2012/09/22

1 $\mathbb{Q}(\sqrt{-1999})$ のイデアル類群

$\theta = (-1+\sqrt{-1999})/2$ とおくと,θ の最小多項式は $f(x) = x^2 + x + 500$ である. また $\mathbb{Z}_{\mathbb{Q}(\theta)} = \mathbb{Z}[\theta]$ であるため, 素イデアル分解は簡単である.(簡単のため $R := \mathbb{Z}[\theta]$ とする)
Minkowski Bound は

$$\sqrt{|D|}\left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} = \frac{2\sqrt{1999}}{\pi} \sim 28.463$$

であるから,Norm が 28 以下のイデアルについて調べれば十分である. (注:$p \geq 3$ のとき

$$x^2 + x + 500 \equiv 0 \pmod{p} \text{ の解が存在する} \iff \left(\frac{-1999}{p}\right) = 1 \text{ が成り立つ (証明略)}$$

という事実が利用できる) 例として,$p = 5$ のときを考える.

$$\left(\frac{-1999}{5}\right) = \left(\frac{4}{5}\right) = 1$$

より, 方程式

$$x^2 + x + 500 \equiv 0 \pmod{5}$$

は (有理整数の) 解をもつ. よって, 因数分解ができる ($x^2 + x + 500 \equiv x(x+1) \pmod{5}$).
これから,

$$(5) = (5, \theta)(5, \theta + 1)$$

がいえる. 同様にして,28 以下の有理素数の (R 上の) 分解を試みたところ, 次の 5 通りで (2 個以上の (R 上の) 素イデアルへの分解に) 成功した.

$$(2) = \mathfrak{p}_0\mathfrak{p}_1, (5) = \mathfrak{p}_2\mathfrak{p}_3, (11) = \mathfrak{p}_4\mathfrak{p}_5, (13) = \mathfrak{p}_6\mathfrak{p}_7, (23) = \mathfrak{p}_8\mathfrak{p}_9$$

ここで,$\mathfrak{p}_0, \cdots, \mathfrak{p}_9$ は以下のとおりである.

$$\begin{aligned}
\mathfrak{p}_0 &= (2, \theta) \\
\mathfrak{p}_1 &= (2, \theta + 1) \\
\mathfrak{p}_2 &= (5, \theta) \\
\mathfrak{p}_3 &= (5, \theta + 1) \\
\mathfrak{p}_4 &= (11, \theta - 2) \\
\mathfrak{p}_5 &= (11, \theta + 3) \\
\mathfrak{p}_6 &= (13, \theta + 5) \\
\mathfrak{p}_7 &= (13, \theta - 4) \\
\mathfrak{p}_8 &= (23, \theta + 14) \\
\mathfrak{p}_9 &= (23, \theta - 13)
\end{aligned}$$

ここで, この 10 個のイデアルの関係を調べるために $f(*)$ を計算する.(これをする理由は,

$$|f(t)| = |N_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta - t)| = N_{\text{ideal}}((\theta - t)\mathbb{Z}[\theta])$$

が成り立つからである.)
$N_{\mathrm{ideal}}(\theta R) = |f(0)| = 500 = 2^2 \cdot 5^3$ であり,

$$\theta \in \mathfrak{p}_0, \theta \notin \mathfrak{p}_1, \theta \in \mathfrak{p}_2, \theta \notin \mathfrak{p}_3$$

であるので,

$$\theta R = \mathfrak{p}_0^2 \mathfrak{p}_2^3$$

であることがわかる. 同様にして,

$$(\theta) = \mathfrak{p}_0^2 \mathfrak{p}_2^3 \quad (f(0) = 500 = 2^2 \cdot 5^3 \text{より}) \tag{1}$$
$$(\theta - 2) = \mathfrak{p}_0 \mathfrak{p}_4 \mathfrak{p}_8 \quad (f(2) = 50 = 2 \cdot 11 \cdot 23 \text{ より}) \tag{2}$$
$$(\theta - 3) = \mathfrak{p}_1^9 \quad (f(3) = 512 = 2^9 \text{より}) \tag{3}$$
$$(\theta - 4) = \mathfrak{p}_0^3 \mathfrak{p}_3 \mathfrak{p}_7 \quad (f(4) = 520 = 2^3 \cdot 5 \cdot 13 \text{ より}) \tag{4}$$
$$(\theta - 8) = \mathfrak{p}_0^2 \mathfrak{p}_5 \mathfrak{p}_6 \quad (f(8) = 572 = 2^2 \cdot 11 \cdot 13 \text{ より}) \tag{5}$$

以上から, 次のような関係式ができる.

$$\mathfrak{p}_0 \mathfrak{p}_1 \sim (1) \tag{6}$$
$$\mathfrak{p}_2 \mathfrak{p}_3 \sim (1) \tag{7}$$
$$\mathfrak{p}_4 \mathfrak{p}_5 \sim (1) \tag{8}$$
$$\mathfrak{p}_6 \mathfrak{p}_7 \sim (1) \tag{9}$$
$$\mathfrak{p}_8 \mathfrak{p}_9 \sim (1) \tag{10}$$
$$\mathfrak{p}_0^2 \mathfrak{p}_2^3 \sim (1) \tag{11}$$
$$\mathfrak{p}_0 \mathfrak{p}_4 \mathfrak{p}_8 \sim (1) \tag{12}$$
$$\mathfrak{p}_1^9 \sim (1) \tag{13}$$
$$\mathfrak{p}_0^3 \mathfrak{p}_3 \mathfrak{p}_7 \sim (1) \tag{14}$$
$$\mathfrak{p}_0^2 \mathfrak{p}_5 \mathfrak{p}_6 \sim (1) \tag{15}$$

これを解くと,

$$\mathfrak{p}_2^{27} \sim (1)$$
$$\mathfrak{p}_0 \sim \mathfrak{p}_2^{12}$$
$$\mathfrak{p}_1 \sim \mathfrak{p}_2^{15}$$
$$\mathfrak{p}_3 \sim \mathfrak{p}_2^{26}$$
$$\mathfrak{p}_4 \sim \mathfrak{p}_2^{5}$$
$$\mathfrak{p}_5 \sim \mathfrak{p}_2^{22}$$
$$\mathfrak{p}_6 \sim \mathfrak{p}_2^{8}$$
$$\mathfrak{p}_7 \sim \mathfrak{p}_2^{19}$$
$$\mathfrak{p}_8 \sim \mathfrak{p}_2^{10}$$
$$\mathfrak{p}_9 \sim \mathfrak{p}_2^{17}$$

よって,

$$\mathrm{Cl}(\mathbb{Q}(\theta)) \simeq \mathbb{Z}/27\mathbb{Z}$$

である.