Pr

$$\varepsilon := \frac{-1+2\sqrt[3]{2}+\sqrt[3]{4}}{3} + \frac{1-\sqrt[3]{2}+\sqrt[3]{4}}{3}\,\zeta_3 \in \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$$

K	r_1	r_2	r_1+r_2-1	W_K	$\mathcal{O}_K^\times$
$\mathbb{Q}(\sqrt{3})$	2	0	1	$\{\pm 1\}$	$\pm(2+\sqrt{3})^{\mathbb{Z}}$
$\mathbb{Q}(\sqrt{5})$	2	0	1	$\{\pm 1\}$	$\pm\left(\frac{1+\sqrt{5}}{2}\right)^{\mathbb{Z}}$
$\mathbb{Q}(\zeta_5)$	0	2	1	μ_{10}	$\mu_{10}\left(\frac{1+\sqrt{5}}{2}\right)^{\mathbb{Z}}$
$\mathbb{Q}(\sqrt[3]{2})$	1	1	1	$\{\pm 1\}$	$\pm(1+\sqrt[3]{2}+\sqrt[3]{4})^{\mathbb{Z}}$
$\mathbb{Q}(\sqrt[3]{6})$	1	1	1	$\{\pm 1\}$	$\pm(1-6\sqrt[3]{6}+3\sqrt[3]{36})^{\mathbb{Z}}$
$\mathbb{Q}(\sqrt[4]{2})$	2	1	2	$\{\pm 1\}$	$\pm(1+\sqrt[4]{2})^{\mathbb{Z}}(1+\sqrt{2})^{\mathbb{Z}}$
$\mathbb{Q}(\sqrt[3]{2}, \zeta_3)$	0	3	2	μ_6	$\mu_6\,\varepsilon^{\mathbb{Z}}\,\bar{\varepsilon}^{\mathbb{Z}}$
$\mathbb{Q}(\sqrt{2}, \sqrt{3})$	4	0	3	$\{\pm 1\}$	$\pm(1+\sqrt{2})^{\mathbb{Z}}(\sqrt{2}+\sqrt{3})^{\mathbb{Z}}\left(\frac{\sqrt{2}+\sqrt{6}}{2}\right)^{\mathbb{Z}}$

Pm

cl $O_K = ?$, $O_K^\times = ?$

$K = \mathbb{Q}(\alpha)$ (1)

$\alpha^3 + \alpha^2 + 5\alpha - 16 = 0$

$f(x) = x^3 + x^2 + 5x - 16$

n	$f(n)$
-10	$-2\cdot 3\cdot 7\cdot 23$
-9	-709
-8	$-2^3\cdot 3^2\cdot 7$
-7	$-3\cdot 5\cdot 23$
-6	$-2\cdot 113$
-5	$-3\cdot 47$
-4	$-2^2\cdot 3\cdot 7$
-3	-7^2
-2	$-2\cdot 3\cdot 5$
-1	$-3\cdot 7$

n	$f(n)$
0	-2^4
1	-3^2
2	$2\cdot 3$
3	$5\cdot 7$
4	$2^2\cdot 3\cdot 7$
5	$3\cdot 53$
6	$2\cdot 7\cdot 19$
7	$3\cdot 157$
8	$2^3\cdot 3\cdot 5^2$
9	839

$f(x)$ nie ma zer mod $11, 13, 17$
$\Longrightarrow f(x)$ nierozkł. w $\mathbb{Q}[x]$

$\Delta(f) = -R(f, f') = -3\cdot 23\cdot 127 \Longrightarrow$
wolny od $\square \Longrightarrow \Delta_K = -8763$
oraz $O = O_K = \mathbb{Z}[\alpha]$

$\Delta(f) < 0 \Longrightarrow f$ ma jeden pierw. rzeczywisty.

(2)

$\Rightarrow r_1 = r_2 = 1$ &

$$M_K = \frac{3!}{3^3}\,\frac{4}{\pi}\sqrt{8763} \approx 26.5$$

$\Rightarrow Cl\,O_K$ generowana przez ideały pierwsze o normie ≤ 25

Rozkładamy pO_K, $p \leq 23$ bez niektórych $p = 11, 13, 17$

$2O = \beta_2\beta_4 = (2,\alpha)(2,\alpha^2+\alpha+1)$

$3O = \beta_3^2\, q_3 = (3,\alpha+1)^2(3,\alpha-1)$

$5O = \beta_5\beta_{25} = (5,\alpha+2)(5,\beta_5)$

$7O = \beta_7\, q_7\, r_7 = (7,\alpha+1)(7,\alpha-3)(7,\alpha+3)$

$19O = \beta_{19}\beta_{361} = (19,\alpha-4)(19,\beta_{19})$

$23O = \beta_{23}^2\, q_{23} = (23,\alpha+7)^2(23,\alpha+$ [illegible]

β_5, β_{19} nie wyliczamy ich.

$Cl\,O_K = \langle [\beta_2], [\beta_3], [\beta_5], [\beta_{19}],$
$[\beta_{23}]$, dwa nad $7 \rangle$

(3)

Ćwiczenie

Niech p l. p. i $k \in \mathbb{Z}$.
Wtedy:
$\exists\, \mathfrak{p} \mid p$ taki, że $\mathfrak{p} \mid (k-\alpha)$

$\Longleftrightarrow \quad p \mid f(k)$ $\qquad \boxed{N_{K/\mathbb{Q}}(k-\alpha) = f(k)}$

J. taki $\mathfrak{p} \mid p$ istnieje, to
$$\mathfrak{p} = (p, k-\alpha) \ \& \ f(\mathfrak{p}/p) = \underline{1}$$
W szczególności istnieje co najwyżej jeden ideał pierwszy $\mathfrak{p}$ mod p taki, że $\mathfrak{p} \mid (k-\alpha)$

Dow

surjekcja $R = \mathbb{Z}[\alpha] \xrightarrow{\varphi} \mathbb{F}$
$\operatorname{char} \mathbb{F} = p$ (skończone ciało $\mathbb{F}$)
z jądrem
$$\ker \varphi \supset (k-\alpha)$$
prowadzi ~~do~~ $\alpha \longmapsto k \in \mathbb{F}_p \subset \mathbb{F}$
czyli jest jedn. określony i ma obraz $\mathbb{F}_p$.
Zatem $\exists\, \varphi : R = \mathbb{Z}[\alpha] \twoheadrightarrow \mathbb{F}_p$ z $\varphi(\alpha) = k$

$\Longleftrightarrow \quad f(k) \equiv 0 \mod p.$ $\quad \underline{\underline{\ }}$

Wartości $a=-7$ z tabeli dają zatem

$$(-7-\alpha)=\mathfrak{p}_3\mathfrak{p}_5\mathfrak{p}_{23}$$

co skreśla $\{\mathfrak{p}_{23}\}$ z listy generatorów $\mathrm{Cl}\,\mathcal{O}_K$

podobnie $k=6$ daje

$$(6-\alpha)=\mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{19}$$

co skreśla $\{\mathfrak{p}_{19}\}$

Ideały nad 7 skreślamy bo

$$(-1-\alpha)=\mathfrak{p}_3\mathfrak{p}_7$$

$$(3-\alpha)=\mathfrak{p}_5\mathfrak{q}_7$$

Ponadto relacja

$$(-2-\alpha)=\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_5$$

$$=\mathfrak{p}_2^3\mathfrak{p}_3\mathfrak{p}_5^2$$

co skreśla $\{\mathfrak{p}_5\}$

W końcu: $(2-\alpha)=\mathfrak{p}_2\mathfrak{p}_3$

$\Rightarrow \mathrm{Cl}\,\mathcal{O}_K=\langle\{\mathfrak{p}_2\}\rangle$

ale $(\alpha)=\mathfrak{p}_2^4$ czyli

$\#\,\mathrm{Cl}\,\mathcal{O}_K \mid 4.$

(22)

$\alpha = \sqrt[3]{11}$, $11^2 \not\equiv 1 \bmod 9$

Wn 6.5: $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

$\Delta_K = -3^3 11^2 \, \ell$

$M_K = \frac{3!}{3^3}\left(\frac{4}{\pi}\right)\sqrt{3^3 11^2} < 17$

$\Rightarrow$ rozważmy $p\mathcal{O}_K$

$p = 2, 3, 5, 7, 11, 13$

dla czyn. $\alpha(\mathcal{O}_K)$.

$$x^3 - 11 = \begin{cases} (x-1)(x^2+x+1) & \bmod 2 \\ (x+1)^3 & \bmod 3 \\ (x-1)(x^2+x+1) & \bmod 5 \\ x^3-4 & \bmod 7 \\ x^3 & \bmod 11 \\ x^3+2 & \bmod 13 \end{cases}$$

z tw. Kummera:

$(2) = \mathfrak{p}_2 \mathfrak{p}_2'$, $N\mathfrak{p}_2 = 2$

$(3) = \mathfrak{p}_3^3$

$(5) = \mathfrak{p}_5 \mathfrak{p}_5'$ $N\mathfrak{p}_5 = 5$

$(11) = \mathfrak{p}_{11}^3$ $\mathfrak{p}_{11} = (\alpha)$ główny

$\Rightarrow Cl\,\mathcal{O}_K$ gen. przez
$[\mathfrak{p}_2]$, $[\mathfrak{p}_3]$ & $[\mathfrak{p}_5]$.

Relacje w $Cl\,\mathcal{O}_K$ — ~~badacy~~ el. małej normy w $\mathcal{O}_K$.

$\forall_{t\in\mathbb{Q}}$ $\alpha - t$ ma wiel. min. $(x+t)^3 - 11 \Rightarrow N(\alpha - t) = -t^3 - 11$

Biorąc małe t dostajemy!

$(\alpha) = \mathfrak{p}_{11}$, $(\alpha - 1) = \mathfrak{p}_2\mathfrak{p}_5$

$(\alpha - 2) = \mathfrak{p}_3$

$(\alpha + 1) = \mathfrak{p}_2^2\mathfrak{p}_3$

$\Rightarrow [\mathfrak{p}_3] = 1$, $[\mathfrak{p}_5] = [\mathfrak{p}_2]^{-1}$, $[\mathfrak{p}_2]^2 = 1$

$$\Rightarrow Cl\,\mathcal{O}_K = \begin{cases} 1 & [\mathfrak{p}_2] = 1 \\ \cong \mathbb{Z}/2 & [\mathfrak{p}_2] \neq 1 \end{cases}$$

Trzeba rozstrz. czy $\mathfrak{p}_2$ główny.
W tym celu przyda się $\mathcal{O}_K^\times$.

<u>Zakładając ≠ 1 jedności</u>

$$\beta_3 = (\alpha - 2)$$

$$\beta_2^2 \beta_3 = (\alpha + 1)$$

$$\beta_2^2 = (\beta), \quad \beta \in O_K$$

$$(\beta)(\alpha - 2) = (\alpha + 1)$$

$$\Rightarrow \beta = \frac{\alpha + 1}{\alpha - 2} = \alpha^2 + 2\alpha + 5 \quad (ALI)$$

<u>Porażka</u>

$$(\beta)^2 = \beta_2^4 = (\alpha - 3) \text{ bo}$$

$$N(\alpha - 3) = 16 \text{ oraz}$$

$$(\alpha - 3) \nmid \beta_2^2 \beta_2' \quad \text{bo}$$

w pr. przypadku byłoby $2 \mid (\alpha - 3)$

Z tego wynika, że:

$$u = \frac{\beta^2}{\alpha - 3} = 18\alpha^2 + 40\alpha + 89 \quad (ALI) \approx 266{,}9889$$

$$\in O_K^\times$$

Niech ε j. podst. $\mathcal{O}_K$

<u>z zadania 7:</u>

$$\varepsilon > \sqrt[3]{\frac{3267-24}{4}} \approx 9{,}3437$$

$$\Rightarrow \varepsilon^2 > 87, \quad \varepsilon^3 > 815$$

$$\Rightarrow u = \varepsilon \text{ lub } u = \varepsilon^2$$

<u>Zał.</u> [nie wprost] $u = \varepsilon^2$

rozważmy:

$$\psi : \mathbb{Z}[\alpha] \longrightarrow \mathbb{Z}/5 = \mathbb{F}_5$$

$$\psi = \pi_{\beta_5}, \quad \beta_5 = (5, \alpha - 1)$$

$$\psi(\alpha) = 1, \qquad N\beta_5 = 5$$

$$\psi(u) = 2 \notin \mathbb{F}_5^{2} \quad ↯$$

$$(!)$$

czyli $u = \varepsilon$ & $\mathcal{O}_K^{\times} = \{\pm u^n\}$

Weźmy lepszy generator

$$v = \frac{1}{u} = -2\alpha^2 + 4\alpha + 1$$

β_2 nie jest główny

$\mathfrak{P}_2^2 = (\beta) = (\gamma^2)$ wcześniej

$\Rightarrow \pm \sigma^m \beta = \gamma^2$

B.z.o. $\underline{m \in \{0,1\}}$

$\Rightarrow$ co najmniej jedna z liczb: $\beta, -\beta, \sigma\beta, -\sigma\beta$ jest kwadratem w $\mathbb{Z}[\alpha]$

Wykluczamy to redukując do $\mathbb{F}_{19}$:

$(19) = \mathfrak{P}_{19}\mathfrak{P}'_{19}\mathfrak{P}''_{19}$ z tw. Kummera

$\sqrt[3]{11}$ modulo 19: $5, -3, -2$

Rozważmy:

$\varphi_1 : \mathbb{Z}[\alpha] \longrightarrow \mathbb{F}_{19}$

$\varphi_1(\alpha) = 5$ Łatwo dostajemy

$\Leftarrow$ $\left.\begin{array}{l}\varphi_1(\beta) = 2 \\ \varphi_1(\sigma\beta) = -1\end{array}\right\} \notin \mathbb{F}_{19}^2$

ale $\psi_1(-\beta), \psi_1(5\beta) \in \mathbb{F}_{19}^{2}$

<u>Wykluczamy</u> pozostałe przypadki

$$\psi_2 : \mathbb{Z}[\alpha] \longrightarrow \mathbb{F}_{19}$$

$$\psi_2(\alpha) = -2$$

Łatwo obliczamy:

$$\psi_2(-\beta) = -5 = 14$$

$$\psi_2(5\beta) = -1 = 18$$

<u>nie</u> są kwadratami w $\mathbb{F}_{19}$.

$\Longrightarrow \mathfrak{p}_2$ <u>nie</u> jest główny

& $Cl\,\mathcal{O}_K = \mathbb{Z}/2$.

$$\psi_1(\beta) = \psi_1(\alpha^2 + 2\alpha + 5)$$
$$= 5^2 + 2\cdot 5 + 5 = 2$$
$$\psi_1(\upsilon\beta) = \psi_1(\upsilon)\,\psi_1(\beta)$$
$$= \psi_1(\upsilon)\,\underline{2}$$
$$= \psi_1(-2\alpha^2 + 4\alpha + 1)\,\underline{2}$$
$$= (-2\cdot 5^2 + 4\cdot 5 + 1)\,2$$
$$\cancel{= -24\cdot 2 = -48}$$
$$= (-50 + 20 + 1)\,2$$
$$= -29\cdot 2 = -58 = \underline{\underline{-1}}$$

Ad 2

$K = \mathbb{Q}(\alpha)$, $x^3 + 10x + 1 = f(x)$

$f(\alpha) = 0$, $\alpha \in \mathbb{R}$

$\Delta = -4027$ l. pierwsza

$\Longrightarrow \mathcal{O}_K = \mathbb{Z}[\alpha]$.

Lemat 7:

$$\varepsilon > \sqrt[3]{\frac{4027-24}{4}} \simeq 10{,}002499\ldots$$

Ale $N_{K/\mathbb{Q}}(\alpha) = -1 \Longrightarrow \alpha \in \mathcal{O}_K^\times$

& $\beta := -\alpha^{-1} \simeq 10{,}00998$

$\Longrightarrow 1 < \beta < \varepsilon^2$

& podobnie jak w (1) sprawdzamy że $\varepsilon = \beta$.

Jedności podstawowe wykorzystujemy przy obliczeniu grupy klas

Pr 9 (Cassels: "Local fields")

$K = \mathbb{Q}(\sqrt[3]{11})$

$\mathcal{O}_K^\times = ?$, $\mathrm{Cl}\,\mathcal{O}_K = ?$