

$\mathbb{Q}(\sqrt[3]{m})$ の類群の 3-rank を計算するアルゴリズム

都立大理 小林新樹

以下の結果は、東大紀要 21(1974), 263-270 に出ているので詳しくは、そちらを見て頂きたい。

k を有限次代数体、 C_k をその ideal 類群とすると、

$$d^{(3)}C_k = \dim_{\mathbb{F}_3} (C_k / C_k^3)$$

とおく。目標は、立方因子を含まない有理整数 m に対して

$$\Omega = \mathbb{Q}(\sqrt[3]{m})$$

としたとき、 $d^{(3)}C_\Omega$ を計算するためのアルゴリズムを求めること。ここで、 m が $p \neq \pm 1 \pmod{9}$ なる素因子 p を少なくも 1 個含めば、実際に実行できるものである。

I $k = \mathbb{Q}(\sqrt{-3})$, $K = k(\sqrt[3]{m})$ とし、 $\tilde{\Omega}$, $\tilde{K}$ をそれぞれ、 C_Ω^3 および C_K^3 に対応する Ω および K 上の類体とする。その時、次数の関係から、 $d^{(3)}C_\Omega = [\tilde{\Omega} : \Omega] = [\tilde{\Omega}K : K]$ で、 $G(\tilde{K}/\tilde{\Omega}K)$ は $G(\tilde{K}/\Omega)$ の交換子群であることがわかるから、それを計算すれば

はよい。ところで τ を複素共役とすれば、 τ は $\rho \mapsto \tau \rho \tau^{-1}$ により、 $G(R/K)$ 上に作用し、これに関して $G(R/\Omega) = G(R/K)$ 。
 $\langle \tau \rangle$ (半直積) となっている。更に $G(\tilde{R}/K)$ は $\mathbb{F}_3$ 上の線型空間
 同になっているので、次のことがわかる。

$G(\tilde{R}/K)$ の勝手な基底に関する τ の作用の表現を X と
 すれば、 $d^{(3)}\zeta_\Omega$ は、 X の固有値の中で、1 の重複度に
 等しい。

Ⅱ よって問題は、 $G(R/K)$ の適当な基底を見つけることに
 帰着される。

① $G(K/k) = \langle \sigma \rangle$ としたとき、 $G_K^{1-\sigma}$ に対応する K 上の
 類体を K_1 とおけば、 $K_1 \subset R$ で、 $G(R/K_1)$ は $G(R/K)$ の τ -不変
 な部分空間である。従って、上述の 1 の重複度は、 $G(R/K_1)$
 上、および $G(R/K)/G(R/K_1) = G(K_1/K)$ 上のそれらの和となる。
 ここで $G(K_1/K)$ 上の重複度は、I におけると同様の意味で、
 Fröhlich の意味での、 Ω 上の genus field に対応して、

$$\# \{ p | m \mid p \equiv 1 \pmod{3} \}$$

に等しいことが知られている。

② 残るのは $G(R/K_1)$ 上での τ の表現である。そのために、
 次の二つの事実に注意する。

(i) $G(R/K_1)$ は $G(R/k)$ の交換子群であって、その中

いに含まれる。従って $[x, y]$ は $G(\tilde{K}/k)$ の中で *balin.* である。その値は $G(\tilde{K}/k)/G(\tilde{K}/K_1) = G(K_1/k)$ における x, y の剰余類にしかよらない。

(12). $f = f(K/k)$ (導手) の各素因子 p に対して $G(K_1/k)$ におけるその惰性群の生成元を σ_p とし、その $\tilde{K}$ への延長をも、同じ文字で表わすことにする。そのとき、 $G(\tilde{K}/k)$ は $\{\sigma_p \mid p \mid f\}$ で、 $G(\tilde{K}/K_1)$ は $\{[\sigma_p, \sigma_q] \mid p, q \mid f\}$ で生成される。

特に (1) によれば、 $\tau[\sigma_p, \sigma_q]\tau^{-1}$ を知るためには、 $\tau\sigma_p\tau^{-1}$ 等を $G(K_1/k)$ の中で知ればよいことがわかる。あとで見るように、常に $\tau\sigma_p\tau^{-1} = \sigma_{\tau p}^{-1}$ となるように σ_p を選ぶことができるから、結局、 $[\sigma_p, \sigma_q]$ の形の元の間の一次関係をすべて求めることができるわけである。

III 上の (1), (12) は Kummer 拡大 K/k の生成元が有理数であることには依存してないので、以下

$$K = k(\sqrt[3]{\alpha}), \quad \alpha \in k^\times$$

として考える。 $f = f(K/k)$ の素因子を $p_1, \dots, p_t$ とし、 $\sigma_i = \sigma_{p_i} \in G(\tilde{K}/k)$ を (12) のようにとる。 $\zeta = \zeta_3$ (1 の原始 3 乗根) を一つ固定したとき、 $\sigma_i \sqrt[3]{\alpha} = \zeta^i \sqrt[3]{\alpha}$ であるとしてよく、特に、

$$(*) \quad \prod_{i=1}^t \sigma_i^{a_i} \in G(\tilde{K}/K) \iff \sum_{i=1}^t a_i \equiv 0 \pmod{3}$$

が成立つ。従って、 $[\sigma_i, \sigma_j] = [\sigma_i, \sigma_h][\sigma_h, \sigma_j]$ となる。結局、 $\{[\sigma_i, \sigma_j] \mid i=2, \dots, t\}$ の間の一次関係を求めればよい。

III_a. $[x, y]$ の bilinearity より、

$$\prod_{i=2}^t [\sigma_i, \sigma_i]^{a_i} = [\sigma_1, \sigma_1^{-a_1} \prod_{i=2}^t \sigma_i^{a_i}] \quad , \quad a_1 = -\sum_{i=2}^t a_i$$

となるので、上の (*) により、 $\sigma_1^{-a_1} \prod_{i=2}^t \sigma_i^{a_i} \in G(\hat{K}/K)$ 、従って、

$$\sigma_1^{-a_1} \prod_{i=2}^t \sigma_i^{a_i} = \left(\frac{R/K}{c} \right) \quad , \quad \exists c \in C_K.$$

と書ける。ここで R は $C_K^3 = C_K^{(1-\sigma_1)^2}$ により生成されるので、

上の交換子を計算して、

$$\prod_{i=2}^t [\sigma_i, \sigma_i]^{a_i} = 1 \iff c \in C_K^{1-\sigma_1} C_K^G.$$

ここで $\mathcal{P}_i$ の K における因子を $\mathcal{P}_i$ とすれば、 C_K^G は $\mathcal{P}_1, \dots, \mathcal{P}_t$ で生成される。そうであるならば、あと 1 つ class を追加すればよく、そのときは、追加する class より 1 つ ideal をとって $\mathcal{P}_{t+1}$ とおく。 $\mathcal{P}_{t+1} = N_{K/k}(\mathcal{P}_{t+1})$ とおく。そうした場合、上の $c \in C_K$ より 1 つ ideal $\mathcal{U}$ をとれば、

$$c \in C_K^{1-\sigma_1} C_K^G \iff \mathcal{U} = \mathcal{O}^{1-\sigma_1} \prod_j \mathcal{P}_j^{z_j}(\gamma) \quad , \quad \exists \mathcal{O}: K \text{ の ideal} \\ \exists \gamma \in K^\times, \exists (z_j).$$

$$\iff N_{K/k}(\mathcal{U}) = \prod_j \mathcal{P}_j^{z_j} (N_{K/k}(\gamma)) \quad , \quad \exists \gamma \in K^\times, \exists (z_j).$$

$$\iff \beta = \zeta^w \prod_j \pi_j^{z_j} N_{K/k}(\gamma) \quad , \quad \exists \gamma \in K^\times, \exists (w, z_j)$$

ここで π_j, β は $\mathcal{P}_j, N_{K/k}(\mathcal{U})$ の k における勝手な生成元である。従って Hasse の norm 定理を使えば、

$$\prod_{i=2}^t [\sigma_i, \sigma_i]^{q_i} = 1 \iff \left(\frac{\zeta, \alpha}{f}\right)^w \prod_j \left(\frac{\pi_j, \alpha}{f}\right)^{z_j} = \left(\frac{\beta, \alpha}{f}\right), \text{ for } k$$

なる連立方程式が (w, τ_j) なる解を持つ。

但し、実際は、両辺とも、 $f \nmid f$ ならば 1 に等しく、方程式は $f \mid f$ に対するものなりである。

III₆. あとは、各 $(a_2, \dots, a_t)$ に対して $\left(\frac{\beta, \alpha}{f}\right)$ を求めればよい。まず、

$$\sigma_1^{-a_1} \prod \sigma_i^{a_i} = \left(\frac{K/K}{\mathcal{O}}\right)$$

となる K の ideal $\mathcal{O}$ を探るのであるが、 $[\sigma_1, *] = 1$ を見るのであるから、II の (1) により、この両辺が $G(K_1/k)$ で等しくなる。即ち、

$$\sigma_1^{-a_1} \prod \sigma_i^{a_i} = \left(\frac{K_1/K}{\mathcal{O}}\right) = \left(\frac{K_1/k}{N_{K/k}(\mathcal{O})}\right) \text{ on } K_1$$

となる $\mathcal{O}$ を探せばよい。今、 $f_1 = f(K_1/k)$ とおいたとき、 $\beta_i \in K^\times$ を、

$$\beta_i \neq 0 \pmod{p_i}, \quad \beta_i \equiv 1 \pmod{f_1^{(p_i)}}, \quad \left(\frac{\beta_i, \alpha}{f_i}\right) = \zeta.$$

なる元とすれば、 $\left(\frac{\beta_i, K_1/k}{f_i}\right)$ は $G(K_1/k)$ における p_i の inertia 群の元で、

$$\left(\frac{\beta_i, K_1/k}{f_i}\right)^{\sqrt[3]{\alpha}} = \zeta^{\sqrt[3]{\alpha}}$$

となる。従って、 $\left(\frac{\beta_i, K_1/k}{f_i}\right) = \left(\frac{K_1/k}{(f_i)}\right)$ は III の初めに選んだ σ_i に等しく、よって、

$$\sigma_1^{-a_1} \prod \sigma_i^{a_i} = \left(\frac{K_1/k}{(\beta_1^{-a_1} \prod \beta_i^{a_i})} \right) \text{ on } K_1.$$

故に、上のようは U_K に対し

$$N_{K/k}(U) \sim (\beta_1^{-a_1} \prod \beta_i^{a_i}) \pmod{f_1}.$$

従って β を適当に選べば、

$$\beta = \beta_1^{-a_1} \prod_{i=2}^t \beta_i^{a_i} \pmod{f_1}.$$

$f \nmid f_1$ であるから、結局、各 $(a_2, \dots, a_t)$ に対し、

$$\prod_{i=2}^t [\sigma_1, \sigma_i]^{a_i} = 1$$

$$\Leftrightarrow \left(\frac{\zeta, \alpha}{f} \right)^w \prod_j \left(\frac{\pi_j, \alpha}{f} \right)^{x_j} = \begin{cases} \zeta^{-a_1}, & j = p_1, a_1 = \sum_{i=2}^t a_i \\ \zeta^{a_i}, & j = p_2, \dots, p_t \end{cases}$$

なる連立方程式が (w, x_j) について解をもつ。

また、 $\alpha = m \in \mathbb{Z}$ のとき、 $T\sigma_j T^{-1} = \sigma_{Tj}^{-1}$ on K_1 とは
ることも、上の σ_i の表現から明らかである。