A note on the monogenity and the unit group

Tomokazu Kashio*

2021, March 11

Second meeting of Monogenity and power integral bases

†

*E-mail: kashio_tomokazu@ma.noda.tus.ac.jp

†Kashio-Sekigawa, The characterization of cyclic cubic fields with power integral bases (arXiv:1912.03103), to appear in Kodai Math. J.

Aim

- Gras (1973) provided a certain characterization of monogenic cyclic cubic fields. (next slide)
- Today: Provide an alternative proof (and something more).
- Focusing on **the first cohomology of the unit group**.
- Joint work with R. Sekigawa.

Gras' characterization of monogenic cyclic cubic fields

Theorem

Let K be a cyclic cubic field (that is, $Gal(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$). Then the following are equivalent.

1. K is monogenic.
2. There exists a unit $\theta \in \mathcal{O}_K^\times$ satisfying that

$$N(\theta) = 1, \quad Tr(\theta + \theta^{-1}) = -3, \quad \frac{Tr(\theta^2 - \theta^{-1})}{\sqrt{d_K}} \in \mathbb{N}^3 := \{n^3 \mid n \in \mathbb{N}\},$$

   where d_K is the discriminant of K.

Note that $d_K \in \mathbb{N}^2$ for any cyclic cubic field K.

Main result

Definition (Shanks' simplest cubic fields)

Let K_t be the splitting field of $f_t(x) = x^3 - tx^2 - (t+3)x - 1$ ($t \in \mathbb{Z}$).
K_t is called a **simplest cubic field**. Each K_t is a cyclic cubic field.

Theorem

A monogenic cyclic cubic field is a simplest cubic field K_t.

Problem

Which K_t is monogenic?

Theorem

K_t is monogenic (except for several t)

$$\Leftrightarrow \frac{\Delta_t}{\sqrt{d_K}} \in \mathbb{N}^3 \ (\Delta_t := t^2 + 3t + 9 = \sqrt{d_{f_t}})$$

$$\Leftrightarrow t \not\equiv 3, 21 \bmod 27 \text{ and } v_p(\Delta_t) \not\equiv 2 \bmod 3 \text{ for all } p \neq 3.$$

The last condition is easy to check.

Example (non-monogenic K_t $(-1 \leqq t \leqq 2000)$)

21,30,41,48,57,75,84,90,100,102,103,111,129,138,139,152,154,156,165,183,188,
192,201,204,210,219,235,237,246,250,264,269,271,273,291,299,300,318,327,335,
345,348,354,356,372,374,381,384,398,399,404,408,426,433,435,438,446,453,462,
480,482,489,495,507,515,516,531,534,543,544,561,565,570,573,577,580,588,593,
597,602,607,615,624,642,651,669,678,691,696,705,716,723,727,732,742,750,759,
776,777,786,789,804,813,825,831,838,840,844,858,867,874,876,885,887,894,912,
921,923,926,936,939,945,948,966,975,985,992,993,1002,1020,1021,1029,1034,
1047,1056,1070,1074,1080,1083,1096,1101,1110,1114,1119,1128,1132,1137,1155,
1164,1168,1181,1182,1191,1209,1210,1217,1218,1230,1236,1237,1245,1249,1263,
1265,1266,1269,1272,1279,1287,1290,1299,1317,1326,1328,1344,1353,1364,1371,
1377,1380,1398,1407,1413,1418,1425,1434,1452,1461,1462,1475,1479,1488,1497,
1506,1511,1515,1524,1533,1542,1560,1563,1569,1573,1587,1596,1609,1614,1621,
1622,1623,1641,1648,1650,1668,1671,1677,1695,1704,1707,1720,1722,1731,1743,
1749,1756,1758,1776,1785,1790,1803,1805,1812,1818,1830,1839,1854,1857,1866,
1867,1884,1893,1903,1911,1916,1920,1925,1938,1947,1952,1959,1965,1974,1992.

Proof for [monogenic $\Rightarrow$ simplest cubic field]

Let K be a cyclic cubic field. There exists a unique integral ideal $\mathfrak{C}_K$ satisfying $N\mathfrak{C}_K = \sqrt{d_K}$.

Assume K is monogenic, i.e., $\mathcal{O}_K = \mathbb{Z}[{}^\exists\gamma]$

$\Rightarrow$ $\mathfrak{C}_K = (\gamma - \gamma')$, where γ' is a conjugate of γ

$\because \mathcal{O}_K = \mathbb{Z}[\gamma]$ implies $d_K \sim ((\gamma-\gamma')(\gamma-\gamma'')(\gamma'-\gamma''))^2 \sim (\gamma-\gamma')^6$

$\Rightarrow$ ${}^\exists\theta \in \mathcal{O}_K^\times$ s.t. $1+\theta+\theta\theta' = 0$. More explicitly, $\theta := \frac{\gamma'-\gamma''}{\gamma-\gamma'} \in \mathcal{O}_K^\times$

$\because 1+\theta+\theta\theta' = 1 + \frac{\gamma'-\gamma''}{\gamma-\gamma'} + \frac{\gamma'-\gamma''}{\gamma-\gamma'}\frac{\gamma''-\gamma}{\gamma'-\gamma''} = \frac{\gamma-\gamma'+\gamma'-\gamma''+\gamma''-\gamma}{\gamma-\gamma'} = 0,$
$\mathfrak{C}_K$ is fixed by the conjugation by definition.

$\Rightarrow$ $K = K_t$ for the parameter $t := Tr(\theta)$

$$\because (x-\theta)(x-\theta')(x-\theta'') = x^3 - Tr(\theta)x^2 + Tr(\theta\theta')x - 1$$
$$= x^3 - tx^2 - (t+3)x - 1 = f_t(x).$$

i.e., K is a simplest cubic field

Need certain additional condition for the opposite direction because there are non-monogenic simplest cubic fields.

Theorem

K_t is monogenic (except for several t)

$\Leftrightarrow \frac{\Delta_t}{\sqrt{d_{K_t}}} \in \mathbb{N}^3 := \{n^3 \mid n \in \mathbb{N}\}$

$\Leftrightarrow t \not\equiv 3, 21 \bmod 27$, $v_p(\Delta_t) \not\equiv 2 \bmod 3$ for all $p \neq 3$.

The second equivalence easily follows since we can write d_{K_t} explicitly:

$$d_{K_t} = \begin{cases} \displaystyle\prod_{v_p(\Delta_t) \not\equiv 0 \bmod 3} p^2 & (3 \nmid t \text{ or } t \equiv 12 \bmod 27), \\ \displaystyle 3^4 \prod_{p \neq 3, v_p(\Delta_t) \not\equiv 0 \bmod 3} p^2 & (\text{otherwise}). \end{cases}$$

Provide a sketch of proof of the first equivalence.

Preparation

- K: a cyclic cubic field, $G := Gal(K/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.
- $P_K := \{(\alpha) \mid \alpha \in K^\times\}$: the group of principal fractional ideals of K

  $\Rightarrow 1 \to \mathcal{O}_K^\times \to K^\times \stackrel{\alpha \mapsto (\alpha)}{\to} P_K \to 1$, with actions by G

  $\Rightarrow \mathbb{Q}^\times \to P_K^G \to H^1(G, \mathcal{O}_K^\times) \to H^1(G, K^\times) \to \cdots 1$, $\because$ Hilbert 90.

  $\Rightarrow Coker[\mathbb{Q}^\times \to P_K^G] = P_K^G/P_\mathbb{Q} \cong H^1(G, \mathcal{O}_K^\times)$, $\overline{(\alpha)} \mapsto \overline{\frac{\alpha'}{\alpha}}$,

  $P_\mathbb{Q} = \mathrm{Image}[\mathbb{Q}^\times \to P_K^G]$: the group of fractional ideals of $\mathbb{Q}$.
- I_K: the group of fractional ideals of K

  $\Rightarrow I_K \stackrel{N}{\to} \mathbb{Q}^\times \twoheadrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$, its kernel $= P_\mathbb{Q}$

  $\Rightarrow I_K/P_\mathbb{Q} \hookrightarrow \mathbb{Q}^\times/(\mathbb{Q}^\times)^3$, $\bar{\mathfrak{a}} \mapsto \overline{N\mathfrak{a}}$.

$$\begin{array}{ccccccc} H^1(G, \mathcal{O}_K^\times) & \cong & P_K^G/P_\mathbb{Q} & \subset & I_K^G/P_\mathbb{Q} & \hookrightarrow & \mathbb{Q}^\times/(\mathbb{Q}^\times)^3 \\ \Cup & & \Cup & & \Cup & & \Cup \\ \overline{\frac{\alpha'}{\alpha}} & \leftarrow\!\shortmid & \overline{(\alpha)} & & \bar{\mathfrak{a}} & \mapsto & \overline{N\mathfrak{a}} \end{array}$$

Proof for $[\mathcal{O}_{K_t} = \mathbb{Z}[\gamma] \Rightarrow \frac{\Delta_t}{\sqrt{d_{K_t}}} \in \mathbb{N}^3]$

Let $K = K_t$, take $\mathfrak{C}_{K_t}$ satisfying $N\mathfrak{C}_{K_t} = \sqrt{d_{K_t}}$.

$$\begin{array}{ccccccc}
H^1(G, \mathcal{O}_{K_t}^\times) & \cong & P_{K_t}^G/P_\mathbb{Q} & \subset & I_{K_t}^G/P_\mathbb{Q} & \hookrightarrow & \mathbb{Q}^\times/(\mathbb{Q}^\times)^3, \\
\Cup & & \Cup & & \Cup & & \Cup \\
\overline{\theta} & \leftarrow\!\shortmid & \overline{(\gamma - \gamma')} & = & \overline{\mathfrak{C}_{K_t}} & \mapsto & \overline{\sqrt{d_{K_t}}} \\
\overline{\theta_t} & \leftarrow\!\shortmid & \overline{(\theta_t - \theta_t')} & \longmapsto & & & \overline{\sqrt{d_{f_t}}} = \overline{\Delta_t}
\end{array}$$

- Take a root θ_t of $f_t(x) = x^3 - tx^2 - (t+3)x - 1 = 0$.
- Assume $\mathcal{O}_{K_t} = \mathbb{Z}[\gamma] \Rightarrow \mathfrak{C}_{K_t} = (\gamma - \gamma')$, $\theta := \frac{\gamma' - \gamma''}{\gamma - \gamma'} \in \mathcal{O}_K^\times$
  $\Rightarrow [\theta] = [\theta_t] \in H^1(G, \mathcal{O}_{K_t}^\times)$ (strictly speaking, replace t if necessarily)
  Key point: a replacement of a generator $\mathfrak{C}_{K_t} = (\alpha) = (\alpha\epsilon)$
  does not change its class $\overline{\frac{\alpha'}{\alpha}} = \overline{\frac{\alpha'\epsilon'}{\alpha\epsilon}} \in H^1(G, \mathcal{O}_{K_t}^\times) = \frac{\{u \in \mathcal{O}_K^\times \mid N(u) = 1\}}{\{\frac{u'}{u} \mid u \in \mathcal{O}_K^\times\}}$

  $\Leftrightarrow \Delta_t \equiv \sqrt{d_{K_t}} \bmod (\mathbb{Q}^\times)^3$.

- Take a root θ_t of $f_t(x) = x^3 - tx^2 - (t+3)x - 1 = 0$.
- Assume $\mathcal{O}_{K_t} = \mathbb{Z}[\gamma] \Rightarrow \mathfrak{C}_{K_t} = (\gamma - \gamma')$, $\theta := \frac{\gamma' - \gamma''}{\gamma - \gamma'} \in \mathcal{O}_K^\times$
  $\Rightarrow [\theta] = [\theta_t] \in H^1(G, \mathcal{O}_{K_t}^\times)$ (strictly speaking, replace t if necessarily)
  Key point is: a replacement of a generator $\mathfrak{C}_{K_t} = (\alpha) = (\alpha\epsilon)$ does not change its class $\overline{\frac{\alpha'}{\alpha}} = \overline{\frac{\alpha'\epsilon'}{\alpha\epsilon}} \in H^1(G, \mathcal{O}_{K_t}^\times) = \frac{\{u \in \mathcal{O}_K^\times | N(u) = 1\}}{\{\frac{u'}{u} | u \in \mathcal{O}_K^\times\}}$

Lemma

Let K be a cyclic cubic field, assume $\mathfrak{C}_K = (\beta)$ is principle, put $u_\beta := \frac{\beta'}{\beta} \in \mathcal{O}_K^\times$. The following statements are equivalent.

1. ${}^\exists\alpha \in \mathcal{O}_K$ s.t. $\mathfrak{C}_K = (\alpha)$, $Tr(\alpha) = 0$.
2. ${}^\exists u \in \mathcal{O}_K^\times$ s.t. $1 + u + uu' = 0$, $\overline{u_\beta} = \overline{u} \in H^1(G, \mathcal{O}_K^\times)$.
3. ${}^\exists t$ s.t. $K = K_t$, $\overline{u_\beta} = \overline{\theta_t} \in H^1(G, \mathcal{O}_K^\times)$.

Lemma

Let K be a cyclic cubic field, assume $\mathfrak{C}_K = (\beta)$ is principle, put $u_\beta := \frac{\beta'}{\beta} \in \mathcal{O}_K^\times$. The following statements are equivalent.

1. ${}^\exists\alpha \in \mathcal{O}_K$ s.t. $\mathfrak{C}_K = (\alpha)$, $Tr(\alpha) = 0$.
2. ${}^\exists u \in \mathcal{O}_K^\times$ s.t. $1 + u + uu' = 0$, $\overline{u_\beta} = \overline{u} \in H^1(G, \mathcal{O}_K^\times)$.
3. ${}^\exists t$ s.t. $K = K_t$, $\overline{u_\beta} = \overline{\theta_t} \in H^1(G, \mathcal{O}_K^\times)$.

Proof.

[(i) ⇔ (ii)]. Write $\alpha := \beta\epsilon$ $(\epsilon \in \mathcal{O}_K^\times)$. Then we have

$$Tr(\alpha) = \beta\epsilon + (\beta\epsilon)' + (\beta\epsilon)'' = \beta\epsilon \left(1 + u_\beta \frac{\epsilon'}{\epsilon} + u_\beta \frac{\epsilon'}{\epsilon} \left(u_\beta \frac{\epsilon'}{\epsilon}\right)'\right).$$

In particular, $Tr(\alpha) = 0 \Leftrightarrow u := u_\beta \frac{\epsilon'}{\epsilon} \in \overline{u_\beta}$ satisfying $1 + u + uu' = 0$. [(ii) ⇐ (iii)] follows from $1 + \theta_t + \theta_t\theta_t' = 0$. [(ii) ⇒ (iii)] u is a root of

$$(x - u)(x - u')(x - u'') = x^3 - Tr(u)x^2 + Tr(uu')x - 1 = f_t(x)$$

for $t = Tr(u)$. That is, u is one of $\theta_t, \theta_t' = \theta_t \frac{\theta_t'}{\theta_t}, \theta_t'' = \theta_t \frac{(\theta_t'\theta_t)'}{\theta_t'\theta_t} \in \overline{\theta_t}$. □

Proof for $[\mathcal{O}_{K_t} = \mathbb{Z}[\gamma] \Leftarrow \frac{\Delta_t}{\sqrt{d_{K_t}}} \in \mathbb{N}^3]$

We explicitly show that

$$\gamma := \frac{\theta_t - a}{\sqrt[3]{\frac{\Delta_t}{\sqrt{d_{K_t}}}}} \text{ for } a \in \mathbb{Z} \text{ with } a \equiv \frac{t}{3} \bmod \sqrt[3]{\frac{\Delta_t}{\sqrt{d_{K_t}}}}$$

is a generator of PIB.

Relation to Gras' characterization

Theorem

Let K be cyclic cubic fields. Then the following are equivalent.

1. K is monogenic.
2. There exists a unit $\theta \in \mathcal{O}_K^\times$ satisfying that

   $N(\theta) = 1$, $Tr(\theta + \theta^{-1}) = -3$, $\frac{Tr(\theta^2 - \theta^{-1})}{\sqrt{d_K}} \in \mathbb{N}^3$.

$$N(\theta) = 1,\ Tr(\theta + \theta^{-1}) = -3$$

$\Rightarrow$ $Tr(\theta) + Tr(\theta\theta') + 3 = 0$

$\Rightarrow$ $(x - \theta)(x - \theta')(x - \theta'') = x^3 - Tr(\theta)x^2 + Tr(\theta\theta')x - 1 = f_t(x)$ with $t = Tr(\theta)$, i.e., $K = K_t$.

$\Rightarrow$ $Tr(\theta^2 - \theta^{-1}) = Tr(\theta)^2 - 3Tr(\theta\theta') = t^2 + 3t + 9 = \Delta_t$.

- A monogenic cyclic cubic field is a simplest cubic field K_t.
- K_t is monogenic $\Leftrightarrow$ $\frac{\Delta_t}{\sqrt{d_K}} \in \mathbb{N}^3$

$\Leftrightarrow t \not\equiv 3, 21 \bmod 27,\ v_p(\Delta_t) \not\equiv 2 \bmod 3\ (p \neq 3)$.

- I believe such arguments can be generalized to other situations.

  e.g., Next talk by Sekigawa.
- I am interested in other relations between the monogenity and the unit group.

  e.g., Sekigawa[‡] found that a kind of congruences of units imply non-monogenity:

  monogenity $\Leftrightarrow$ Diophantine equation(s)
  $\Rightarrow$ a unit equation, in some cases
  (equation in the form of $a_1u_1 + \cdots + a_ru_r = 0$ under $u_i \in \mathcal{O}_K^\times$)
  $\Rightarrow$ no solution because of certain congruence relations among units in several settings.

[‡] Relative power integral bases in certain ray class fields of an imaginary quadratic number field, preprint