-Rubin-Thaine の研究により Stickelberger 元の類似物が構成されており，Gauss 和の代わりに円単数の Euler System から得られる元が生成元を記述する．数学的な部分は投稿中の論文を見て頂くことにして，ここではアルゴリズムを中心に解説しよう．

この共同研究は隅田浩樹氏が最近開発した $A_F^+$ の位数を計算する優れたアルゴリズムに触発され，著者の一人 (青木) が研究していた類群の構造を Gauss 和と円単数で記述する無限時間アルゴリズムに隅田の方法を採り入れ有限時間アルゴリズムを開発する方向で始まったが，できあがってみると隅田の方法とは独立の新しいアルゴリズムとなった．しかし基本的な部分に隅田氏のアイデアが本質的に利用されており，この場をかりて隅田氏に感謝の意を表します．

Acknowledgement. This paper is supported by the 21 COE program “Constitution of wide-angle mathematical basis focused on knots”.

## 2. Notations and main results

$F$ を有限次アーベル体，$p$ を $F$ の次数を割らない奇素数とする．ガロア群 $\Delta = \mathrm{Gal}(F/\mathbb{Q})$ の指標 $\chi : \Delta \to \overline{\mathbb{Q}_p}^{\times}$ から原始巾等元

$$e_\chi = \frac{1}{|\Delta|}\sum_{\sigma\in\Delta} Tr(\chi^{-1}(\sigma))\sigma \quad \in \mathbb{Z}_p[\Delta],$$

を作る．$Tr : \mathbb{Q}_p(\chi(\sigma)|\sigma\in\Delta) \to \mathbb{Q}_p$ は trace map である．$\mathbb{Z}_p[\Delta]$-加群 $M$ に対し，$M$ の $\chi$-part $M_\chi$ を $M_\chi = e_\chi M$ で定義する．$\mathcal{O}_\chi = \mathbb{Z}[\chi(\Delta)]$ とおくと，

$$\chi(\sigma)a = \sigma a \ \text{ for any } a\in M \text{ and } \sigma\in\Delta$$

により $M_\chi$ は $\mathcal{O}_\chi$-加群になる．$p$ に関する仮定より $A_F = \oplus_\chi A_{F,\chi}$ であるから，$A_{F,\chi}$ の $\mathcal{O}_\chi$-加群としての構造がわかれば $A_F$ の $\mathcal{O}_\chi$-加群としての構造がわかる．更に $F$ の $\mathrm{Ker}\chi$ による固定体を $F^\chi$ とすれば，$\mathcal{O}_\chi$-加群としての自然な同型 $A_{F,\chi} \simeq A_{F^\chi,\chi}$ があるので，$F = F^\chi$ と思ってよい．

そこで $\chi$ を $\Delta$ の任意の指標，$K = F^\chi$ とし，$A_{K,\chi}$ を調べることにする．$\chi$ が奇指標であれば $K$ は総虚アーベル体，偶指標でれば総実アーベル体であることに注意しておく．$\chi$ が自明指標または Theichmüller 指標 $\omega$ であれば $A_{K,\chi} = 0$ であるから $\chi \neq 1, \omega$ としてよい．

$N$ を $\chi$ の導手 (i.e. $K$ の導手) とし，$N = p^{\mathrm{ord}_p(N)}N_0$ $(p \nmid N_0)$ と分解しておく．仮定より $\mathrm{ord}_p(N) \le 1$ である．我々のアルゴリズムの基礎である Gauss 和 $\tau_{\mathcal{L}} \in K(\mu_\ell)^\times$ と円単数 $\xi_{K,n} \in K(\mu_n)^\times$ は次のように定義される．

**定義 2.1.** (Gauss 和) $\ell$ を $\ell \equiv 1 \pmod N$ をみたす有理素数とし，$\ell$ の上にある $K$ の素イデアル $\mathcal{L}$ および，$\mathcal{L}$ の上にある $\mathbb{Q}(\mu_N)$ の素イデアル $\widetilde{\mathcal{L}}$ を一つ固定する時

$$\tau_{\widetilde{\mathcal{L}}} = \sum_{a=1}^{\ell-1} \chi_{\widetilde{\mathcal{L}}}(a)\zeta_\ell{}^a, \quad \tau_{\mathcal{L}} = N_{\mathbb{Q}(\mu_{N\ell})/K(\mu_\ell)}\,\tau_{\widetilde{\mathcal{L}}}\,.$$

ここで $\chi_{\widetilde{\mathcal{L}}} : (\mathbb{Z}/\ell)^\times \to \mu_N$ は $\chi_{\widetilde{\mathcal{L}}}(a) \equiv a^{-\frac{\ell-1}{N}} \pmod{\widetilde{\mathcal{L}}}$ で定まる指標，$N_{\mathbb{Q}(\mu_{N\ell})/K(\mu_\ell)} : \mathbb{Q}(\mu_{N\ell})^\times \to K(\mu_\ell)^\times$ はノルム写像である．$\tau_{\mathcal{L}}$ は $\widetilde{\mathcal{L}}$ に依らず $\mathcal{L}$ から一意的に定まる．

**定義 2.2.** (円単数) 正整数 $n$ に対し

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

ここで $\zeta_{Nn}$ は $1$ の原始 $n$ 乗根である．

さて $d_0^{[\mathcal{O}_\chi:\mathbb{Z}_p]} = |A_{K,\chi}|$ とし，次の条件をみたす $p$ の巾 $d$ を固定する．

$$\boxed{d \text{ の条件}}: \quad \chi \text{ が奇指標の時は } d = d_0\,.\ \chi \text{ が偶指標の時は } d \ge d_0\,. \qquad (1)$$

*Remark .* この条件をみたす $d$ を具体的に与えるのは易しい．実際 $\chi$ が奇指標であれば $d_0$ は容易に計算可能であるし，$\chi$ が偶指標の時は 補題 2.3 を用いて $d_0$ の上限を与えることができる．$d_0$ については以下を参照.
1) $\chi$ が奇指標の時は，Mazur-Wiles により証明された岩澤主予想により，一般 Bernoulli 数 $B_{1,\chi^{-1}}$ を割る $p$ の最大巾が $d_0$ であり，$B_{1,\chi^{-1}}$ の計算は容易である．
2) $\chi$ が偶指標の時 $d_0$ の計算は難しい．$E_K$ を $K$ の単数群とし $E_{K,\chi} = (E_K \otimes_{\mathbb{Z}} \mathbb{Z}_p)_\chi$ とおくと，$\chi \neq 1$ であれば $E_{K,\chi} \simeq \mathcal{O}_\chi$ であり，$C_{K,\chi} = \langle \xi_{K,1}{}^{e_\chi} \rangle_{\mathcal{O}_\chi}$ が円単数の $\chi$-part になる．再び岩澤主予想により $|A_{K,\chi}| = |E_{K,\chi}/C_{K,\chi}|$ であるから，

$$\xi_{K,1}{}^{e_\chi} \in E_{K,\chi}{}^{d_0} \qquad (2)$$

をみたす $p$ の最大巾が $d_0$ であるが，(2) のチェックには一般に代数体における計算が必要であり，$K$ の次数が高くなると，有理整数の計算に帰着できる $B_{1,\chi^{-1}}$ に比べて格段に難しい．

3) 最近，隅田 [4] は $\chi$ が $\chi^{-1}\omega(p)\neq 1$ をみたす偶指標の時に，(2) を有理整数の合同計算でチェックできる優れたアルゴリズムを開発した．それによれば $\chi^{-1}\omega(p)\neq 1$ の時 $d_0$ は有理整数の計算で効率的に求めることができる．一方，後で述べる定理 2.5 によれば，$d_0$ の上限がわかれば，$\chi^{-1}\omega(p)=1$ の場合を含めて，$A_{K,\chi}$ の構造を計算することができる．

$x\in\mathbb{Z}_p[\Delta]$ に対し，$x_{p^n}$ を $x_{p^n}\equiv x \pmod{p^n}$ をみたす $Z[\Delta]$ の元とする．次の補題により $\chi$ が偶の時の $d_0$ の上限を知ることができる．

**補題 2.3.** $\chi(\neq 1)$ を偶指標とする．$\ell\equiv 1 \pmod{p^{n+1}}$ をみたし $K$ で完全分解する素数 $\ell$ および $\ell$ の上にある $K$ の素イデアル $\mathcal{L}$ で

$$(\xi_{K,1}{}^{e_{\chi,p^{n+1}}})^{\frac{\ell-1}{p^{n+1}}}\not\equiv 1 \pmod{\mathcal{L}} \tag{3}$$

をみたすものが存在すれば $|A_{K,\chi}|\le p^{n[\mathcal{O}_\chi:\mathbb{Z}_p]}$ である．

$\ell$ は $K$ で完全分解しているから (3) は有理整数の合同計算でチェックできることに注意しておく．次に有理素数からなる有限集合 $L, L^*$ を以下のように選ぶ．

### $L$ と $L^*$ の条件

**$\chi$ が奇指標の時**

- $L$ は $\ell\equiv 1 \pmod N$ をみたす有理素数 $\ell$ の有限集合．
- $L^*$ は任意の $\ell\in L$ に対し $\ell^*\equiv 1 \pmod{dN_0\ell}$ をみたす有理素数 $\ell^*$ の有限集合．

**$\chi$ が偶指標の時**

- $L$ は $\ell\equiv 1 \pmod{d^2}$ であり，更に次の条件をみたす有理素数 $\ell$ の有限集合．

$$\chi(\ell) = 1, \tag{4}$$

$$\exists\,\mathcal{L}:\text{ prime ideal of } K \text{ lying over } \ell \quad (\xi_{K,1}{}^{e_{\chi,dp}})^{\frac{\ell-1}{dp}} \not\equiv 1 \pmod{\mathcal{L}}, \tag{5}$$

$$\forall\,\mathcal{L}:\text{ prime ideal of } K \text{ lying over } \ell \quad (\xi_{K,1}{}^{e_{\chi,d}})^{\frac{\ell-1}{d}} \equiv 1 \pmod{\mathcal{L}}. \tag{6}$$

- $L^*$ は任意の $\ell\in L$ に対し $\ell^*\equiv 1 \pmod{d^2N_0\ell}$ をみたす有理素数 $\ell^*$ の有限集合．

$\chi$ が奇指標の時 $\ell$ は $\mathbb{Q}(\mu_N)$ で完全分解する．これは Gauss 和の計算を単純化するための条件である．一方 $\chi$ が偶指標の時，$\ell$ の合同条件は $\ell\equiv 1 \pmod{d^2}$ であり，$\ell\equiv 1 \pmod N$ ではない．Gauss 和の計算には FFT が利用できるので $\ell$ が大きくなっても深刻ではないが (計算時間は $\ell\varphi(\ell)$ に比例)，円単数の計算には今のところ FFT が使えないので $\ell$ はできるだけ小さくする必要がある (計算時間は $\ell^2$ に比例)．そこで $\ell$ は $\mathbb{Q}(\mu_N)$ でなく $K$ で完全分解するようにとり，大きさを押えるのである．一方，$\ell^*$ はいずれの場合にも $\mathbb{Q}(\mu_{Nr_L})$ $(r_L=\prod_{\ell\in L}\ell)$ で完全分解する．これらの性質により (5), (6) を除く全ての計算を有理整数の範囲内で行うことができる．

後で見るように，実例計算において我々は $\ell\in L$ 上の素イデアルが $A_{K,\chi}$ を生成していると思われる程度に $L$ を大きくとり，実際に生成していることを $L^*$ を用いて確かめるのである．

$$r=\begin{cases}1 & \text{if } \chi \text{ is odd,}\\ r_L=\prod_{\ell\in L}\ell & \text{if } \chi \text{ is even,}\end{cases}\quad\text{and}\quad J_{L^*}=\prod_{\mathcal{L}^*|\ell^*,\,\ell^*\in L^*}(\mathcal{O}_{K(\mu_r)}/\mathcal{L}^*)^\times$$

とおく．$\mathcal{L}^*$ は $\ell^*$ の上にある $K(\mu_r)$ の素イデアルであり，各 $\ell^* \in L^*$ に対し一つ選ぶ．$W_{L^*,\chi}$ を全ての $\ell^*$ と素な元で生成される $(K(\mu_r)^\times/K(\mu_r)^{\times d}E_K)_\chi$ の $\mathcal{O}_\chi$-部分加群とする．$\chi$ が $\omega$ と異なる奇指標であれば $(K(\mu_r)^\times/K(\mu_r)^{\times d}E_K)_\chi = (K^\times/K^{\times d})_\chi$ であることに注意する．$\chi(\neq 1)$ が偶指標の時は $(E_K/{E_K}^d)_\chi \cong \mathcal{O}_\chi/d$ だから，$\mathcal{O}_\chi$-加群 $(E_K/{E_K}^d)_\chi$ の生成元 $\varepsilon \in E_K$ を一つ固定する．$J_{L^*}$ の部分群 $\overline{E}_K$ を

$$\overline{E}_K = \begin{cases} 1 & \text{if } \chi \text{ is odd,} \\ \langle (\varepsilon^\sigma \bmod \mathcal{L}^*)_{\mathcal{L}^*} \in J_{L^*} \mid \sigma \in \Delta \rangle_{\mathbb{Z}} & \text{if } \chi \text{ is even.} \end{cases}$$

で定義する．$\overline{E}_K$ は $\varepsilon$ の選び方によるが $J_{L^*}/(J_{L^*})^d\overline{E}_K$ は $\varepsilon$ によらず一意的に定まることに注意する．$D^* : W_{L^*,\chi} \to J_{L^*}/(J_{L^*})^d\overline{E}_K$ を対角写像とする．$\mathrm{Gal}(K(\mu_\ell)/K)$ の生成元 $\sigma_\ell$ を一つ固定し，$D_\ell = \sum_{i=0}^{\ell-2} i\sigma_\ell{}^i$ とおく．我々のアルゴリズムの要である $\mathbb{Z}_p$-加群 $\mathcal{M}_{L,L^*}$ は次のように定義される．

**定義 2.4.**

$$\mathcal{M}_{L,L^*} := \begin{cases} D^*\big(\langle {\tau_{\mathcal{L}}}^{e_\chi} \bmod K^{\times d} \mid \mathcal{L}|\ell, \ell \in L \rangle_{\mathcal{O}_\chi}\big) & \textit{if } \chi \textit{ is odd,} \\ D^*\big(\langle {\xi_{K,\ell}}^{D_\ell e_\chi} \bmod K(\mu_r)^{\times d}E_K \mid \ell \in L \rangle_{\mathcal{O}_\chi}\big) & \textit{if } \chi \textit{ is even.} \end{cases}$$

ここで $\langle * \rangle_{\mathcal{O}_\chi}$ は $*$ で生成される $(K(\mu_r)^\times/K(\mu_r)^{\times d}E_K)_\chi$ の $\mathcal{O}_\chi$-部分加群を表す．$\mathcal{L}$ は $\ell$ の上にある $K$ の素イデアルであるが，$\mathcal{O}_\chi$-加群として生成させるので一つ固定してもよいし，動かしてもよい．

*Remark* . $\tau_{\mathcal{L}}$ は $K(\mu_\ell)$ の元であるが，${\tau_{\mathcal{L}}}^{e_\chi}$ (正確には ${\tau_{\mathcal{L}}}^{e_{\chi,d}}$) は $K$ に含まれる．$(\tau_{\mathcal{L}}^{e_\chi})$ は $\ell$ 上の素イデアルの積であり，$\xi_{K,\ell}$ は $K(\mu_r)$ の単数であるから，${\tau_{\mathcal{L}}}^{e_\chi}$ および ${\xi_{K,\ell}}^{e_\chi}$ (これも正確には ${\xi_{K,\ell}}^{e_{\chi,d}}$) は $W_{L^*,\chi}$ の元となる．

次の定理が我々の得た結果である．§4 で見るように $\mathcal{M}_{L,L^*}$ (の構造および位数) は $\chi$ が奇であれば有理整数の範囲で，$\chi$ が偶であれば有理整数と代数体の範囲で計算できるから，$A_{K,\chi}$ のアーベル群としての構造もそれに準じて計算できることになる．更に $\mathcal{O}_\chi/p^a \simeq (\mathbb{Z}/p^a)^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$ に注意すれば，$A_{K,\chi}$ の $\mathcal{O}_\chi$-加群としての構造も決定できることがわかる．

**定理 2.5.**
(1) $\chi$ が奇指標の時，$|\mathcal{M}_{L,L^*}| = d^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$ となる $L$, $L^*$ が存在する．
(2) $\chi$ が偶指標の時，$d = d_0$ であれば $|\mathcal{M}_{L,L^*}| = d^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$ となる $L$, $L^*$ が存在する．
(3) $|\mathcal{M}_{L,L^*}| = d^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$ の時，アーベル群として $A_{K,\chi} \cong \mathcal{M}_{L,L^*}$ である．

## 3. Algorithms for $\mathcal{M}_{L,L^*}$

定理 2.5 を用いて $A_{K,\chi}$ の構造を決定するには，等式 $|\mathcal{M}_{L,L^*}| = d^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$ を成立させる $L$ と $L^*$ (それから $\chi$ が偶指標であれば $d$ ) を見つければよい．この節では $d$, $L$, $L^*$ を固定した時，$\mathcal{M}_{L,L^*}$ の構造を計算する方法を説明する．

3.1. **奇指標の場合.** $g$ を $\ell \in L$ の原始根とすると，定義 2.1 における指標 $\chi_{\widetilde{\mathcal{L}}} : (\mathbb{Z}/\ell\mathbb{Z})^\times \longrightarrow \mu_N$ は $\chi_{\widetilde{\mathcal{L}}}(g)$ で定まる．1 の任意の原始 $n$ 乗根 $\zeta_N$ に対し，$\ell$ 上の $\mathbb{Q}(\mu_N)$ の素イデアル $\widetilde{\mathcal{L}}$ をうまく選ぶと $\chi_{\widetilde{\mathcal{L}}}(g) = \zeta_N$ となる．$\widetilde{\mathcal{L}}$ を特定する必要はないので，任意に選んだ $g$ および任意に選んだ $\zeta_N$ に対し $\chi_{\widetilde{\mathcal{L}}}(g) = \zeta_N$ と思ってよい．

$g_{\ell^*}$ を $\ell^* \in L^*$ の原始根とし，$s, t \in \mathbb{Z}$ を $s \equiv g_{\ell^*}^{(\ell^*-1)/N} \pmod{\ell^*}$, $t \equiv g_{\ell^*}^{(\ell^*-1)/\ell} \pmod{\ell^*}$ で定める．この時，$\zeta_N \equiv s \pmod{\widetilde{\mathcal{L}^*}}$, $\zeta_\ell \equiv t \pmod{\widehat{\mathcal{L}^*}}$ となる $\ell^*$ 上の

$\mathbb{Q}(\mu_N)$ の素イデアル $\widetilde{\mathcal{L}^*}$ および $\mathbb{Q}(\mu_\ell)$ の素イデアル $\widehat{\mathcal{L}^*}$ が存在する．従って $\overline{\mathcal{L}^*}$ を $\widetilde{\mathcal{L}^*}$ および $\widehat{\mathcal{L}^*}$ の上にある $\mathbb{Q}(\mu_{N\ell})$ の素イデアルとすれば，

$$\tau_{\widetilde{\mathcal{L}}} = \sum_{i=0}^{\ell-2} \zeta_N^i \zeta_\ell^{g^i} \equiv \sum_{i=0}^{\ell-2} s^i t^{g^i} \pmod{\overline{\mathcal{L}^*}}$$

となる．$\tau_{\mathcal{L}}^{e_x}$ を求めるには $\zeta_N^{\sigma_r} = \zeta_N^r$ で定まる各 $\sigma_r \in G(\mathbb{Q}(\mu_N)/\mathbb{Q})$ に対し

$$\tau_{\widetilde{\mathcal{L}}}^{\sigma_r} \equiv \sum_{i=0}^{\ell-2} s^{ri} t^{g^i} \pmod{\overline{\mathcal{L}^*}}$$

を計算する必要がある．まともにやると $\ell\varphi(N)$ に比例する時間がかかるが，[4] に従い $2ri = r^2 + i^2 - (r-i)^2$ に注意して

$$\tau_{\widetilde{\mathcal{L}}}^{\sigma_r} = \sum_{i=0}^{\ell-2} \zeta_N^{ri} \zeta_\ell^{g^i} = \zeta_{2N}^{r^2} \sum_{i=0}^{\ell-2} \zeta_{2N}^{-(r-i)^2} \zeta_{2N}^{i^2} \zeta_\ell^{g^i} \tag{7}$$

と変形すると $\zeta_{2N}^{-r^2}\tau_{\widetilde{\mathcal{L}}}^{\sigma_r}$ は $u_i = \zeta_{2N}^{-i^2}$ と $v_i = \zeta_{2N}^{i^2}\zeta_\ell^{g^i}$ の convolution になるから，高速フーリエ変換 (FFT) を用いて $\ell\log(\ell)$ に比例する時間で計算できるようになる．これを少し詳しく説明しよう．

3.1.1. 自前で *FFT* プログラムを書く場合. $\ell \equiv 1 \pmod{2N}$, $\ell^* \equiv 1 \pmod{2N}$ となるように $\ell, \ell^*$ をとり，$s \equiv g_{\ell^*}^{(\ell^*-1)/2N} \pmod{\ell^*}$, $t \equiv g_{\ell^*}^{(\ell^*-1)/\ell} \pmod{\ell^*}$ とする．(7) を $K = 2^k$ 個の和に直し

$$w_r = \sum_{i=0}^{K-1} u_{r-i} v_i$$

を $1 \le r \le N-1$ の範囲で計算したいのだが，

$$\begin{aligned} w_1 &= u_1v_0 + u_0v_1 + u_{-1}v_2 + \cdots + u_{-\ell+3}v_{\ell-2} + \cdots \\ w_{N-1} &= u_{N-1}v_0 + \cdots + u_{-1}v_N + \cdots + u_{-\ell+1+N}v_{\ell-2} + \cdots \end{aligned}$$

において $i < 0$ の時は $u_i = u_{K+i}$ と考えるから，この範囲で $u_i$ の index は $N-1$ が最大で $-\ell+3$ が最小である．従って $K = 2^k$ を $N-1 < K-\ell+3$ 即ち $N+\ell-3 \le K$ となるようにとり，

$$\begin{aligned} u_i &= \begin{cases} s^{-i^2} & (0 \le i \le N-1) \\ 0 & (N \le i \le K-\ell+2) \\ s^{-(K-i)^2} & (K-\ell+3 \le i \le K-1) \end{cases} \\ v_i &= \begin{cases} s^{i^2} t^{g^i} & (0 \le i \le \ell-2) \\ 0 & (\ell-1 \le i \le K-1) \end{cases} \end{aligned}$$

とおくと，

$$\tau_{\widetilde{\mathcal{L}}}^{\sigma_r} \equiv s^{r^2} w_r \pmod{\overline{\mathcal{L}^*}} \quad \text{for } 1 \le r \le N-1$$

となる．後は [1] に従って

$$\widehat{u}_s = \sum_{0 \le t < K} \zeta_K^{st} u_t \quad (0 \le s < K) \tag{8}$$

$$\widehat{v}_s = \sum_{0 \le t < K} \zeta_K^{st} v_t \quad (0 \le s < K) \tag{9}$$

を求め

$$\widehat{w}_s = \widehat{w}_s\widehat{w}_s, \quad \widehat{\widehat{w}}_r = Kw_{-r \bmod K} \tag{10}$$

を利用すればよい．$\zeta_K$ を $\bmod \ell^*$ で考えるので

$$\ell^* \equiv 1 \pmod{K} \tag{11}$$

が必要である．(8), (9), (10) はそれぞれ $k$ 回のプロセスで計算可能であるが $\zeta_K \bmod \ell^*$ との積をとるためオーバフローし易い．そこで毎回 $\bmod \ell^*$ で計算することになるが，これはかなりのオーバーヘッドになる．

3.1.2. 既存のパッケージを利用する場合. FFT そのものを提供するソフトウェアパッケージは稀だと思われるが，FFT を用いた多倍長乗算を提供するものとして例えば GMP がある．

$$0 \le u_i, v_i < \ell^*, \ \ u_i \equiv s^{-i^2} \pmod{\ell^*}, \ \ v_i \equiv s^{i^2} t^{g^i} \pmod{\ell^*} \quad (0 \le i \le \ell - 2)$$

とすると，$U = \sum_{i=0}^{\ell-2} u_i X^i$ と $V = \sum_{i=0}^{\ell-2} v_i X^i$ の積は

$$UV = \sum_{0 \le i,j \le \ell-2} u_i v_j X^{i+j} = \sum_{k=0}^{2\ell-4} \Big( \sum_{i+j=k} u_i v_j \Big) X^k$$

となる．$X = 2^{32k}$ (或は $2^{64k}$) を $X > (\ell^*)^3$ となるようにとり，$U, V$ を多倍長数だと考えて

$$W = UV = \sum_{k=0}^{2\ell-4} a_k X^k$$

を求めると，$a_k = \sum_{i+j=k} u_i v_j$ となる．この時

$$\begin{aligned}
w_1 &= u_1v_0 + u_0v_1 + u_{-1}v_2 + \cdots + u_{-\ell+3}v_{\ell-2} \\
&= u_1v_0 + u_0v_1 + u_{\ell-2}v_2 + \cdots + u_2v_{\ell-2} \\
&= a_1 + a_\ell \\
w_{\ell-3} &= u_{\ell-3}v_0 + \cdots + u_0v_{\ell-3} + u_{-1}v_{\ell-2} \\
&= u_{\ell-3}v_0 + \cdots + u_0v_{\ell-3} + u_{\ell-2}v_{\ell-2} \\
&= a_{\ell-3} + a_{2\ell-4} \\
w_{\ell-2} &= u_{\ell-2}v_0 + \cdots + u_0v_{\ell-2} \\
&= a_{\ell-2} \\
w_{\ell-1} &= u_{\ell-1}v_0 + u_{\ell-2}v_1 + \cdots + u_1v_{\ell-2} \\
&= u_0v_0 + u_{\ell-2}v_1 + \cdots + u_1v_{\ell-2} \\
&= a_0 + a_{\ell-1}
\end{aligned}$$

であり，$\ell$ は $\ell \equiv 1 \pmod{2N}$ となるように選んでおくので (i.e. $N - 1 \le \ell - 3$)，$w_r = a_r + a_{r+\ell-1}$ $(1 \le r \le N-1)$ となる．

GMP では配列 $U[i]$ $(0 \le i \le n)$ が表す多倍長数は $\sum_{i=0}^{n} U[i]2^{32i}$ (或は $\sum_{i=0}^{n} U[i]2^{64i}$) であるから考え易い (PARI は $\sum_{i=0}^{n} U[n-i]2^{32i}$ である)．この方法では積 $UV$ の後で $\bmod \ell^*$ の計算を行うので 3.1.1 に比べオーバーヘッドが少なく，また (11) を必要としないため $\ell^*$ の大きさを押えることができ，従って高速である．そのかわり多量のメモリーが必要になる．1GB のメモリーでは Table 1 の $m = 36227, 36322$ には不足であった．

3.1.3. $\mathcal{M}_{L,L^*}$ の構造. $\tau_{\mathcal{L}}^{\sigma_r} \bmod \overline{\mathcal{L}^*}$ $(r \in (\mathbb{Z}/N\mathbb{Z})^\times)$ が求まれば $\tau_{\mathcal{L}}^{e_\chi} \equiv x \pmod{\mathcal{L}^*}$ となる $x \in \mathbb{Z}$ が求まる．$\mathcal{L}^*$ は $\widetilde{\mathcal{L}^*}$ で割れる $K$ の素イデアルである．

$\mathcal{M}_{L,L^*}$ の構造は次のようにしてわかる．多くの場合 $|L| = |L^*| = 1$ であり，この時 $J_{L^*} = (\mathcal{O}_K/\mathcal{L}^*)^\times$ は巡回群であるから $\mathcal{M}_{L,L^*}$ も巡回群である．$d = p^a$, $\tau_{\mathcal{L}}^{e_\chi} \equiv x \pmod{\mathcal{L}^*}$ の時，$x^{(\ell^*-1)/p^i} \equiv 1 \pmod{\ell^*}$, $x^{(\ell^*-1)/p^{i+1}} \not\equiv 1 \pmod{\ell^*}$ であれば $|\mathcal{M}_{L,L^*}| = p^{a-i}$ である．これにかかる時間は $O(a \log \ell^*)$ であるから無視できる．

$|L^*| > 1$ の時は若干面倒になる．$|L| = |L^*| = m$ の場合を説明しよう (一般には $|L| \le |L^*|$)．$L = \{\ell_1, \cdots, \ell_m\}$, $L^* = \{\ell_1^*, \cdots, \ell_m^*\}$ とし $g_i$ を $\ell_i^*$ の原始根とする．$\mathcal{L}_i$ (resp. $\mathcal{L}_j^*$) を $\ell_i$ (resp. $\ell_j^*$) 上の素イデアルとし，まず $\tau_{\mathcal{L}_i}^{e_\chi} \equiv x_{i,j} \pmod{\mathcal{L}_j^*}$ となる $x_{i,j} \in \mathbb{Z}$ を求める．

$$(x_{i,j} g_j^{y_{i,j}})^{\frac{\ell_j^*-1}{d}} \equiv 1 \pmod{\ell_j^*}$$

となる $y_{i,j} \in \mathbb{Z}$ は $O(d \log \ell_j^*)$ 時間で求めることができる．$m \times m$ 行列 $N = (y_{i,j})$ の $\mathbb{Z}_p$ における単因子を $(d_1, \cdots, d_m)$ とすれば，アーベル群として

$$\mathcal{M}_{L,L^*} \simeq \prod_{i=1}^{m} \mathbb{Z}/(d/d_i)\mathbb{Z}$$

である．必要な時間は $O(d(\log \ell_1^* + \cdots + \log(\ell_m^*))$ である．$d$ が大きくなるのは，大きな $p$ に対し $d = p^a$ $(a > 1)$ となる時であり，同時に $|L^*| > 1$ となるのは稀であるから，殆どの場合をこの方法で処理できる．

3.2. **偶指標の場合.** まず (4), (5), (6) をみたす $d, \ell$ をいくつか見つける．補題 2.3 により，これらの $d$ は $|A_{K,\chi}|$ の上限を与える．最小の $d$ が $d^{[\mathcal{O}_\chi:\mathbb{Z}_p]} = |A_{K,\chi}|$ をみたしていると考えられるから，$\ell^*$ を小さい順に選び $|\mathcal{M}_{L,L^*}| = d^{[\mathcal{O}_\chi:\mathbb{Z}_p]}$ となるかどうか調べればよい．

$\ell$ が $\mathbb{Q}(\mu_N)$ で完全分解すれば条件 (5), (6) は有理整数の計算で高速にチェックできるが，$K$ でしか完全分解しないため代数体における計算が必要となる．$[K:\mathbb{Q}] = n$ とし $\{v_1, \cdots, v_n\}$ を $K$ の整数基とする．$\xi_{K,1}^\rho$ の値を近似計算し，連立方程式

$$\sum_{i=0}^{n} x_i v_i^\rho = \xi_{K,1}^\rho \quad (\rho \in G(K/\mathbb{Q}))$$

の解を整数に丸めれば $\xi_{K,1}$ の $\{v_i\}$ に関する係数 $x_i \in \mathbb{Z}$ が求まる．$v_i^\rho \equiv y_{i,\rho} \pmod{\mathcal{L}}$ となる $y_{i,\rho} \in \mathbb{Z}$ を求めるのは易しく，

$$\xi_{K,1}^\rho \equiv \sum_{i=1}^{n} x_i y_{i,\rho} \pmod{\mathcal{L}} \tag{12}$$

であるから，最終的に $\xi_{K,1}^{e_{\chi,dp}} \equiv z \pmod{\mathcal{L}}$ となる $z \in \mathbb{Z}$ を求めることができる．この時，条件 (5), (6) はそれぞれ $z^{(\ell-1)/dp} \not\equiv 1 \pmod{\ell}$, $z^{(\ell-1)/d} \equiv 1 \pmod{\ell}$ と同値になる．

偶の時，$\mathcal{M}_{L,L^*}$ は $J_{L^*}/J_{L^*}^d \overline{E}_K$ の部分群であり，単数の計算は類群の計算と同程度に難しいと考えられているから，$\mathcal{M}_{L,L^*}$ の計算も難しそうに見える．しかし次のようにすれば単数の影響を避けることができる．

$[K:\mathbb{Q}]$ が $p-1$ を割る場合を考え $d = |A_{K,\chi}|$ と仮定する．$x \in \mathcal{O}_{K(\mu_r)}$ に対し，$\bar{x} = (x, \cdots, x) \in J_{L^*}^d \overline{E}_K$ かどうか判定できれば，$\mathcal{M}_{L,L^*}$ の構造がわかる．$d = |A_{K,\chi}|$

だから $\eta = \sqrt[d]{\xi_{K,1}^{e_{\chi,d^2}}}$ が $(E_K/E_K^d)_\chi$ を生成し，従って

$$\begin{aligned}
\bar{x} \in J_{L^*}^d \overline{E}_K &\iff \exists\, \varepsilon \in (E_K/E_K^d)_\chi \ \forall\, \mathcal{L}^* \quad x\varepsilon \in (\mathcal{O}_{K(\mu_r)}/\mathcal{L}^*)^{\times d} \\
&\iff \exists\, \varepsilon \in (E_K/E_K^d)_\chi \ \forall\, \mathcal{L}^* \quad (x\varepsilon)^{\frac{\ell^*-1}{d}} \equiv 1 \pmod{\mathcal{L}^*} \\
&\iff \exists\, i (0 \le i < d) \ \forall\, \mathcal{L}^* \quad (x\eta^i)^{\frac{\ell^*-1}{d}} \equiv 1 \pmod{\mathcal{L}^*} \\
&\iff \exists\, i (0 \le i < d) \ \forall\, \mathcal{L}^* \quad (x^d \xi_{K,1}^{ie_{\chi,d^2}})^{\frac{\ell^*-1}{d^2}} \equiv 1 \pmod{\mathcal{L}^*} \\
&\iff \exists\, i (0 \le i < d) \ \forall\, \mathcal{L}^* \quad \left(\xi_{K,1}^{e_{\chi,d^2}\frac{\ell^*-1}{d^2}}\right)^i \equiv x^d \pmod{\mathcal{L}^*}
\end{aligned}$$

となる．このプロセスを吟味すると，$|L^*| = 1$ の場合には，$(\xi_{K,1}^{e_{\chi,d^2}})^{(\ell^*-1)/d^2} \not\equiv 1 \pmod{\mathcal{L}^*}$ であれば必ず $|\mathcal{M}_{L,L^*}| < d$ となることがわかる．従って，$|L^*| > 1$ の場合も含めて，$L^*$ に関する追加条件

$$\forall\, \ell^* \in L^* \ \forall\, \mathcal{L}^* \mid \ell^* \ (\xi_{K,1}^{e_{\chi,d^2}})^{\frac{\ell^*-1}{d^2}} \equiv 1 \pmod{\mathcal{L}^*} \tag{13}$$

を設定する．(13) は一見極めて強く思えるが，上で見たように実は合理的な条件なのである．一旦 (13) を仮定してしまえば，$d$ に関する条件 $d^{[\mathcal{O}_\chi:\mathbb{Z}_p]} \ge |A_{K,\chi}|$ より $\overline{E}_K \subset J_{L^*}^d$ となるから $J_{L^*}/J_{L^*}^d\overline{E}_K = J_{L^*}/J_{L^*}^d$ となる．後は奇指標の時と同じ方法で $\mathcal{M}_{L,L^*}$ の構造を計算できる．

(13) をみたす $\ell^*$ を見つけるのは難しくない．実際，$\xi_{K,1} = \sum_{i=1}^n x_i v_i$ となる $x_i \in \mathbb{Z}$ は計算済みだから，(12) と同様の合同計算で (13) をチェックすればよい．$\ell^*$ を捜す時間は $\xi_{K,\ell}$ の計算に較べると無視できる．

$\xi_{K,\ell}$ の計算は単純である．$\rho$ (resp. $g$) を $\ell$ (resp. $\ell^*$) の原始根とすれば，$\ell^*$ 上の $\mathbb{Q}(\mu_N)$ の適当な素イデアル $\widetilde{\mathcal{L}^*}$ および $\mathbb{Q}(\mu_\ell)$ の適当な素イデアル $\widehat{\mathcal{L}^*}$ に対し，

$$\begin{aligned}
\zeta_N &\equiv g^{\frac{\ell^*-1}{N}} \pmod{\widetilde{\mathcal{L}^*}} \\
\zeta_\ell &\equiv g^{\frac{\ell^*-1}{\ell}} \pmod{\widehat{\mathcal{L}^*}}
\end{aligned}$$

となる．$\overline{\mathcal{L}^*}$ を $\widetilde{\mathcal{L}^*}$ を割る $K$ の素イデアル，$\mathcal{L}^*$ を $\overline{\mathcal{L}^*}$ および $\widehat{\mathcal{L}^*}$ 上にある $K(\mu_r)$ の素イデアルとすると，

$$\xi_{K,\ell}^{D_\ell} \equiv \prod_{j\in H}\prod_{i=0}^{\ell-2}\left(g^{\frac{\ell^*-1}{N}j+\frac{\ell^*-1}{\ell}\rho^i-1}\right)^i \pmod{\mathcal{L}^*},$$

である．$H$ は $K$ に対応する $(\mathbb{Z}/N\mathbb{Z})^\times$ の部分群である．これは $O(N\ell)$ アルゴリズムである．

最後に $\xi_{K,\ell}^{D_\ell}$ の計算の高速化の可能性について注意する．$f(X)$ を $\zeta_N$ の $K$ 上の最小多項式とすれば

$$\begin{aligned}
\xi_{K,\ell}^{D_\ell} &= \prod_{j\in H}\prod_{i=0}^{\ell-2}(\zeta_N^j\zeta_\ell^{\rho^i}-1)^i \\
&\equiv \prod_{i=0}^{\ell-2}\prod_{j\in H}(\zeta_\ell^{-\rho^i}-\zeta_N^j)^i \pmod{K(\mu_r)^{\times d^2}} \\
&= \prod_{i=0}^{\ell-2} f(\zeta_\ell^{-\rho^i})^i
\end{aligned}$$

となり，よく知られているように，FFT を使えば，$f(\zeta_\ell^{-\rho^i})$ $(0 \le i \le \ell-2)$ は $O(\ell \log \ell)$ 時間で計算できる．巾は $i \bmod d^2$ でよいので，積にかかる時間は $O(\ell \log d^2)$ である．従って，$f(X)$ を高速に求めることができれば，$\xi_{K,\ell}^{D_\ell}$ は $O(\ell \log \ell)$ 時間で計算できる．

## 4. Examples

定理 2.5 を使ってみよう．$m \neq 1, 5$ を平方因子をもたない整数とする．$K = \mathbb{Q}(\sqrt{m}, \mu_5)$ は $\mathbb{Q}$ 上 8 次のアーベル拡大である．$\chi$ を $\mathbb{Q}(\sqrt{m})$ の指標，$\omega$ を $\mathbb{Q}(\zeta_5)$ の Teichmüller 指標とすると，$\Delta = G(K/\mathbb{Q})$ の指標群は $\{1, \omega, \omega^2, \omega^3, \chi, \chi\omega, \chi\omega^2, \chi\omega^3\}$ である．$\mathbb{Q}(\zeta_5)$ の類数は 1 だから $A_{K,\omega} = A_{K,\omega^2} = A_{K,\omega^3} = 0$ である．$\chi$ と $\chi\omega^2$ の固定体はそれぞれ $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{5m})$ であり，$\chi\omega$ と $\chi\omega^3$ の固定体は (唯一存在する) 4 次の巡回部分拡大である．

### 4.1. $p = 5$ の場合．

$A_K = A_{K,\chi} \oplus A_{K,\chi\omega} \oplus A_{K,\chi\omega^2} \oplus A_{K,\chi\omega^3}$ であり，任意の $\psi \in \widehat{\Delta}$ に対し $\mathcal{O}_\psi = \mathbb{Z}_5$ である．

例 4.1. $m = 1111, \psi = \chi\omega$ とする．$\psi$ は奇指標であり $N = 22220$．$B_{1,\psi^{-1}}$ の計算により $|A_{K,\psi}| = 5^2$．$\ell \equiv 1 \pmod N$ をみたす素数は $133321, 177761, 266641, 444401$.....．$L = \{\ell\}$ をいくつか試して $|\mathcal{M}_{L,L^*}| < 5^2$ であるので，$A_{K,\psi}$ は巡回群ではなさそうである．そこで $L = \{133321, 177761\}$, $L^* = \{126383489885716801, 221171107300004401\}$ をとると

$$N = \begin{pmatrix} 0 & 5 \\ 20 & 0 \end{pmatrix} \sim \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$$

となり，$|\mathcal{M}_{L,L^*}| = 5^2$．従って定理 2.5 より $A_{K,\psi} \simeq \mathcal{M}_{L,L^*} \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

例 4.2. $m = 36227, \psi = \chi\omega^3$ とする．$\psi$ は奇指標であり $N = 724540$．$B_{1,\psi^{-1}}$ の計算により $|A_{K,\chi\omega}| = 5^3$．$\ell \equiv 1 \pmod N$ をみたす素数は $5075561, 7250801, 11601281$.....．$L = \{5075561\}$ とする．$L^* = \{551617045041001\}$ に対しては $|\mathcal{M}_{L,L^*}| = 5^2$ であるが，$L^* = \{1287106438429001\}$ に対しては $|\mathcal{M}_{L,L^*}| = 5^3$．従って定理 2.5 より $A_{K,\psi} \simeq \mathcal{M}_{L,L^*} \simeq \mathbb{Z}/5^3\mathbb{Z}$.

例 4.3. $m = 36293, \psi = \chi\omega^3$ とする．$\psi$ は奇指標であり $N = 181465$．$B_{1,\psi^{-1}}$ の計算により $|A_{K,\chi\omega}| = 5^2$．$\ell \equiv 1 \pmod N$ をみたす素数は $725861, 1814651, 3266371$.....．$L = \{725861\}$ とする．$L^* = \{10537469309201\}$ に対しては $|\mathcal{M}_{L,L^*}| = 5$，$L^* = \{18440571291101\}$ に対しては $|\mathcal{M}_{L,L^*}| = 1$．この様子から $\ell = 725861$ の上の素イデアルは $A_{K,\chi}$ を生成していないようであり，他の素数が必要である．巡回群ではないかもしれないが，とりあえず $L = \{1814651\}$, $L^* = \{39515477245801\}$ としてみると $|\mathcal{M}_{L,L^*}| = 5^2$．従って定理 2.5 より $A_{K,\psi} \simeq \mathcal{M}_{L,L^*} \simeq \mathbb{Z}/5^2\mathbb{Z}$.

例 4.4. $m = -14606, \psi = \chi\omega$ とする．$\psi$ は偶指標であり $N = 292120$．$\ell = 11251$ に対し補題 2.3 を使うと $|A_{K,\psi}| \le 5^2$ が得られる．他の $\ell$ を使っても $|A_{K,\psi}|$ の上限はこれ以上下がらないので $d = 5^2$ とする．$\ell \equiv 1 \pmod{5^2}$ および (4), (5), (6) をみたす素数は $11251, 22501, 26251, 37501, 47501$.....．この場合も $L = \{\ell\}$ では $|\mathcal{M}_{L,L^*}| < 5^2$ であるので，$L = \{11251, 22501\}$, $L^* = \{68683602020243950 01, 136627676697066700 01\}$ とする．$L^*$ は (13) をみたしている．この時

$$N = \begin{pmatrix} 15 & 15 \\ 0 & 15 \end{pmatrix} \sim \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$$

となり，$|\mathcal{M}_{L,L^*}| = 5^2$．従って定理 2.5 より $A_{K,\psi} \simeq \mathcal{M}_{L,L^*} \simeq \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$.

Table 1 に他のいくつかの例を示す．例えば $(5,5)$ は $\mathbb{Z}/5\mathbb{Z}\oplus\mathbb{Z}/5\mathbb{Z}$ を意味する．

Table 1

| $m$ | $A_{K,\chi}$ | $A_{K,\chi\omega}$ | $A_{K,\chi\omega^2}$ | $A_{K,\chi\omega^3}$ |
|---|---|---|---|---|
| 1111 | $(5)$ | $(5,5)$ | 0 | 0 |
| 7523 | 0 | 0 | $(5)$ | $(5^2,5)$ |
| 36227 | 0 | 0 | 0 | $(5^3)$ |
| 36293 | 0 | 0 | 0 | $(5^2)$ |
| 36322 | $(5)$ | $(5^3,5)$ | 0 | 0 |
| 42853 | $(5)$ | $(5^3,5)$ | 0 | $(5)$ |
| −5657 | 0 | 0 | $(5,5)$ | $(5^2)$ |
| −14606 | $(5,5)$ | $(5,5)$ | 0 | 0 |

4.2. $p=3$ **の場合.** $\chi\omega^3$ は $\chi\omega$ の共役であるから，$A_K=A_{K,\chi}\oplus A_{K,\chi\omega}\oplus A_{K,\chi\omega^2}$. 更に $\mathcal{O}_\chi=\mathcal{O}_{\chi\omega^2}=\mathbb{Z}_5$, $\mathcal{O}_{\chi\omega}=\mathbb{Z}[\zeta_4]$ である．

例 4.5. $m=15338$, $\psi=\chi\omega$ とする．$\psi$ は奇指標であり $N=306760$. $B_{1,\psi^{-1}}$ の計算より $|A_{K,\psi}|=3^4$. $L=\{920281,1840561\}$, $L^*=\{539392008975136984557158 41,$ $612945464744473846087680 01,907159287821821292209766 41,$ $129944438525828455370588161\}$ を選ぶと

$$N=\begin{pmatrix}0&6&3&0\\3&6&3&6\\3&0&6&6\\0&3&3&6\end{pmatrix}\sim\begin{pmatrix}3&0&0&0\\0&3&0&0\\0&0&3&0\\0&0&0&3\end{pmatrix}$$

となり $|\mathcal{M}_{L,L^*}|=5^4$. 従って定理 2.5 よりアーベル群として $A_{K,\psi}\simeq\mathcal{M}_{L,L^*}\simeq\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$. $\mathcal{O}_\psi$-加群としては $A_{K,\psi}\simeq\mathcal{O}_\psi/3\mathcal{O}_\psi\oplus\mathcal{O}_\psi/3\mathcal{O}_\psi$ である．

他の例を Table 2 にあげる．

Table 2

| $m$ | $A_{K,\chi}$ | $A_{K,\chi\omega}$ | $A_{K,\chi\omega^2}$ | $A_{K,\chi\omega}$ as $\mathcal{O}=\mathcal{O}_{\chi\omega}$-modlue |
|---|---|---|---|---|
| 853 | 0 | $(3^2,3^2)$ | 0 | $\mathcal{O}/3^2$ |
| 9546 | 0 | $(3^3,3^3)$ | 0 | $\mathcal{O}/3^3$ |
| 11703 | 0 | $(3^3,3^3)$ | 0 | $\mathcal{O}/3^3$ |
| 13767 | $(3)$ | $(3^3,3^3)$ | $(3)$ | $\mathcal{O}/3^3$ |
| 13894 | 0 | $(3^3,3^3)$ | $(3^2)$ | $\mathcal{O}/3^3$ |
| 15338 | 0 | $(3,3,3,3)$ | $(3)$ | $\mathcal{O}/3\oplus\mathcal{O}/3$ |

4.3. **計算時間.** 任意の有限次代数体 $F$ のイデアル類群 $Cl_F$ を計算するアルゴリズムがいくつかのソフトウェアパッケージに実装されている．一方我々のアルゴリズムは有限次アーベル体 $F$ と $F$ の次数 $[F:\mathbb{Q}]$ を割らない奇素数 $p$ に対し，類群の $p$-part $Cl_F\{p\}$ を計算する．適用できる状況は制限されているが，その代わり計算速度の面でメリットがある．また類群の $p$-part の振舞いを研究する岩澤理論においても有用であると思われる．

例えば，類群を計算するのに使われる代表的なソフト PARI では，計算速度を調節するために類群の生成元を捜す上限を指定できる．何も指示しない時 (A) は経験的に十分であると思われる上限が使われ，経験的に正しい結果を与える．GRH を仮定した時の理論的な上限を使うと (B)，GRH の下で正しい結果を与える．GRH を仮

定しなくても十分である理論的な上限を使うと (C)，厳密に正しい結果を与える．一方我々のアルゴリズム (D) は GRH を必要とせず，$Cl_F\{p\}$ を厳密に求める．Table 3 は Alpha 21264 667MHz (メモリーは 4GB) を使った時の計算時間である．$*$ の部分では PARI は segmentaion fault をおこし途中で止まった．

Table 3

| $m$ | (A) | (B) | (C) | (D) |
|---|---|---|---|---|
| 1111 | 26s | 1h20m | 1h33m | 24s |
| 7523 | 3m6s | 3h30m | 31h10m | 7m22s |
| 36227 | 2m51s | 5h45m | $*$ | 10m30s |
| 36293 | 1m28s | 5h49m | $*$ | 2m54s |
| 36322 | 6m13s | 6h30m | $*$ | 29m28s |
| 42853 | 4m31s | 3h59m | $*$ | 8m47s |
| $-5657$ | 1m35s | 3h24m | 11h | 24m33s |
| $-14606$ | 4m15s | 4h6m | $*$ | 6h42m |

## References

[1] D. E. Knuth, The Art of Computer Programming vol.2, 1998, Addison-Wesley
[2] V.Kolyvagin, Euler systems, in The Grothendieck Festschrift II, Prog.Math.**87** 435-483 (1990)
[3] K.Rubin, The main conjecture, Appendix to Cyclotomic Fields I and II (S.Lang), Springer-Verlag, Berlin/New York, 1990.
[4] H.Sumida, Computation of the Iwasawa invariants of certain real abelian fields, Journal of Number Theory **105** 235–250 (2004).
[5] F.Thaine, On the ideal class groups of real abelian number fields, Ann. of Math. **128** 1-18 (1988).
[6] L.Washington, Introduction to Cyclotomic Fields, 2nd ed., Graduate Texts in Mathematics, Vol.83, Springer-Verlag, Berlin/New York, 1997.

Department of Mathematics, Tokyo Metropolitan University, Minami-Ohsawa, Hachioji, Tokyo, Japan
*E-mail address*: maoki@comp.metro-u.ac.jp

Department of Mathematics, College of Industrial Technology, Nihon University, 2-11-1 Shin-ei, Narashino, Chiba, Japan
*E-mail address*: fukuda@math.cit.nihon-u.ac.jp