The simplest cubic fields are non-isomorphic to each other

by

Ryotaro Okazaki

at

Doshisha University, Kyoto, Japan

email: rokazaki@dd.iij4u.or.jp

http: //www1.doshisha.ac.jp/~rokazaki/

The simplest cubic form

$$F_n(X,Y) = X^3 + (n-1)X^2Y - (n+2)XY^2 + Y^3, \quad (n \geq 0).$$

Shanks Units $\rho^{(1)} < \rho^{(2)} < \rho^{(3)}$: three real roots of $F_n(X,1)$.

The simplest cubic field :

$$K_n = \mathbf{Q}(\rho^{(1)}) = \mathbf{Q}(\rho^{(2)}) = \mathbf{Q}(\rho^{(3)}) \text{ of conductor } f(K_n).$$

Theorem 1. $(n \neq n'.)$

$$\begin{aligned} K_n = K_{n'} &\Longrightarrow n, n' \in \{0,1,2,3,4,6,13,55,67,1260,2390\} \\ &\Longrightarrow f(K_n) \leq 19. \end{aligned}$$

Remark

Here, $\mathbf{Z}[\rho^{(i)}]$ can be a suborder of the ring of integers of K_n.

Remark

$K_0 = K_6 = K_{13} = K_{1260}$; $K_1 = K_4 = K_{55}$; $K_2 = K_{67}$; $K_3 = K_{2390}$.

The representation number of a cubic form $F(X,Y)$:

$$\mathcal{R}(F) = \ \#\{(x,y) \in \mathbf{Z}^2 : F(x,y) = 1\}.$$

The automorphism group of F :

$$\mathrm{Aut}(F) = \{M \in GL_2(\mathbf{Z}) : F \circ M = F\} \simeq 1 \text{ or } \mathbf{Z}/3\mathbf{Z}.$$

Theorem 2.

$$\begin{aligned} \#\,\mathrm{Aut}(F) = 3 \ \&\ \mathcal{R}(F) > 3 \ &\Longrightarrow\ F \sim F_0, F_1 \text{ or } F_3 \\ &\Longrightarrow\ D(F) \in \{7^2, 9^2, 19^2\}. \end{aligned}$$

Previous Result Bennett (2001) :

$$\#\,\mathrm{Aut}(F) = 3 \Longrightarrow \mathcal{R}(F) \leq 9.$$

Remark Baulin (1960) $\mathcal{R}(F_0) = 9$; Ljunggren (1971) $\mathcal{R}(F_1) = 6$;
Gaál-Schuulte (1989) $\mathcal{R}(F_3) = 6$.

Problem. Does $n \longmapsto K_n$ nicely parametrizes all cyclic cubic fields.

injective? Almost Yes. (Theorem 1.)

surjective? No.

For $f_n = \sqrt{D(F_n)} \in \mathbf{Z}$, we have

$$f_n = n^2 + n + 7.$$

In particular,

$$f_n \equiv 1 \pmod{2},$$

which implies 2 never splits in K_n .

Note: ρ, ρ', ρ'' cannnot be incongruent modulo an ideal of norm 2.

Note: 2 splits in many cyclic cubic fields,

e.g. the one defined by $X^3 - 31X - 2 \times 31$.

Previous results on $\mathcal{R}(F)$ under $\#\,\mathsf{Aut}(F) = 3$.

Thomas 1990, Mignotte 1993.

$$n \geq 3 \Longrightarrow \mathcal{R}(F_n) = 3.$$

Bennett (2001). Nonvanishing of $\mathcal{R}$:

$G_n(X, Y) = (2n + 1)X^3 - (3n + 1)X^2 - (3n + 2)XY^2 + (2n + 1)Y^3.$

$$G_n(2, 1) = G(-1, 1) = G(-1, -2) = 0;$$

$$\mathcal{R}(G_n) \geq 3, \quad \#\,\mathsf{Aut}(G_n) = 3.$$

Since G_n and $F_{n'}$ are reduced, $G_n \not\sim F_{n'}$ unless $(n, n') = (0, 0)$. $(n \geq 0)$

Vanishing of $\mathcal{R}$:

$\mathcal{R}(mX^3 + nX^2Y - (n + 3m)XY^2 + mY^3) > 0 \Longrightarrow m \equiv 1 \pmod 2.$

Norm Form and Hessian.

Assume $\# \operatorname{Aut}(F) = 3$ and $\mathcal{R}(F) > 0$.

$$F(X,Y) = \textstyle\prod_{i=1}^{3} (\alpha^{(i)} X + \beta^{(i)} Y),$$

$$K(F) = \mathbf{Q}(\alpha, \beta), \quad \text{cyclic cubic field.}$$

$$K(F) \hookrightarrow \mathbf{R}^3, \quad \text{by} \quad \alpha \longmapsto \vec{\alpha} = (\alpha_i), \quad \beta \longmapsto \vec{\beta} = (\beta_i)$$

$$(\delta_i) = \vec{\delta} = \alpha \times \beta, \quad \text{invariant of} \quad \mathbf{Z}\alpha + \mathbf{Z}\beta.$$

$$\mathfrak{L}^{\natural}(F) = \mathbf{Z}\delta\alpha + \mathbf{Z}\delta\beta \quad \perp \vec{1}, \quad \text{invariant of} \quad F/\sim.$$

$$\operatorname{Aut}(\mathfrak{L}^{\natural}(F)) = \langle \sigma \rangle = \operatorname{Gal}(K(F)/\mathbf{Q}), \quad \sigma : (z_i) \in \mathbf{R}^3 \longmapsto (z_{i+1}) \in \mathbf{R}^3.$$

$$\delta^{1-\sigma} \in \mathfrak{O}(K(F))^{\times}$$

Note: $F(X,Y) = N(\delta)^{-1} \prod_{i=1}^{3} (\delta\alpha^{(i)} X + \delta\beta^{(i)} Y)$.

Connection of the two Theorems.

Assume $\#\,\mathrm{Aut}(F) = 3$ and $F(x,y) = 1$. Set

$$\varepsilon = x\alpha + y\beta \qquad \in \mathfrak{O}(K(F))^{\times}.$$

Consider

$$F_{[\delta\varepsilon]}(X,Y) = N(\delta)^{-1} \prod_{i=1}^{3} (((\delta\varepsilon)^{\sigma})^{(i)} X + (\delta\varepsilon)^{(i)} Y) = X^3 + \cdots + Y^3.$$

We have $\quad \#\,\mathrm{Aut}(F_{[\delta\varepsilon]}) = 3$.

Therefore, $(\exists n \geq 0) \quad F_n(X,Y) = F_{[\delta\varepsilon]}(X,Y)$ or $F_{[\delta\varepsilon]}(Y,X)$.

Remark : $\quad$ When $F = F_n$, we can recover $F_n = F_{[\delta\varepsilon]}$.

Theorem 1 now implies Theorem 2:

$$\mathcal{R}(F) \leq 3 \cdot \#\{n \geq 0 : K_n = K(F)\}.$$

Geometry of Representations on the Logarithmic Plane.

Assume $F = F_n$. Set $\varepsilon = 1$. ("$\varepsilon = x\alpha + y\beta$")

Define $$\log : (z_i) \in (\mathbf{R}^\times)^3 \longmapsto (\log|z_i|) \in \mathbf{R}^3.$$

Set $$\vec{u} = \vec{u}(n) = \log(N(\delta)^{-1/3}\, \vec{\delta}\, \vec{\varepsilon}).$$

Since $\delta^{1-\sigma} \in \mathfrak{O}(K(F))^\times$, we have

$$(1-\sigma)\vec{u} \in \mathfrak{E} = \log \mathfrak{O}(K(F))^\times.$$

Since $\vec{\delta}\, \vec{\varepsilon} \perp \vec{1}$, we have $\quad \vec{u} \in \mathcal{C}, \quad$ where

$$\mathcal{C} : e^{u_1} + e^{u_2} + e^{u_3} = 2 \max\{e^{u_1}, e^{u_2}, e^{u_3}\}.$$

WLOG. $u_1, u_2 > u_3$.

Set $s(\vec{u}) = (u_1 - u_2)/\sqrt{2} \doteq 0$, $t(\vec{u}) = -\sqrt{6}\, u_3/2 \doteq \|\vec{u}\|$.

Upper Bound.

Let ξ, η be a pair of fundamental unit of $K(F)$.

Since $(1-\sigma)\vec{u} \in \mathfrak{E} = \log \mathfrak{O}(K(F))^\times = \mathbf{Z}\log\xi + \mathbf{Z}\log\eta$,

we apply Laurent-Mignotte-Nesterenko (1995) to

$$|s| = |(u_1 - u_2)/\sqrt{2}| < \exp\left(-\sqrt{6}\,t/2\right)/\sqrt{2}.$$

We obtain

$$t \le 1.68 \cdot 10^4 \,\mathrm{disc}(\mathfrak{E}).$$

If $\vec{u}' \in \mathcal{C}$, $\vec{u}' \notin \{\vec{u}, \sigma\vec{u}, \sigma^2\vec{u}\}$, also satisfies $(1-\sigma)\vec{u}' \in \mathfrak{E}$, we have

$$t(\vec{u}') \ge \frac{\sqrt{2}/3 \cdot \mathrm{disc}(\mathfrak{E}) \exp\left(\sqrt{6}\,t/2\right)}{1 + \exp\left(-2(t(\vec{u}') - t)/\sqrt{6}\log 2\right)}$$

Hence, $t \le 8.56$, $\|\vec{u}\| \le 8.65$, $D(F) \le 40000^4$,

$f_n \le 40000^2$, $n \le 40000$.

The Rest is Continued Fraction on $\mathfrak{E}$.

Let $K_n = K_{n'}$ with $n' > n \geq 0$.

What we obtained is as follows: $n \leq 40000, \quad t' = t(\vec{u}(n')) \leq 10^7$.

We can now apply continued fraction algorithm to

$\mathfrak{E}$ of K_n along the t-axis up to $t \leq 10^7$.

We relax the condition on s' as

$$|s'| < \exp\left(-\sqrt{6}\, t'/2\right)/\sqrt{2} < \frac{\sqrt{2}}{(\sqrt{6}t'/2)^2} \cdot \frac{3.3\,\mathrm{disc}(\mathfrak{E})}{3}.$$

Search such s' to find 14 candidates.

Check the original condition to find 8 candidates.

The candidates satsify $\quad n \leq 3,\ t' \leq 7$.

Hence, $\quad f(K_n) \leq 19,\ n' \leq 40000$.

Pick up all $n' \leq 40000$ such that $f(K_n) \leq 19$ to establish Theorem 1.

Unit Group.

Let $F = F_n$. $(f(K_n) \neq 9)$ Then,

$$[\mathfrak{E} : \mathbf{Z} \log \rho + \mathbf{Z}\sigma \log \rho] \notin \{2, 3, 4, 5, 6\}.$$

Hence,

$$\frac{\operatorname{disc}(\mathbf{Z} \log \rho + \mathbf{Z}\sigma \log \rho)}{\frac{\sqrt{3}}{16} \log^2(f(K_n)^2/4)} < 7 \Longrightarrow \mathfrak{E} = \mathbf{Z} \log \rho + \mathbf{Z}\sigma \log \rho.$$

Within $n \leq 40000$,

$$(n, f(K_n), \text{ratio}) \in \begin{cases} (6, 7, 10.1), \quad (13, 7, 17.9), \quad (55, 9, 28.7), \\ (67, 13, 20.3), \ (1260, 7, 129.9), \ (1599, 373, 8.0), \\ (2390, 19, 47.8), \quad (7838, 1213, 7.8), \\ (12746, 1381, 8.7) \end{cases}$$

fail to satisfy the criteria. $f(K_n) \leq 19$ are handled by $f(K_0), ..., f(K_3)$.
In the three reamining cases, $\mathfrak{E} = \mathbf{Z} \log \rho + \mathbf{Z}\sigma \log \rho$ is shown by 7th-power residue symbol modulo suitable primes.

Determination of Unit Group.

Let b be the cube-free part of $f_n = n^2 + n + 7$ and $a = b/\prod_{9<p^2|b} p$.

Filling in the missing case of Washington (1987), we obtain

$$f(K_n) = \begin{cases} 9a & \text{if} \quad n \equiv 4, 22 \pmod{27}; \\ a & \text{otherwise.} \end{cases}$$

We also have

$$\mathrm{disc}(\mathbf{Z}\log\rho + \mathbf{Z}\sigma\log\rho) \le \sqrt{3}\cdot\log^2(n+1+4/(2n+1))$$

Therefore,

$$\frac{\mathrm{disc}(\mathbf{Z}\log\rho + \mathbf{Z}\sigma\log\rho)}{\frac{\sqrt{3}}{16}\log^2(f(K_n)^2/4)} < \frac{\log^2(n+1+4/(2n+1))}{\log^2(a^{1/2}/4)}\,.$$

Interesting Logarithmic Form.

$$n = 41, \quad F_n(X,Y) = X^3 + 40X^2Y - 43XY^2 + Y^3.$$

$$\rho^{(1)} = -41.0481\cdots,\ \rho^{(2)} = 0.0237823\cdots,\ \rho^{(3)} = 1.02436\cdots;$$

$$\Lambda = 3\log\rho^{(2)} + 466\log\rho^{(3)} = -8.9\cdots\times 10^{-8}.$$

$$h(\rho) \;=\; \frac{1}{6}\sum_{i=1}^{3}\Big|\log\Big|\rho^{(i)}\Big|\Big| = 1.24627\cdots.$$

$$B = \frac{3}{3h} + \frac{466}{3h} = 125.44\cdots.$$

$$\log|\Lambda| = -16.2317\cdots.$$

$$\frac{\log|\Lambda|}{3^4h^2\log^2 B} = 5.5526\cdots\times 10^{-3}.$$