JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **27**, No. 2, May 2014
http://dx.doi.org/10.14403/jcms.2014.27.2.205

GALOIS STRUCTURES OF DEFINING FIELDS OF FAMILIES OF ELLIPTIC CURVES WITH CYCLIC TORSION

Daeyeol Jeon*

Abstract. The author with C. H. Kim and Y. Lee constructed infinite families of elliptic curves over cubic number fields K with prescribed torsion groups which occur infinitely often. In this paper, we examine the Galois structures of such cubic number fields K for the families of elliptic curves with cyclic torsion.

1. Introduction

Over cubic number fields K, it is proved in [4] that all the group structures occurring infinitely often as torsion groups $E(K)_{\text{tors}}$ are exactly the following 38 types:

$$\begin{array}{ll} \mathbb{Z}/N_1\mathbb{Z}, & N_1 = 1-16, 18, 20 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z}, & N_2 = 1-7 \end{array} \tag{1.1}$$

where K varies over all cubic number fields and E varies over all elliptic curves over K. In [3] the author with C. H. Kim and Y. Lee construct infinite families of elliptic curves with torsion structures in Eq. (1.2) over cubic number fields K.

In this paper we examine the Galois structures of defining fields of the constructed infinite families of elliptic curves with cyclic torsion in [3]. For our purpose, it is sufficient to consider the families of elliptic curves with cyclic torsion groups which do not occur over $\mathbb{Q}$. That is, we consider the following groups

$$\mathbb{Z}/N\mathbb{Z}, \quad N = 11, 13, 14, 15, 16, 18, 20 \tag{1.2}$$

Received December 24, 2013; Accepted April 16, 2014.
2010 Mathematics Subject Classification: Primary 11G05; Secondary 11G18.
Key words and phrases: elliptic curve, torsion, cubic number field, modular curve.
The author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2010-0023942).

2. Preliminaries

The *Tate normal form* of an elliptic curve with $P = (0, 0)$ as follows:

$$E = E(b, c) : Y^2 + (1 - c)XY - bY = X^3 - bX^2,$$

and this is nonsingular if and only if $b \neq 0$. On the curve $E(b, c)$ we have the following by the chord-tangent method:

$$\begin{aligned} P &= (0,\ 0), \\ 2P &= (b,\ bc), \\ 3P &= (c,\ b - c), \\ 4P &= \big(r(r-1),\ r^2(c - r + 1)\big)\,; \quad b = cr, \\ 5P &= \big(rs(s-1),\ rs^2(r - s)\big)\,; \quad c = s(r-1), \\ 6P &= \left(\frac{s(r-1)(r-s)}{(s-1)^2},\ \frac{s^2(r-1)^2(rs - 2r + 1)}{(s-1)^3}\right). \end{aligned} \tag{2.1}$$

Very recently, by using the Tate normal form, Sutherland [5] found optimized forms for defining equations of the modular curves $X_1(N)$ for $N = 11, 13 - 50$.

In fact, the condition $NP = O$ in $E(b, c)$ gives a defining equation for $X_1(N)$. For example, $11P = O$ implies $5P = -6P$, so

$$x_{5P} = x_{-6P} = x_{6P},$$

where x_{nP} denotes the x-coordinate of the n-multiple nP of P. Eq. (2.1) implies that

$$rs(s-1) = \frac{s(r-1)(r-s)}{(s-1)^2}. \tag{2.2}$$

Without loss of generality, the cases $s = 1$ and $s = 0$ may be excluded. Then Eq. (2.2) becomes as follows:

$$r^2 - 4sr + 3s^2r - s^3r + s = 0,$$

which is one of the equation $X_1(11)$, called the *raw form* of $X_1(11)$. By the coordinate changes $s = 1 - x$ and $r = 1 + xy$, we get the following equation:

$$f(x, y) := y^2 + (x^2 + 1)y + x = 0.$$

In this case, b and c can be expressed by x and y as follows:

$$\begin{aligned} b &= -xy(x-1)(xy+1), \\ c &= -xy(x-1). \end{aligned}$$

TABLE 1. Families of elliptic curves $E(b_N, c_N)$ and polynomials $f_N(x,t)$.

N	$E(b_N, c_N)$ and $f_N(x,t)$
11	$E_{11}(t) := E(b_{11}, c_{11})$ with $\begin{cases} b_{11} = \frac{t(t+1)(\alpha_t+t)}{\alpha_t}, \\ c_{11} = \frac{t(\alpha_t+t)}{\alpha_t}, \end{cases}$ where α_t is a root of $f_{11}(x,t) = x^3 - x^2 - t^2 - t$.
13	$E_{13}(t) := E(b_{13}, c_{13})$ with $\begin{cases} b_{13} = \frac{\alpha_t^2(\alpha_t-1)(\alpha_t^3-\alpha_t+t)(\alpha_t^3-\alpha_t^2+t)}{t^2(\alpha_t^2-\alpha_t+t)}, \\ c_{13} = \frac{\alpha_t^2(\alpha_t-1)(\alpha_t^3-\alpha_t+t)}{t(\alpha_t^2-\alpha_t+t)}, \end{cases}$ where α_t is a root of $f_{13}(x,t) = tx^3 - (t+1)x^2 + x + t^2 - t$.
14	$E_{14}(t) := E(b_{14}, c_{14})$ with $\begin{cases} b_{14} = -\frac{8(3\alpha_t-t-4)(\alpha_t^2-2\alpha_t-2t+8)(\alpha_t^2+2\alpha_t-2t-8)}{(\alpha_t-4)^3(\alpha_t^2-2\alpha_t-2t-8)^2}, \\ c_{14} = -\frac{8(3\alpha_t-t-4)(\alpha_t^2+2\alpha_t-2t-8)}{\alpha_t(\alpha_t-4)^2(\alpha_t^2-2\alpha_t-2t-8)}, \end{cases}$ where α_t is a root of $f_{14}(x,t) = x^3 + x^2 - 8x - t^2 + 16$.
15	$E_{15}(t) := E(b_{15}, c_{15})$ with $\begin{cases} b_{15} = -\frac{\alpha_t(\alpha_t^3+t\alpha_t^2-t\alpha_t-t^2)(\alpha_t^3+t\alpha_t^2-t^2)}{(\alpha_t^2+\alpha_t-t)(\alpha_t^3+\alpha_t^2+t\alpha_t^2+t\alpha_t-t^2)^2}, \\ c_{15} = -\frac{\alpha_t(\alpha_t^3+t\alpha_t^2-t\alpha_t-t^2)}{(\alpha_t^2+\alpha_t-t)(\alpha_t^3+\alpha_t^2+t\alpha_t^2+t\alpha_t-t^2)}, \end{cases}$ where α_t is a root of $f_{15}(x,t) = x^3 + x^2 - tx - t^2 - t$.
16	$E_{16}(t) := E(b_{16}, c_{16})$ with $\begin{cases} b_{16} = \frac{t(t-1)\alpha_t(\alpha_t-t)(t^2\alpha_t+\alpha_t-t)}{(t\alpha_t+\alpha_t-t)^3}, \\ c_{16} = \frac{t(t-1)\alpha_t(\alpha_t-t)}{(t\alpha_t+\alpha_t-t)^2}, \end{cases}$ where α_t is a root of $f_{16}(x,t) = 2t^2x^3 + (-2t^2+2t-1)x^2 + (-t^2+1)x + t^2 - t$.
18	$E_{18}(t) := E(b_{18}, c_{18})$ with $\begin{cases} b_{18} = -\frac{t(\alpha_t-t)(\alpha_t^2+t)(\alpha_t^2-t\alpha_t+t)}{(\alpha_t^2-t^2+t)(\alpha_t^2+t\alpha_t-t^2+t)^2}, \\ c_{18} = -\frac{t(\alpha_t-t)(\alpha_t^2-t\alpha_t+t)}{(\alpha_t^2-t^2+t)(\alpha_t^2+t\alpha_t-t^2+t)}, \end{cases}$ where α_t is a root of $f_{18}(x,t) = (-t+1)x^3 + (t^2-1)x^2 + (-2t^2+t)x + t^2 - t$.
20	$E_{20}(t) := E(b_{20}, c_{20})$ with $\begin{cases} b_{20} = \frac{t((t^2-t+1)\alpha_t+t^3-t^2+1)((t-1)\alpha_t+t^2-t)(t^2\alpha_t+t^3-t+1)}{(t\alpha_t+t^2-t+1)(\alpha_t+1)^2} \\ c_{20} = \frac{((t-1)\alpha_t+t^2-t)(t^2\alpha_t+t^3-t+1)}{(t\alpha_t+t^2-t+1)(\alpha_t+1)} \end{cases}$ where α_t is a root of $f_{20}(x,t) = t^2x^3 + t^3x^2 - (t^3-4t^2+4t-1)x - t^4 + 3t^3 - 3t^2 + t$.

Therefore for each a point (x,y) on $X_1(11)$ satisfying $f(x,y) = 0$ there is a corresponding elliptic curve $E(b,c)$ defined over $K = \mathbb{Q}(x,y)$ such that $E(b,c)_{\text{tors}}$ contains $\mathbb{Z}/11\mathbb{Z}$. This is a basic strategy to construct infinite families of elliptic curves in [3].

Table 1 are taken from [3, Table 1] which contains infinite families elliptic curves and polynomials whose roots generate defining fields of that families.

3. Galois structures of the defining field of the constructed elliptic curves

In this section we determine the Galois group structure of the defining field $K_t = \mathbb{Q}(\alpha_t)$ of the constructed elliptic curves $E_N(t)$ where α_t is a root of $f_N(x,t)$ for $t \in \mathbb{Q}$. For the families of elliptic curves $E_N(t)$ over K_t we prove that the Galois groups of the Galois closures L_t of K_t over $\mathbb{Q}$ are the symmetric group S_3 of order 6 for almost all $t \in \mathbb{Q}$ with finite exceptions. For the proof, we apply the techniques about computations of Galois groups of polynomials of degree 3 in [1] and the following theorem by Faltings.

THEOREM 3.1. [2] *Let C be a nonsingular curve of genus $g \geq 2$ over a number field K, then the set of K-rational points $C(K)$ is finite.*

If C is a singular curve in the affine space $\mathbb{A}^2$, then it is understood that C is a nonsingular projective curve birational to this singular curve. Suppose C is a plane curve defined by

$$y^2 = f(x)$$

where $f(x) \in \mathbb{Q}[x]$ is of degree d and square-free in $\mathbb{Q}[x]$. Then the genus C is equal to $\left[\frac{d-1}{2}\right]$ where $[\,\cdot\,]$ is the greatest integer function. Thus if $d \geq 5$, then $C(\mathbb{Q})$ is finite by Faltings' theorem.

Since $K_t = \mathbb{Q}(\alpha_t)$ are cubic number fields for almost all $t \in \mathbb{Q}$, $G_t = Gal(L_t/\mathbb{Q})$ are S_3 or A_3. We will prove that G_t is equal to S_3 for almost all $t \in \mathbb{Q}$. According to [1, Theorem 3.6], G_t is S_3 if and only if the discriminant $\Delta_N(t)$ of $f_N(x,t)$ is non-square in $\mathbb{Q}$ for $t \in \mathbb{Q}$. For example, in the case $N = 13$,

$$\Delta_{13}(t) = -(t-1)(27t^5 - 31t^4 + 6t^3 + 6t^2 - 5t + 1).$$

We thus have to determine whether or not the curve

$$y^2 = -(t-1)(27t^5 - 31t^4 + 6t^3 + 6t^2 - 5t + 1)$$

has finitely many $\mathbb{Q}$-rational points. Since the curve is of genus 2, this curve has only finitely many $\mathbb{Q}$-rational points, and hence G_t is S_3 for almost all t.

We list discriminants $\Delta_N(t)$ of $f_N(x,t)$ in Table 2. By the exact the same reason as $N = 13$, we see that G_t is S_3 for almost all t when $N = 16, 18, 20$.

Now consider the cases $N = 11, 14, 15$. In these cases, the curves

$$y^2 = \Delta_N(t)$$

are elliptic curves.

TABLE 2. Discriminants of $f_N(x,t)$

N	$\Delta_N(t)$
11	$\Delta_{11}(t) = -t(t+1)(27t^2+27t+4)$.
13	$\Delta_{13}(t) = -(t-1)(27t^5-31t^4+6t^3+6t^2-5t+1)$.
14	$\Delta_{14}(t) = -(27t^2-256)(t^2-28)$.
15	$\Delta_{15}(t) = -t(27t^3+32t^2+4t-4)$.
16	$\Delta_{16}(t) = (t-1)(8t^7-56t^6+88t^5-64t^4+41t^3-19t^2+7t-1)$.
18	$\Delta_{18}(t) = 4t(t-1)(t^2-t+1)(t^3-6t^2+3t+1)$.
20	$\Delta_{20}(t) = t^2(t-1)^2(4t^9-12t^8+16t^7-47t^6+168t^5-308t^4$ $+300t^3-156t^2+40t-4)$.

Consider $N = 11$. Then we have to determine whether or not the elliptic curve

$$E_{11}: \ y^2 = -t(t+1)(27t^2+27t+4)$$

has finitely many $\mathbb{Q}$-rational points. That is, whether the $\mathbb{Q}$-rank of E_{11} is positive or not.

Using Maple we have the Weierstrass form of E_{11} as follows:

$$E_{11}: \ y^2 = t^3 + \frac{313}{3}t + \frac{10982}{27},$$

and using Magma, we can compute the $\mathbb{Q}$-rank E_{11} is equal to 0, and hence we can conclude that G_t is S_3 for almost all t. For $N = 14, 15$, the corresponding elliptic curves are as follows:

$$E_{14}: y^2 = t^3 - \frac{3346576}{3}t - \frac{12028939648}{27},$$
$$E_{15}: y^2 = t^3 - \frac{400}{3}t - \frac{16400}{27},$$

and their $\mathbb{Q}$-ranks are zero. Therefore we have the following main result:

THEOREM 3.1. *Let $N = 11, 13, 14, 15, 16, 18, 20$, let E_t be elliptic curves defined over $K_t = \mathbb{Q}(\alpha_t)$ in Table 1. Then, for almost all $t \in \mathbb{Q}$, the Galois group $Gal(L_t/\mathbb{Q})$ is isomorphic to the symmetric group S_3 where L_t are Galois closures of K_t over $\mathbb{Q}$.*

References

[1] K. Conrad, Galois groups of cubics and quartics (Not in Characteristic 2), (expository paper) http://www.math.uconn.edu/ kconrad/blurbs/galoistheory/cubicquartic.pdf

[2] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, *Invent. Math.* **73** (1983), no. 3, 349-366.
[3] D. Jeon, C. H. Kim, and Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, *Math. Comp.* **80** (2011), 579-591.
[4] D. Jeon, C. H. Kim, and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, *Acta Arith.* **113** (2004), 291-301.
[5] A. V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, *Math. Comp.* **81** (2012), 1131-1147.

*

Department of Mathematics Education
Kongju National University
Kongju 314-701, Republic of Korea
E-mail: dyjeon@kongju.ac.kr