55. *The Galois Representation of Type* E_8 *Arising from Certain Mordell-Weil Groups*

By Tetsuji SHIODA
Department of Mathematics, Rikkyo University

(Communicated by Shokichi IYANAGA, M. J. A., June 13, 1989)

In this note, we report our recent result on the rational points of certain elliptic curves over rational function field. We have a complete determination of the Mordell-Weil group, and we also study the E_8-lattice and the algebraic number fields arising naturally from this situation. For the computational purpose, we used "Mathematica" by S. Wolfram, run on Mac-SE. Details and more general accounts will appear elsewhere.

1. The main result. We consider the elliptic curve

$$E_\gamma : y^2 = x^3 + \gamma x + t^5 \qquad (\gamma \in \bar{\boldsymbol{Q}},\ \gamma \neq 0)$$

over $\bar{\boldsymbol{Q}}(t)$, t being a variable over $\bar{\boldsymbol{Q}}$, the algebraic closure of the rational number field $\boldsymbol{Q}$. Let $E_\gamma(\bar{\boldsymbol{Q}}(t))$ denote the Mordell-Weil group of the $\bar{\boldsymbol{Q}}(t)$-rational points of E_γ. It is a torsion-free abelian group of rank 8, and the height pairing defines a structure of "E_8-lattice", i.e. the (unique) lattice of rank 8 having a negative-definite even unimodular form.

The main result is the following:

Theorem 1. *There is a natural isomorphism*

$$E_\gamma(\bar{\boldsymbol{Q}}(t)) \simeq \boldsymbol{Z}[\zeta_{20}]\left(\frac{\gamma}{G}\right)^{1/20}$$

which is compatible with the action of the Galois group $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q}(\gamma))$. *Here* $\zeta_{20} = e^{2\pi i/20}$, *and* G *is a fixed element of* $\boldsymbol{Q}(\zeta_{20})$:

$$G = (-11261 + 6745\sqrt{5})/8 + (-1275 + 1365\sqrt{5}/2)\sqrt{(5+\sqrt{5})/2}.$$

2. Some consequences. Let K_γ be the smallest extension of $\boldsymbol{Q}$ such that all $\bar{\boldsymbol{Q}}(t)$-rational points of E_γ are defined over $K_\gamma(t)$. Then

$$K_\gamma = \boldsymbol{Q}(\zeta_{20})((\gamma/G)^{1/20})$$

and it is a Galois extension of degree at most 160 over $\boldsymbol{Q}(\gamma)$; for instance, for $\gamma = 1$, K_γ is a non-abelian extension of degree 160 over $\boldsymbol{Q}$.

Here are some consequences of Theorem 1.

(1) The Galois representation ρ of $\mathrm{Gal}(K_\gamma/\boldsymbol{Q})$ on the E_8-lattice $E_\gamma(\bar{\boldsymbol{Q}}(t))$ is equivalent to the subspace $\boldsymbol{Q}(\zeta_{20})\cdot(\gamma/G)^{1/20}$ of K_γ, which is a unique irreducible representation of degree 8 of this Galois group when $[K_\gamma : \boldsymbol{Q}] = 160$ $(\gamma \in \boldsymbol{Q})$.

The Artin L-function attached to ρ turns out to be the Hecke L-function of the cyclotomic field $\boldsymbol{Q}(\zeta_{20})$ with the character ψ belonging to the cyclic extension K_γ of $\boldsymbol{Q}(\zeta_{20})$:

$$L(s, \rho, K_\gamma/\boldsymbol{Q}) = L(s, \psi, K_\gamma/\boldsymbol{Q}(\zeta_{20})).$$

(2) Let S_γ be the elliptic surface over $\boldsymbol{P}^1$ associated with E_γ; it is a nonsingular rational surface defined over $\boldsymbol{Q}$ if $\gamma \in \boldsymbol{Q}$. The Hasse zeta function of this surface is equal to

$$\zeta(s)\,\zeta(s-1)^2\,\zeta(s-2)\,L(s-1,\rho)$$

(possibly up to the Euler factor for $p=2, 5$), where $\zeta(s)$ is the Riemann zeta function. The L-function is also related to certain Jacobi sums (cf. [6], [4]). Compare Weil's remark in [7, p. 558].

(3) Changing the viewpoint, Theorem 1 allows one to realize the E_8-lattice in a number field like K_γ. For example, if we take $\gamma=G$, then the structure of E_8-lattice on $\boldsymbol{Z}[\zeta_{20}]$, transported from $E_\gamma(\bar{\boldsymbol{Q}}(t))$, is given as follows. For $|n-m|<10$, we have

$$\langle \zeta^n, \zeta^m \rangle = -2, 1, 0 \quad \text{or} \quad -1$$

according as $n=m$, $|n-m|\equiv 1 \pmod 3$, $\equiv 2 \pmod 3$ or $n\neq m$ and $n\equiv m \pmod 3$ (cf. [1, Ch. 8]).

3. Sketch of the proof of Theorem 1. First we find some rational points $P=(x, y)$ of E_γ of the form:

$$(*) \qquad x=gt^2+at+b, \qquad y=ht^3+ct^2+dt+e,$$

where $a, b, \cdots, g, h \in \bar{\boldsymbol{Q}}$, $g\cdot h\neq 0$.

Proposition 2. *There are exactly 240 rational points of the form (*), and they are given as follows. There are 12 absolute constants $G_j \in \boldsymbol{Q}(\zeta_{20})$ $(1\leqq j\leqq 12)$ with $G_1=G$ such that for each 20-th root of G_j/γ, say ξ, there exists a unique point P_ξ of the form (*) with $g=\xi^2$ and $h=\xi^3$.*

Second, we consider the rational elliptic surface $\pi: S_\gamma \to \boldsymbol{P}^1$ associated with E_γ. It has 10 singular fibres of type I_1 at $t\neq\infty$ and a singular fibre of type II at $t=\infty$ (cf. [2], [5], [4, §5]). Since there are no reducible fibres, the Mordell-Weil group is of rank 8 and the height pairing $\langle P, P'\rangle$ on that group is defined by the intersection number of the divisors (P)-(0) and (P')-(0), where (P) denotes the divisor of the section of π corresponding to P and (0) is that of the 0-section (cf. [3], §1]).

The 240 points P_ξ correspond to the minimal vectors in the E_8-lattice.

Proposition 3. *Let P_n $(1\leqq n\leqq 20)$ be the point P_ξ for $j=1$ and $\xi=\zeta_{20}^{-n}\cdot\xi_0$ where ξ_0 is a fixed 20-th root of G/γ. Then*

$$\det(\langle P_n, P_m\rangle)_{1\le n,m\le 8}=1.$$

Hence $P_1, \cdots, P_8$ are independent and generate the full Mordell-Weil group $E_\gamma(\bar{\boldsymbol{Q}}(t))$.

Third, we look at the singular fibre at $t=\infty$, of type II (a rational curve with a cusp). Its smooth part is the additive group with the group parameter tx/y. The specialization $t\to\infty$ induces a group homomorphism

$$sp: \quad E_\gamma(\bar{\boldsymbol{Q}}(t)) \longrightarrow \bar{\boldsymbol{Q}}$$

which is compatible with the Galois action. Then we see easily

$$sp(P_n)=\zeta_{20}^n\cdot\xi_0^{-1}.$$

It follows that the map sp gives an isomorphism of $E_\gamma(\bar{\boldsymbol{Q}}(t))$ onto $\boldsymbol{Z}[\zeta_{20}]\xi_0^{-1}$, which proves Theorem 1.

References

[1] Conway, J. and Sloane, N.: Sphere Packings, Lattices and Groups. Grund. Math. Wiss., **290**, Springer-Verlag (1988).

[2] Kodaira, K.: On compact analytic surfaces. II–III. Ann. of Math., **77**, 563–626 (1963), **78**, 1–40 (1963); Collected Works, vol. III, Iwanami and Princeton Univ. Press, pp. 1269–1372 (1975).

[3] Shioda, T.: On elliptic modular surfaces. J. Math. Soc. Japan, **24**, 20–59 (1972).

[4] ——: An explicit algorithm for computing the Picard number of certain algebraic surfaces. Amer. J. Math., **108**, 415–432 (1986).

[5] Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil. Lect. Notes in Math., **476**, 33–52 (1975).

[6] Weil, A.: Jacobi sums as "Grössencharaktere". Trans. A.M.S., **73**, 487–495 (1952); Collected Papers, vol. II, Springer-Verlag, pp. 63–71 (1980).

[7] ——: Abstract versus classical algebraic geometry. Proc. Intern. Math. Congr. Amsterdam, vol. III, 550–558 (1954); Collected Papers, vol. II, Springer-Verlag, pp. 180–188 (1980).