J. Math. Soc. Japan
Vol. 43, No. 4, 1991

Construction of elliptic curves with high rank via the invariants of the Weyl groups

Dedicated to Professor G. Shimura on his 60th birthday

By Tetsuji SHIODA

(Received July 20, 1990)

1. Introduction.

In this paper, we shall establish a general method for constructing elliptic curves over the rational function field $\boldsymbol{Q}(t)$ or $k(t)$ with relatively high rank (up to 8), together with explicit rational points forming the generators of the Mordell-Weil group. The construction is based on the theory of Mordell-Weil lattices (see [**S1**] for the summary and [**S5**] for more details).

In order to better explain our method and, especially, the role played by the invariants of the Weyl groups, we first recall the analogous situation in the theory of algebraic equations. Letting $a_1, \cdots, a_n$ be algebraically independent over the ground field k, say $k=\boldsymbol{Q}$, consider the algebraic equation

$$X^n+a_1X^{n-1}+\cdots+a_n=0 \tag{1.1}$$

over $k_0=\boldsymbol{Q}(a_1, \cdots, a_n)$. If $x_1, \cdots, x_n$ are the roots, then we have the relation of the roots and coefficients:

$$\pm a_i=\varepsilon_i(x_1, \cdots, x_n) \quad (i\text{-th elementary symmetric polynomial}) \tag{1.2}$$

If $\mathcal{K}$ denotes the splitting field of (1.1) over k_0, then we have

$$\mathcal{K}=k_0(x_1, \cdots, x_n)=\boldsymbol{Q}(x_1, \cdots, x_n)$$

$$\mathrm{Gal}(\mathcal{K}/k_0)=\mathfrak{S}_n \quad (n\text{-th symmetric group}).$$

In particular, the invariant field $\mathcal{K}^{\mathfrak{S}_n}$ is k_0 by Galois theory, but a stronger result holds:

$$\boldsymbol{Q}[x_1, \cdots, x_n]^{\mathfrak{S}_n}=\boldsymbol{Q}[a_1, \cdots, a_n],$$

the fundamental theorem on symmetric functions ($\boldsymbol{Q}$ may be replaced by $\boldsymbol{Z}$ here).

With slight modification, the above can be viewed as follows. Take $a_1=0$ and let $a_2, \cdots, a_n$ be still algebraically independent; thus $x_1+\cdots+x_n=0$ and

$k_0 = \boldsymbol{Q}(a_2, \cdots, a_n)$. Then we have

(1.3) $\mathcal{K} = k_0(x_1, \cdots, x_n)$

$= \boldsymbol{Q}(x_2, \cdots, x_n)$ (a purely transcendental extension of $\boldsymbol{Q}$)

(1.4) $\mathrm{Gal}(\mathcal{K}/k_0) = \mathfrak{S}_n = W(A_{n-1})$

(1.5) $\boldsymbol{Q}[x_2, \cdots, x_n]^{W(A_{n-1})} = \boldsymbol{Q}[a_2, \cdots, a_n]$.

Here $W(A_{n-1})$ is the Weyl group of type A_{n-1} (cf. [**B**]), and (1.5) can be regarded as a special case of Chevalley's theorem on the invariants of a finite reflection group. The formula (1.2) expresses the fundamental invariants of $W(A_{n-1})$ in terms of the standard basis of the root system A_{n-1}, or more precisely, of the dual lattice A_{n-1}^*. By the formula (1.2), one can easily write down an algebraic equation having the prescribed roots.

It is remarkable that an entirely similar situation arises from the Mordell-Weil lattices of certain elliptic curves, which enables us to write down the equation of elliptic curves over $\boldsymbol{Q}(t)$ with relatively high rank, having the prescribed data for the generators of the Mordell-Weil group.

For example, for the case of rank $r=8$, consider the elliptic curve

(1.6) $$E: y^2 = x^3 + x\Big(\sum_{i=0}^{3} p_i t^i\Big) + \Big(\sum_{i=0}^{3} q_i t^i + t^5\Big)$$

defined over $k_0(t)$, where $k_0 = \boldsymbol{Q}(p_0, \cdots, p_3, q_0, \cdots, q_3)$. (This equation defines a family of affine surfaces, known as the universal deformation of the rational double point of type E_8, parametrized by $\lambda = (p_i, q_j) \in \boldsymbol{A}^8$ (affine space of dimension 8); the origin $\lambda = 0$ corresponds to the E_8-singularity: $y^2 = x^3 + t^5$.) Assume that λ is generic, that is, $p_0, \cdots, q_3$ are algebraically independent over $\boldsymbol{Q}$, and let $k = \bar{k}_0$ be the algebraic closure of k_0. Then the Mordell-Weil lattice $E(k(t))$ turns out to be the root lattice of type E_8. Let $\mathcal{K}$ be the smallest extension of $k_0 = \boldsymbol{Q}(\lambda) = \boldsymbol{Q}(p_i, q_j)$ such that $E(k(t)) = E(\mathcal{K}(t))$; $\mathcal{K}/k_0$ is a finite Galois extension. Then we can prove (see Theorems 8.3, 8.4)

(1.7) $\mathcal{K} = k_0(u_1, \cdots, u_8) = \boldsymbol{Q}(u_1, \cdots, u_8)$

(1.8) $\mathrm{Gal}(\mathcal{K}/k_0) = W(E_8)$

(1.9) $\boldsymbol{Q}[u_1, \cdots, u_8]^{W(E_8)} = \boldsymbol{Q}[p_0, \cdots, q_3]$.

Here the parameters $u_1, \cdots, u_8$ correspond to the basis of the root system of type E_8, and they are defined in terms of the specialization homomorphism $sp_\infty: E(k(t)) \to \boldsymbol{G}_a(k)$ from the Mordell-Weil group to the singular fibre of (1.6) at $t=\infty$.

The equality (1.9) says that the coefficients $p_0, \cdots, q_3$ of the elliptic curve (1.6) form the fundamental invariants of the Weyl group $W(E_8)$; in particular, we can write

$$p_i = I_{20-6i}(u_1, \cdots, u_8), \qquad q_j = I_{30-6j}(u_1, \cdots, u_8), \tag{1.10}$$

which is an analogue of (1.2), the relation of roots and coefficients of an algebraic equation. Actually we have a universal algebraic equation of degree $N=240$ whose roots are the N "roots" of the root system E_8. (1.10) represents the essential part of the relation of the roots and coefficients of this universal equation. As a by-product, we obtain explicit fundamental invariants of the Weyl group $W(E_8)$ (see Theorem 7.2, Theorem 8.3).

Now we consider the elliptic curve (1.6) over the field $\mathcal{K}(t)=\boldsymbol{Q}(u_1, \cdots, u_8)(t)$. Then the Mordell-Weil group $E(\mathcal{K}(t))$ is isomorphic to the root lattice E_8, and it has a basis $\{P_1, \cdots, P_8\}$ such that $sp_\infty(P_i)=u_i$; more explicitly, we have $P_i=(x, y)$ where x, y are polynomials in t with coefficients in $\boldsymbol{Q}[u_1, \cdots, u_8][u_i^{-1}]\cap \boldsymbol{Q}(p_0, \cdots, q_3)(u_i)$, of the following form:

$$x = u_i^{-2}t^2+a_i t+b_i, \qquad y = u_i^{-3}t^3+c_i t^2+d_i t+e_i\,. \tag{1.11}$$

In order to obtain some elliptic curves over $\boldsymbol{Q}(t)$ with rank $r=8$, it suffices to specialize $u_1, \cdots, u_8$ to some rational numbers in such a way that the rank remains the same (or, as we would say, that the Mordell-Weil lattice does not "degenerate"). Then (1.6) and (1.10) determine the equation of an elliptic curve over $\boldsymbol{Q}(t)$ with rank 8, which is given with a basis $\{P_i\}$ of $E(\boldsymbol{Q}(t))$ of the form (1.11).

The variation of the above theme can be played, in addition to the case E_8, in the cases E_7, E_6, D_4, A_2, where we take the elliptic curve E and the parameter λ as follows.

(E_7)
$$y^2 = x^3+x(p_0+p_1t+t^3)+(\textstyle\sum_{i=0}^4 q_it^i)$$
$$\lambda = (p_0, p_1, q_0, q_1, q_2, q_3, q_4)\in \boldsymbol{A}^7$$

(E_6)
$$y^2 = x^3+x(\textstyle\sum_{i=0}^2 p_it^i)+(\sum_{i=0}^2 q_it^i+t^4)$$
$$\lambda = (p_0, p_1, p_2, q_0, q_1, q_2)\in \boldsymbol{A}^6$$

(D_4)
$$y^2 = x^3+x(p_0-t^2)+(\textstyle\sum_{i=0}^2 q_it^i)$$
$$\lambda = (p_0, q_0, q_1, q_2)\in \boldsymbol{A}^4$$

(A_2)
$$y^2 = x^3+x\cdot p_0+q_0+t^2$$
$$\lambda = (p_0, q_0)\in \boldsymbol{A}^2\,.$$

These equations define universal deformation of the rational double points of type $E_7, \cdots, A_2$. In each case, the Mordell-Weil lattice $E(\mathcal{K}(t))$ is equal to the dual lattice $E_7^*, \cdots$ of the root lattice $E_7, \cdots$, with the "narrow" Mordell-Weil lattice $E(\mathcal{K}(t))^0$ being exactly the root lattice (cf. §4 below).

In the next section, we formulate the part of the above results relevant to the construction of elliptic curves over $\boldsymbol{Q}(t)$, together with explicit generators of the Mordell-Weil groups. Indeed, everything can be stated in elementary terms, with no mention of rational double points, their universal deformation or even the invariants of the Weyl groups, although the last are visibly there.

Also the results give a complete algorithm for constructing numerical examples. The interested reader could use our algorithm to produce as many examples of elliptic curves over $\boldsymbol{Q}(t)$ with rank 2 or 4 (by hand) or with rank 6, 7 or 8 (by computer) as desired. We give a few numerical examples in §3. The proof will occupy the rest of the paper. The general outline of the proof will be given in §4, together with a brief review on the Mordell-Weil lattices. Then we treat the cases (A_2), (D_4) in §5, 6. After some preliminaries on the root lattices E_r $(r=6, 7, 8)$ in §7, we treat the case (E_8) in §8, and then the cases (E_6), (E_7) in §9, 10.

We add a few remarks on the related subjects.

(1) A natural question: what about the other type A_n or D_n, not mentioned in the above? The same idea seems to work, but with some modification. First of all, the defining equation of the family does not give an elliptic curve but rather a hyperelliptic curve of higher genus in general. The Mordell-Weil group of the Jacobian variety of this curve will be of rank at least n, and we may expect that, as a lattice, it will be the root lattice of the desired type or some lattice closely related to it. Some preliminary calculation indicates that the family for type A_3 (or D_5) gives an elliptic curve whose Mordell-Weil lattice is D_4^* (or E_6^*) rather than A_3^* (or D_5^*). We hope to come back to this question in some other occasion.

(2) We have treated here only one side of the arithmetic application of the theory of Mordell-Weil lattices: construction of elliptic curves with relatively high rank. The other side will be the construction of Galois representation ρ: $\mathrm{Gal}(\bar{\boldsymbol{Q}}/\boldsymbol{Q})\to\mathrm{Aut}(E(\bar{\boldsymbol{Q}}(t)))$ whose image is the full Weyl group $W(E_8)$, etc. The existence of such follows from (1.8) and its variants for E_7, E_6, $\cdots$, in view of Hilbert's irreducibility theorem (cf. [**S1**], Theorem 7.1). This essentially answers the question raised by Weil and Manin (see [**W1**], p. 558, [**M**], Ch. 4, 23.13). Moreover our method will allow explicit construction of such Galois representations, and in particular, of Galois extensions over $\boldsymbol{Q}$ with Galois group $W(E_8)$, etc. We shall discuss this in more detail in a forthcoming paper.

(3) In [**S1**, §6], we have sketched the proof of (1.8), by making use of the monodromy theory of the Milnor lattice of a rational double point. But this can now be avoided, since we have more elementary, purely algebraic proof of (1.8). Our results might be of some interest to people in the singu-

larity theory, because (i) the field $\mathcal{K}$ provides the smallest extension of $\boldsymbol{Q}(\lambda)$ over which the simultaneous resolution of singularities for the family (1.6) can be performed, and (ii) the universal algebraic equation, mentioned before, can be used to give a very precise description of the stratification of the parameter space according to the type of singularities (see [**S4**]).

(4) Once we have an elliptic curve over $\boldsymbol{Q}(t)$ of rank r, we obtain an infinite family of elliptic curves over $\boldsymbol{Q}$ of rank at least r, by specializing t to rational numbers. This method was initiated by Néron [**N1**], who showed further that there exists an infinite family of elliptic curves over $\boldsymbol{Q}$ with rank $\geqq 11$. It seems very likely that our results, combined with Néron's idea, will allow some explicit construction of such a family.

(5) The numerical examples for (E_6), (E_7) or (E_8) in § 3 will give at the same time explicit examples of del Pezzo surfaces of degree 3, 2 or 1, defined over $\boldsymbol{Q}$, such that all the exceptional curves of the first kind (27, 56 or 240 in number, cf. [**M**]) are defined over $\boldsymbol{Q}$. In particular, we can construct in this way smooth cubic surfaces over $\boldsymbol{Q}$ such that all the 27 lines on them are defined over $\boldsymbol{Q}$, and also smooth plane quartic curves over $\boldsymbol{Q}$ such that all the 28 double tangents are defined over $\boldsymbol{Q}$.

2. The construction theorems.

In the following, we make the statements for the case of $\boldsymbol{Q}(t)$, but $\boldsymbol{Q}$ can be replaced by any field whatsoever, as far as its characteristic does not divide the denominators of rational numbers appearing in the formulas and is different from 2 or 3 (cf. Remark at the end of § 4).

THEOREM (A_2). *Take $(b_1, b_2) \in \boldsymbol{Q}^2$ such that b_1, b_2 and $b_3 = -b_1 - b_2$ are mutually distinct. Let E be the elliptic curve over $\boldsymbol{Q}(t)$:*

$$E:\ y^2 = (x-b_1)(x-b_2)(x-b_3)+t^2\,. \tag{2.1}$$

Then the Mordell-Weil group $E(\boldsymbol{Q}(t))$ is torsion-free and of rank 2. Any two of the three rational points

$$P_i = (b_i,\, t) \qquad (i=1, 2, 3) \tag{2.2}$$

generate $E(\boldsymbol{Q}(t))$. (Note that $P_1+P_2+P_3=0$ since the 3 points are collinear.) The Mordell-Weil lattice is isomorphic to A_2^*, the dual lattice of the root lattice A_2. The Gram matrix is:

$$(\langle P_i,\, P_j\rangle)_{1\leq i, j\leq 2} = \begin{pmatrix} 2/3 & -1/3 \\ -1/3 & 2/3 \end{pmatrix}. \tag{2.3}$$

THEOREM (D_4). *Take $(d_1, \cdots, d_4) \in \boldsymbol{Q}^4$ such that $d_1^2, \cdots, d_4^2$ are mutually* *distinct. Define*

$$
(2.4)\qquad \begin{cases} q_2 = \dfrac{1}{3}\sum_{i=1}^4 d_i^2 \\ p_0 = \sum_{i<j} d_i^2 d_j^2 - 3q_2^2 \\ q_0 = \sum_{i<j<k} d_i^2 d_j^2 d_k^2 - p_0 q_2 - q_2^3 \\ q_1 = \varepsilon \cdot 2 d_1 d_2 d_3 d_4 \qquad (\varepsilon = \pm 1). \end{cases}
$$

Then the elliptic curve over $\boldsymbol{Q}(t)$

$$
(2.5)\qquad E: y^2 = x^3 + x(p_0 - t^2) + (q_0 + q_1 t + q_2 t^2)
$$

has a torsion-free Mordell-Weil group of rank 4, *and, as a lattice,* $E(\boldsymbol{Q}(t))$ *is isomorphic to* D_4^*, *the dual lattice of the root lattice* D_4. *There exist* 4 *rational points of the form:*

$$
(2.6)\qquad P_i = (b_i,\ d_i t + e_i),
$$

where d_i *are as given at the beginning and*

$$
(2.7)\qquad b_i = -d_i^2 + q_2
$$

$$
(2.8)\qquad \begin{aligned} e_i &= \varepsilon d_j d_k d_l \qquad (\textit{for } \{i, j, k, l\} = \{1, 2, 3, 4\}) \\ &= q_1/(2d_i) \qquad \textit{in case } d_i \neq 0 . \end{aligned}
$$

These points are independent, with the Gram matrix

$$
(2.9)\qquad (\langle P_i, P_j \rangle) = 1_4 ,
$$

which generate a subgroup of index 2 *in* $E(\boldsymbol{Q}(t))$. *Further there are* 16 *points of the form*

$$
(2.10)\qquad P' = (\pm t + b',\ d't + e'),
$$

and any such P', together with any 3 *of* P_i*'s, give a set of generators of* $E(\boldsymbol{Q}(t))$.

Before proceeding to the case E_r (r=6, 7, 8), let us fix some notation. For a moment, suppose that $u_1, \cdots, u_r$ form a $\boldsymbol{Z}$-basis of E_r^* (the dual lattice of the root lattice E_r) consisting of minimal vectors, and let the Gram matrix be

$$
(2.11)\qquad I_r = (\langle u_i, u_j \rangle)_{1 \leq i, j \leq r} .
$$

Let $\{u_i \mid 1 \leqq i \leqq N\}$ denote all the minimal vectors of E_r^* (thus N=54, 56, 240 for r=6, 7 or 8; cf. [**CS**, Ch. 4]). Further, let $\{\alpha_j \mid 1 \leqq j \leqq n\}$ denote all the roots of E_r, i.e., the minimal vectors of E_r with $\langle \alpha_j, \alpha_j \rangle = 2$. (Thus n=72, 126 or 240 for r=6, 7 or 8.) For instance, we can take as $\alpha_1, \cdots, \alpha_r$ the basis of E_r given by [**B**, Ch. 6] and $\alpha_1, \cdots, \alpha_{n/2}$ the positive roots (i.e. the roots which can be written as positive linear combination of $\alpha_1, \cdots, \alpha_r$) so that $\{\alpha_1, \cdots, \alpha_n\}$

$=\{\pm\alpha_1, \cdots, \pm\alpha_{n/2}\}$. To fix the idea, let us make this choice.

Now, writing each u_i and α_j as a $\boldsymbol{Z}$-linear combination of $u_1, \cdots, u_r$, we define the following polynomials in $\boldsymbol{Z}[u_1, \cdots, u_r]$:

$$\varepsilon_\nu(u) = \nu\text{-th elementary symmetric function of } u_1, \cdots, u_N \tag{2.12}$$

$$\delta_1(u) = \textstyle\prod_{1\le i<j\le N} (u_i - u_j), \tag{2.13}$$

$$\delta_0(u) = \textstyle\prod_{1\le j\le n} \alpha_j = \pm(\prod_{1\le j\le n/2} \alpha_j)^2 . \tag{2.14}$$

For $r=6$ ($N=54$), we can choose $u_1, \cdots, u_6$ so that $\langle u_i, u_j\rangle \equiv 1/3 \pmod 1$ for all $i, j\leqq 6$. We arrange $\{u_i\}$ so that the same congruence holds for all $i, j\leqq N/2 =27$, and we replace N by $N/2$ in the definition of ε_ν and δ_1 above. With this notation, we have:

THEOREM (E_6). *Take $a=(a_1, \cdots, a_6)\in\boldsymbol{Q}^6$ such that $\delta_0(a)\neq 0$. Let $\varepsilon_\nu=\varepsilon_\nu(a)$, and define*

$$\begin{cases} p_2 = \varepsilon_2/12 \\ p_1 = \varepsilon_5/48 \\ q_2 = (\varepsilon_6 - 168p_2^3)/96 \\ p_0 = (\varepsilon_8 - 294p_2^4 - 528p_2q_2)/480 \\ q_1 = (\varepsilon_9 - 1008p_1p_2^2)/1344 \\ q_0 = (\varepsilon_{12} - 608p_1^2p_2 - 4768p_0p_2^2 - 252p_2^6 - 1200p_2^3q_2 + 1248q_2^2)/17280. \end{cases} \tag{2.15}$$

Then the elliptic curve over $\boldsymbol{Q}(t)$

$$E: y^2 = x^3 + x(p_0 + p_1t + p_2t^2) + (q_0 + q_1t + q_2t^2 + t^4) \tag{2.16}$$

has a torsion-free Mordell-Weil group of rank 6, and, as a lattice, $E(\boldsymbol{Q}(t))$ is isomorphic to E_6^*, the dual lattice of the root lattice E_6. There is a basis of $E(\boldsymbol{Q}(t))$ consisting of the 6 rational points

$$P_i = (a_i t + b_i, t^2 + d_i t + e_i) \qquad (1\leqq i\leqq 6) \tag{2.17}$$

such that

$$(\langle P_i, P_j\rangle) = I_6 . \tag{2.18}$$

Here a_i has the prescribed value and

$$\begin{cases} b_i = \beta_i(a_1, \cdots, a_6) \\ d_i = (a_i^3 + a_ip_2)/2 \\ e_i = (3a_i^2b_i - d_i^2 + a_ip_1 + b_ip_2 + q_2)/2 , \end{cases} \tag{2.19}$$

where β_i is a certain polynomial in $u_1, \cdots, u_6$ such that

$$\beta_i(u_1, \cdots, u_6)\in\boldsymbol{Q}[u_1, \cdots, u_6] \cap \boldsymbol{Q}(p_0, \cdots, q_2)(u_i) . \tag{2.20}$$

There are exactly 27 *rational points* P_i $(1\leqq i\leqq 27)$ *of the form* (2.17), *and* $\{\pm P_i\}$ *give all the minimal vectors of norm* 4/3 *in the lattice* E_6^*. *Moreover, in case* $\delta_1(a)\neq 0$, *each* P_i *is uniquely determined by* a_i $(1\leqq i\leqq 27)$.

Next, for the case E_7 and E_8, the Weyl group $W(E_r)$ contains -1, so we have $\varepsilon_\nu=0$ for all ν odd and $\varepsilon_{2\nu}=(-1)^\nu\varepsilon'_\nu$, where ε'_ν is the ν-th elementary symmetric function of $u_1^2, \cdots, u_{N/2}^2$ if we arrange $\{u_i\}$ so that $\{\pm u_j \mid 1\leqq j\leqq N/2\}=\{u_i\}$. We use ε'_ν simply because it is more suited to constructing examples.

THEOREM (E_7). *Take* $c=(c_1, \cdots, c_7)\in\boldsymbol{Q}^7$ *such that* $\delta_0(c)\neq 0$. *Let* $\varepsilon'_\nu=\varepsilon'_\nu(c)$, *and define*

$$(2.21)\quad \begin{cases} q_4=\varepsilon'_1/36 \\ q_3=(-\varepsilon'_3+6084q_4^3)/72 \\ p_1=(\varepsilon'_4-43875q_4^4+1800q_4q_3)/60 \\ q_2=(\varepsilon'_5-238680q_4^5+21600q_4^2q_3-1008q_4p_1)/504 \\ p_0=(-\varepsilon'_6+1022580q_4^6-165600q_4^3q_3+7008q_4^2p_1+10344q_4q_2+540q_3^2)/540 \\ q_1=(-\varepsilon'_7+3552120q_4^7-910800q_4^4q_3+11592q_4q_3^2+20592q_4^3p_1 \\ \qquad +100824q_4^2q_2-7944q_4p_0+1092q_3p_1)/3828 \\ q_0=(\varepsilon'_9-24667500q_4^9+12751200q_4^6q_3-771120q_4^3q_3^2+683760q_4^5p_1 \\ \qquad -2702280q_4^4q_2+145200q_4^3p_0+489288q_4^2q_1-224040q_4^2q_3p_1 \\ \qquad +61824q_4q_3q_2+8760q_3p_0+1848q_3^3-12656q_4p_1^2+5024p_1q_2)/29496. \end{cases}$$

Then the elliptic curve E *over* $\boldsymbol{Q}(t)$

$$(2.22)\qquad y^2=x^3+x(p_0+p_1t+t^3)+(q_0+q_1t+q_2t^2+q_3t^3+q_4t^4)$$

has a torsion-free Mordell-Weil group of rank 7, *and, as a lattice,* $E(\boldsymbol{Q}(t))$ *is isomorphic to* E_7^*, *the dual lattice of the root lattice* E_7. *It is generated by the* 7 *rational points*

$$(2.23)\qquad P_i=(a_it+b_i,\ c_it^2+d_it+e_i)\qquad (1\leqq i\leqq 7)$$

having the Gram matrix

$$(2.24)\qquad (\langle P_i, P_j\rangle)=I_7\,.$$

Here c_i *has the prescribed value and* a_i, b_i, d_i, e_i *are determined rationally from* c_i *over* $\boldsymbol{Q}[p_0, \cdots, q_4]$ *and also polynomially from* $c_1, \cdots, c_7$ *over* $\boldsymbol{Q}$.

There are exactly 56 *rational points* P_i *of the form* (2.22), *which give the minimal vectors of norm* 3/2 *in the lattice* E_7^*. *In case* $\delta_1(c)\neq 0$, *each* P_i *is uniquely determined by* c_i $(1\leqq i\leqq 56)$.

THEOREM (E_8). *Take $u=(u_1, \cdots, u_8)\in \boldsymbol{Q}^8$ such that $\delta_0(u)\neq 0$. Let $\varepsilon'_\nu=\varepsilon'_\nu(u)$, and define $p_3, p_2, \cdots, q_0$ by the following formulas:*

$$
(2.25)\quad \left\{
\begin{aligned}
p_3 &= -\varepsilon'_1/60\\
p_2 &= (\varepsilon'_4-478170p_3^4)/720\\
q_3 &= (\varepsilon'_6-1030320p_2p_3^2-47747700p_3^6)/15120\\
p_1 &= -(\varepsilon'_7+17858880p_2p_3^3+361791144p_3^7+753840p_3q_3)/79200\\
q_2 &= -(\varepsilon'_9+5240640p_2^2p_3+96593280p_1p_3^2+2277007200p_2p_3^5\\
&\quad +13257944700p_3^9+293378400p_3^3q_3)/2620800\\
p_0 &= (\varepsilon'_{10}-128513424p_2^2p_3^2-1545977808p_1p_3^3-18595558800p_2p_3^6\\
&\quad -65910925080p_3^{10}-123173712p_3q_2-2492208p_2q_3\\
&\quad -3431681424p_3^4q_3)/11040480\\
q_1 &= (\varepsilon'_{12}-4551984p_2^3-387688872p_1p_2p_3-11556147624p_0p_3^2\\
&\quad -24236204440p_2^2p_3^4-168171466680p_1p_3^5-749135368800p_2p_3^8\\
&\quad -1153992168420p_3^{12}-42618310896p_3^3q_2-2516521104p_2p_3^2q_3\\
&\quad -234127252800p_3^6q_3+35394408q_3^2)/419237280\\
q_0 &= (-\varepsilon'_{15}+422863200p_1p_2^2+18339605640p_1^2p_3\\
&\quad +3209804640p_0p_2p_3-71061462976p_2^3p_3^3\\
&\quad -1528645019808p_1p_2p_3^4-15986969259936p_0p_3^5\\
&\quad -10597571701120p_2^2p_3^7-43713099157440p_1p_3^8\\
&\quad -68920453929600p_2p_3^{11}-39472177353840p_3^{15}\\
&\quad -5508702912024p_3^3q_1-234901945584p_2p_3^2q_2\\
&\quad -28604105079744p_3^6q_2-8050693680p_2^2p_3q_3\\
&\quad -250521815304p_1p_3^2q_3-3139744251456p_2p_3^5q_3\\
&\quad -36016821822240p_3^9q_3+4971002400q_2q_3\\
&\quad +521644115232p_3^3q_3^2)/65945880000.
\end{aligned}
\right.
$$

Then the elliptic curve over $\boldsymbol{Q}(t)$

$$(2.26)\qquad E: y^2=x^3+x(\textstyle\sum_{i=0}^3 p_i t^i)+(\sum_{i=0}^3 q_i t^i+t^5)$$

has a torsion-free Mordell-Weil group of rank 8, and as a lattice, it is isomorphic to the root lattice E_8. It has the 8 rational points

$$(2.27)\qquad P_i = (g_i t^2+a_i t+b_i,\ h_i t^3+c_i t^2+d_i t+e_i) \qquad (1\leqq i\leqq 8)$$

having the Gram matrix

$$(2.28) \qquad (\langle P_i, P_j \rangle) = I_8 .$$

The coefficients of P_i *are determined as follows: first*

$$g_i = u_i^{-2}, \qquad h_i = u_i^{-3},$$

where u_i *has the prescribed value, and* a_i, b_i, c_i, d_i, e_i *are given by certain expressions in* $\boldsymbol{Q}[u_1, \cdots, u_8][u_i^{-1}]$ *which are also expressed by some rational functions of* u_i *with coefficients in* $\boldsymbol{Q}(p_0, \cdots, q_3)$.

There are exactly 240 *rational points* P_i *of the form* (2.27), *which correspond to the roots in the lattice* E_8. *In case* $\delta_1(u) \neq 0$, *each* P_i *is uniquely determined by* u_i $(1 \leqq i \leqq 240)$.

Application to elliptic curves over $\boldsymbol{Q}$. Following the tradition since A. Néron [**N1**], for each elliptic curve E over $\boldsymbol{Q}(t)$ constructed by the above method, we can further specialize t to some rational numbers (called t again) to obtain a family of elliptic curves $E^{(t)}$ over $\boldsymbol{Q}$, given with the rational points $\{P_i^{(t)}\}$, where $\{P_i \mid 1 \leqq i \leqq r\}$ denotes a basis of $E(\boldsymbol{Q}(t))$. By a theorem of Néron, Silverman and Tate (cf. [**Si**], [**T2**]), we have:

COROLLARY. *The Mordell-Weil group* $E^{(t)}(\boldsymbol{Q})$ *has rank at least* r *and the rational points* $P_i^{(t)}$ $(i=1, \cdots, r)$ *are independent, for all* $t \in \boldsymbol{Q}$ *with only finitely many exception. The "partial" regulator of these points (with respect to the canonical height on* $E^{(t)}(\boldsymbol{Q})$) *has the asymptotic behavior:*

$$(2.29) \qquad \lim_{h(t) \to \infty} \det(\langle P_i^{(t)}, P_j^{(t)} \rangle_{can} / h(t)) = 1/(2^r \cdot d)$$

where $h(t)$ *is the standard height of a point* $t \in \boldsymbol{P}^1$ *(esp.* $h(t) = \log|t|$ *for* $t \in \boldsymbol{Z}$), *and* d *is the determinant of the corresponding root lattice. Thus, according to the cases* A_2, D_4, E_6, E_7 *or* E_8, *the right hand side* of (2.29) *is equal to*

$$1/12,\ 1/64,\ 1/192,\ 1/256 \text{ or } 1/256 .$$

3. Examples.

The algorithm given by Theorems (A_2) and (D_4) is so explicit that it may not be necessary to give any numerical examples. But, just for fun, we write down one such example for each type. Then we go on to the examples for E_6, E_7, E_8.

EXAMPLE (A_2). Take $b_1=0$, $b_2=1$, $b_3=-1$. The elliptic curve E over $\boldsymbol{Q}(t)$ defined by

$$y^2 = x^3 - x + t^2$$

has the Mordell-Weil group of rank 2, generated by

$$P_1=(0,\,t) \quad \text{and} \quad P_2=(1,\,t)\,.$$

When we specialize t to any rational number, $E^{(t)}$ is an elliptic curve over $\boldsymbol{Q}$ (note that the discriminant $-2^4(27t^4-4)$ never vanishes for any $t\in\boldsymbol{Q}$). The points $P_1^{(t)}$ and $P_2^{(t)}$ are independent except for a finite number of t (such as $t=0$, 1, etc.) and we have

$$\lim_{h(t)\to\infty}\det(\langle P_i^{(t)},\,P_j^{(t)}\rangle_{can}/h(t))=1/12\,.$$

EXAMPLE (D_4). Take $(d_1,\cdots,d_4)=(1,2,3,4)$. Then the elliptic curve E has the equation

$$y^2=x^3-x(t^2+27)+(10\,t^2+48\,t+90)\,.$$

Then $E(\boldsymbol{Q}(t))$ has rank 4 and it is generated by

$$\begin{aligned} P_1 &= (9,\,t+24)\\ P_2 &= (6,\,2\,t+12)\\ P_3 &= (1,\,3\,t+8)\\ P_4 &= (t+3,\,4\,t+6)\,. \end{aligned}$$

For the specialized curves, we have rank $E^{(t)}(\boldsymbol{Q})\geqq 4$ for almost all $t\in\boldsymbol{Q}$ and

$$\lim_{h(t)\to\infty}\det(\langle P_i^{(t)},\,P_j^{(t)}\rangle_{can}/h(t))=1/64\,.$$

EXAMPLE (E_6). Take $(a_1,\cdots,a_6)=(0,1,3,7,11,21)\in\boldsymbol{Q}^6$. Then we have

$$\begin{aligned} E:\,y^2 = x^3&+x(-381\,t^2+202752\,t-36577584)\\ &+t^4+427420\,t^2-319993344\,t+61357067136\,. \end{aligned}$$

The Mordell-Weil group $E(\boldsymbol{Q}(t))$ is free of rank 6, and the 6 generators P_i of $E(\boldsymbol{Q}(t))\cong E_6^*$ corresponding to the given values of a_i are as follows:

$$\begin{aligned} P_1 &= (6313/4,\,t^2-695573/8)\\ P_2 &= (t+1788,\,t^2-190\,t-40896)\\ P_3 &= (3\,t+1420,\,t^2-558\,t+110816)\\ P_4 &= (7\,t+12,\,t^2-1162\,t+246816)\\ P_5 &= (11\,t-1092,\,t^2-1430\,t+316224)\\ P_6 &= (21\,t-5252,\,t^2+630\,t-329563)\,. \end{aligned}$$

Furthermore, for the specialized curves, we have rank $E^{(t)}(\boldsymbol{Q})\geqq 6$ for almost all $t\in\boldsymbol{Q}$ and

$$\lim_{h(t)\to\infty}\det(\langle P_i^{(t)},\,P_j^{(t)}\rangle_{can}/h(t))=1/192\,.$$

We insert a remark about the 27 lines on a cubic surface. For an elliptic curve over $\boldsymbol{Q}(t)$ having the Mordell-Weil lattice of type E_6, the associated elliptic surface can be blown down to a smooth cubic surface defined over $\boldsymbol{Q}$ so that the 27 minimal sections (i.e. those corresponding to the 27 rational points mentioned in Theorem (E_6)) are mapped to the 27 lines on this cubic surface. Therefore these 27 lines are all defined over $\boldsymbol{Q}$. The existence of such a cubic surface over $\boldsymbol{Q}$ is classically known, but our construction provides explicit examples of such in a systematic way.

EXAMPLE (E_7). Take $(c_1, \cdots, c_7)=(1, 2, 4, 8, 16, 32, 64)\in\boldsymbol{Q}^7$. Then we have

$$\begin{aligned} E: y^2 = x^3&+x(t^3-2716410100150129/27\cdot t \\ &\qquad -28171549086867743575 1762/3^6) \\ &+8878/3\cdot t^4+1195761874250/27\cdot t^3 \\ &+16664903183774046 86/9\cdot t^2 \\ &+20193960549267845801903566/3^7\cdot t \\ &-1721910568378418619666559349151361 6/3^9 . \end{aligned}$$

The Mordell-Weil group $E(\boldsymbol{Q}(t))$ is free of rank 7, and the 7 generators P_i of $E(\boldsymbol{Q}(t))\cong E_7^*$ corresponding to the given values of c_i are as follows:

$$\begin{aligned} P_1 &= (-8875/3\cdot t-494991007099/27, \\ &\quad t^2+287657546/9\cdot t+17764798463061529/81), \\ P_2 &= (-8866/3\cdot t-493630525042/27, \\ &\quad 2t^2+434245276/9\cdot t+22809130472754890/81), \\ P_3 &= (-8830/3\cdot t-490138015714/27, \\ &\quad 4t^2+714936314/9\cdot t+32207272905385006/81), \\ P_4 &= (-8686/3\cdot t-478143731698/27, \\ &\quad 8t^2+1297687702/9\cdot t+52177541751701366/81), \\ P_5 &= (-8110/3\cdot t-427412515282/27, \\ &\quad 16t^2+2447266958/9\cdot t+91486391172386950/81), \\ P_6 &= (-5806/3\cdot t-224940010642/27, \\ &\quad 32t^2+4036998526/9\cdot t+107654483240065190/81), \\ P_7 &= (+3410/3\cdot t+584853492206/27, \\ &\quad 64t^2+4740279134/9\cdot t-77609819934613274/81). \end{aligned}$$

The specialized elliptic curve $E^{(t)}(\boldsymbol{Q})$ has rank $\geqq 7$ for almost all $t\in\boldsymbol{Q}$, and the rational points $P_i^{(t)}$ have the regulator asymptotic to $h(t)^7/256$ as $h(t)\to\infty$.

The above examples for the case (E_6) or (E_7) are constructed from the data $(a_i)_{i\leq 6}$ or $(c_i)_{i\leq 7}$ satisfying the (stronger) non-degeneracy condition $\delta_1\neq 0$. Likewise, we have given the first example for the case (E_8) in [**S2**] corresponding to the data $u_i=2^{i-1}$ $(1\leqq i\leqq 8)$ which satisfies the condition $\delta_1\neq 0$. (Indeed, Theorem 7.2 of [**S1**] has been stated with this stronger assumption. Thus Theorem (E_8) given above is not only more explicit but also stronger than the previously announced one. Note that δ_0 is a factor of δ_1 in this case.)

Below we give a new example for (E_8) corresponding to the prescribed data $u_i=1$ $(1\leqq i\leqq 8)$, which satisfies the condition $\delta_0\neq 0$ but $\delta_1=0$. We have much smaller coefficients here than in [**S2**].

EXAMPLE (E_8). Let $u_i=1$ for $i=1,\cdots,8$. Then the 120 "positive roots" u_j take the value 1 8-times, 2, $\cdots$, or 7 7-times, and so on; symbolically, they are:

$$(*)\qquad \begin{aligned}&1^8,\ \{2,3,4,5,6,7\}^7,\ \{8,9,10,11\}^6,\ \{12,13\}^5,\ \{14,15,16,17\}^4,\\ &\{18,19\}^3,\ \{20,21,22,23\}^2,\ \{24,25,26,27,28,29\}^1.\end{aligned}$$

Hence $\delta_0\neq 0$ and we can apply Theorem (E_8) to obtain an elliptic curve E over $\boldsymbol{Q}(t)$ with rank $E(\boldsymbol{Q}(t))=8$. The equation of E reads:

$$\begin{aligned}y^2 = {}& x^3+x(-310\,t^3+243896065\,t^2-60857017136860\,t\\ &+13936180986780637484/3)\\ &+t^5-2763436738910/3\cdot t^3+16813002074529175 40/3\cdot t^2\\ &-38455063890842840105 7560/3\cdot t\\ &+282412962406880649939736350128/27,\end{aligned}$$

The 8 generators P_i of $E(\boldsymbol{Q}(t))$ are given as follows:

$$\begin{aligned}P_1 = {}& (t^2-541045\,t+218476650754/3,\\ & t^3-811722\,t^2+219092370780\,t-19661726638639000),\\ P_2 = {}& (t^2-618805\,t+286705607554/3,\\ & t^3-928362\,t^2+287022107100\,t-29551900557554200),\\ P_3 = {}& (t^2-651925\,t+319030396354/3,\\ & t^3-978042\,t^2+318964426140\,t-34686244462893400),\\ P_4 = {}& (t^2-682165\,t+348384666754/3,\\ & t^3-1023402\,t^2+348767821020\,t-39580648307551000),\\ P_5 = {}& (t^2-782965\,t+457679889154/3,\\ & t^3-1174602\,t^2+458789609820\,t-59594315820808600),\end{aligned}$$

$$P_6 = (t^2-951445\,t+673629129154/3,$$
$$t^3-1427322\,t^2+676331322780\,t-106406856287968600),$$
$$P_7 = (t^2-1206325\,t+1079980986754/3,$$
$$t^3-1809642\,t^2+1085727346140\,t-215998191424639000),$$
$$P_8 = (t^2-1569205\,t+1824534541954/3,$$
$$t^3-2353962\,t^2+1835670395100\,t-474295484395883800).$$

The coefficient of t^2 (resp. t^3) in the x (resp. y)-coordinate of each P_i is 1, as prescribed. The 8 points P_i are so arranged that the Gram matrix $(\langle P_i, P_j\rangle)$ is equal to the standard Cartan matrix of E_8 as in [**B**]. We note that there are altogether 240 rational points P of the above form, and the t^2-coefficients of x-coordinate of P can be read off from $(*)$: there are so many P's corresponding to a given value in $(*)$ as the multiplicity there indicates.

As before, the specialized elliptic curve $E^{(t)}(\boldsymbol{Q})$ has rank $\geqq 8$ for almost all $t \in \boldsymbol{Q}$, and the rational points $P_i^{(t)}$ have the regulator asymptotic to $h(t)^8/256$ as $h(t)\to\infty$.

4. General outline of the proof.

We start from the elliptic curve E_λ over $K=k(t)$

$$y^2 = x^3+x\cdot p(t)+q(t) \tag{4.1}$$
$$\lambda = (p_i, q_j) \in \boldsymbol{A}^r$$

which is given in the introduction by one of the equations (E_8) $(=(1.6))$, (E_7), (E_6), (D_4) or (A_2). The ground field k is supposed to be an algebraically closed field of characteristic 0 containing p_i and q_j (cf. Remark at the end of this section).

Let

$$f : S_\lambda \longrightarrow \boldsymbol{P}^1 \tag{4.2}$$

denote the associated elliptic surface (the Kodaira-Néron model) of E_λ/K. In general, an elliptic surface of the form (4.1) is a rational surface, provided that $p(t)$ and $q(t)$ are polynomials in t of degree $\leqq 4$ and $\leqq 6$. (This follows from the canonical bundle formula of an elliptic surface and Castelnuovo's rationality criterion.) In particular, our S_λ is a rational elliptic surface, and hence we can make use of the basic results on the Mordell-Weil lattice of such a surface (cf. [**S1**, II], [**S5**, § 10]).

First let us briefly review the generalities on Mordell-Weil lattices, fixing some notation (cf. [**S1**, I], [**S5**, § 7-9]).

In general, consider an elliptic surface $f: S \to C$ with the generic fibre E over $K=k(C)$ where S (or C) is a smooth projective surface (or curve) defined over an algebraically closed field k of arbitrary characteristic and $k(C)$ denotes the function field of C. Then the global sections of $f: S \to C$ are in a natural one-to-one correspondence with the K-rational points of E so that we identify $E(K)$ with the group of sections of f. For $P \in E(K)$, we denote by (P) the image curve of the section $P: C \to S$.

We can define a natural bilinear pairing on $E(K)$ as follows, by using intersection theory on the surface S.

Let $NS(S)$ be the Néron-Severi group of S, which is an indefinite integral lattice with respect to the intersection pairing $(D_1 \cdot D_2)$. Let T be the "trivial" sublattice of $NS(S)$, which is generated by the zero section and all the irreducible components of fibres. The quotient group $NS(S)/T$ is naturally isomorphic to $E(K)$. There is a unique map $\varphi: E(K) \to NS(S) \otimes \boldsymbol{Q}$ splitting this isomorphism such that $\mathrm{Im}(\varphi)$ is orthogonal to T. Now the orthogonal complement of T in $NS(S)$, $L=T^{\perp}$, is a negative-definite even integral lattice (by the Hodge index theorem and the adjunction formula). Then the map φ induces an injection of $E(K)/E(K)_{tor}$ into $L \otimes \boldsymbol{Q}$. For $P, Q \in E(K)$, we define

$$\langle P, Q\rangle = -(\varphi(P) \cdot \varphi(Q)). \tag{4.3}$$

The *Mordell-Weil lattice* of E/K or $f: S \to C$ is defined as $E(K)/E(K)_{tor}$ with the above pairing $\langle\, ,\rangle$. Further, let $E(K)^{\circ}$ be the subgroup of finite index in the Mordell-Weil group $E(K)$ consisting of those sections which pass through the same irreducible component of every fibre as the zero section. Then φ maps $E(K)^{\circ}$ isomorphically onto L, and we call it the *narrow Mordell-Weil lattice* of E/K or f, which is a positive-definite even integral lattice.

More explicitly, the pairing is given by the formula

$$\langle P, Q\rangle = \chi+(PO)+(QO)-(PQ)-\textstyle\sum_{v \in R} \mathrm{contr}_v(P, Q). \tag{4.4}$$

Here χ is the arithmetic genus of S and we write (PO) for the intersection number $((P)\cdot(O))$, and similarly for (QO) or (PQ). R is the set of reducible fibres of f, and for each $v \in R$, the local contribution $\mathrm{contr}_v(P, Q)$ is a rational number depending only on the type of the singular fibre $f^{-1}(v)$ and on its components hit by the sections (P) and (Q) (see below). In particular, we have

$$\langle P, P\rangle = 2\chi+2(PO)-\textstyle\sum_{v \in R} \mathrm{contr}_v(P) \tag{4.5}$$

and

$$\langle P, Q\rangle = \chi+(PO)+(QO)-(PQ) \in \boldsymbol{Z} \qquad \text{if } P \text{ or } Q \in E(K)^{\circ}.$$

Also the other data can be made more explicit in terms of the singular fibres. For each $v \in R$, write

$$f^{-1}(v) = \Theta_{v,0}+\textstyle\sum_{i\geq 1}\mu_{v,i}\Theta_{v,i} \qquad (\mu_{v,0}=1) \tag{4.6}$$

where $\Theta_{v,i}$ $(0\leqq i\leqq m_v-1)$ are the irreducible components, m_v being their number, such that $\Theta_{v,0}$ is the unique component of $f^{-1}(v)$ meeting the zero section. Let F be any fixed fibre of f. Then the trivial sublattice T of $NS(S)$ is the direct sum of $\langle(O), F\rangle$ and $T_v=\langle\Theta_{v,i}\ (i\geqq 1)\rangle$ $(v\in R)$, with $\mathrm{rk}(T)=2+\sum_{v\in R}(m_v-1)$, and we have

$$\mathrm{rk}\,E(K) = \rho(S)-2-\textstyle\sum_{v\in R}(m_v-1)\,, \tag{4.7}$$

$$\det T = \Pi_{v\in R}m_v^{(1)}\,, \qquad m_v^{(1)} = \det T_v = \#\{i\geqq 0 \mid \mu_{v,i}=1\} \tag{4.8}$$

where $\rho(S)=\mathrm{rk}\,NS(S)$ is the Picard number of S. Further, if we denote by $A_v=((\Theta_{v,i}\Theta_{v,j}))_{i,j\geqq 1}$ the Gram matrix of T_v, then

$$\mathrm{contr}_v(P, Q) = (i, j)\text{-entry of } (-A_v)^{-1} \tag{4.9}$$

if P meets $\Theta_{v,i}$ and Q meets $\Theta_{v,j}$, with $i, j\geqq 1$, and $=0$ otherwise.

Now we suppose that S is a rational surface. In this case, we have $C=\boldsymbol{P}^1$, $K=k(t)$, $\chi=1$ and $\rho(S)=10$. Then the narrow Mordell-Weil lattice $M=E(K)^\circ$ is a positive-definite even integral lattice of rank

$$r = 8-\textstyle\sum_{v\in R}(m_v-1)\,. \tag{4.10}$$

The Mordell-Weil lattice $E(K)/E(K)_{tor}$ is isomorphic to the dual lattice M^* of M. We have $\det M^*=1/\det M$ and

$$\det M = \det T/n^2, \qquad \det T = \Pi_{v\in R}m_v^{(1)} \tag{4.11}$$

where n is the order of the torsion subgroup $E(K)_{tor}$. In particular, the Mordell-Weil group is torsion-free if $\det T$ is square-free.

When E is defined by a Weierstrass equation such as (4.1), a rational point $P=(x, y)$ in $E(K)$ has the property $(PO)=0$ if and only if x, y are polynomials in t of degree at most 2 or 3, i.e.,

$$x = gt^2+at+b, \qquad y=ht^3+ct^2+dt+e\,. \tag{4.12}$$

Now, going back to the situation at the beginning of this section, we describe the general outline of the proof of the theorems stated in § 2. It will be done in each case in the following steps.

Step 1. First we determine the singular fibre $f^{-1}(\infty)$ of f at $t=\infty$. Letting $s=1/t$, $X=x/t^2$, $Y=y/t^3$, we rewrite (4.1) as

$$Y^2 = X^3+X\cdot P(s)+Q(s) \tag{4.13}$$

where $P(s)=p(t)/t^4$ and $Q(s)=q(t)/t^6$ are polynomials in s. (Later (4.13) will be referred to as the "∞-model" of (4.1).) The type of the singular fibre $f^{-1}(\infty)$

is determined by the order of the discriminant

$$\Delta = -2^4 \cdot (4P(s)^3 + 27Q(s)^2)$$

at $s=0$ (cf. [**K**], [**N2**], [**T1**]). The result is summarized as follows:

(4.14)

case	(E_8)	(E_7)	(E_6)	(D_4)	(A_2)
type	II	III	IV	I_0^*	IV^*
m_∞	1	2	3	5	7
T_∞	$\{0\}$	A_1^-	A_2^-	D_4^-	E_6^-
$\det T_\infty$	1	2	3	4	3

Here $A_1^-, \cdots$ denotes the root lattice $A_1, \cdots$ with opposite inner product.

Step 2. Until Step 5, assume that (#) $f: S_\lambda \to \boldsymbol{P}^1$ has no reducible singular fibres other than $f^{-1}(\infty)$. This is certainly the case for λ generic. Under this assumption, the Mordell-Weil group $E_\lambda(K)$ is torsion-free and the structure of the Mordell-Weil lattice on $E_\lambda(K)$ is completely determined. It is isomorphic to the dual lattice of the root lattice corresponding to the type of the equation we started with. Namely we have

$$E_\lambda(K) \cong E_8,\ E_7^*,\ E_6^*,\ D_4^* \text{ or } A_2^*, \tag{4.15}$$

according to the case (E_8), (E_7), (E_6), (D_4) or (A_2) (cf. [**S5**, § 10], [**OS**]). The minimal norm and the number of the minimal vectors in these lattices are well-known (cf. [**CS**, Ch. 4]):

(4.16)

minimal norm	2	3/2	4/3	1	2/3
# min. vectors	240	56	54	24	6.

Compare the minimal norms with the following values of $\mathrm{contr}_\infty(P)$ for P meeting $\Theta_{\infty,i}$ for some $i \geqq 1$, computed by (4.9) (cf. [**S5**, (8.16)]:

(4.17)

$\mathrm{contr}_\infty(P)$	0	1/2	2/3	1	4/3.

By (4.5), we see that a minimal section of $E(K)$ takes the form (4.12).

Step 3. Next we consider the specialization homomorphism

$$sp_\infty : E_\lambda(K) \longrightarrow f^{-1}(\infty)^\# \tag{4.18}$$

which maps each K-rational point P of E_λ to the unique intersection point of (P) and $f^{-1}(\infty)$. In the above, $f^{-1}(\infty)^\#$ is the smooth part of $f^{-1}(\infty)$, which has a natural structure of algebraic group over k. More explicitly, it is a direct product of the additive group $\boldsymbol{G}_a$ and a finite abelian group H of order $m_\infty^{(1)} = \det T_0$, and we have

$$H \cong \{0\},\ \boldsymbol{Z}/2,\ \boldsymbol{Z}/3,\ (\boldsymbol{Z}/2)^{\oplus 2} \text{ or } \boldsymbol{Z}/3\,, \tag{4.19}$$

according to the case $(E_8), \cdots, (A_2)$ (cf. [**K**], [**N2**], [**T1**]).

Now we take the minimal sections $P \in E_\lambda(K)$ and consider $sp_\infty(P)$. It turns out that the $\boldsymbol{G}_a$-component of $sp_\infty(P)$, say $sp'_\infty(P)$, is a very important parameter, which determines P for λ generic.

Step 4. Next we choose a basis $\{P_\nu \mid 1 \leqq \nu \leqq r\}$ of $E_\lambda(K)$ consisting of minimal sections, and let

$$u_\nu = sp'_\infty(P_\nu)\,. \tag{4.20}$$

Then $(u_1, \cdots, u_r)$ completely determines the coefficients p_i, q_j of the equation (4.1) of the elliptic curve E_λ. This step is crucial.

For the case (E_r) $(r=6, 7, 8)$, we consider the *universal polynomial of type* E_r

$$\Phi_{E_r}(X) = \Pi_{\nu=1}^{N}(X-u_\nu), \qquad u_\nu = sp'_\infty(P_\nu)\,, \tag{4.21}$$

where P_ν $(1 \leqq \nu \leqq N)$ denote all the minimal sections in $E_\nu(K) \cong E_r^*$. On the one hand, this can be expressed by the elementary symmetric functions of u_ν's, which are obviously the invariants of the Weyl group $W(E_r)$. On the other hand, we can prove that it is a polynomial with coefficients in $\boldsymbol{Q}[\lambda] = \boldsymbol{Q}[p_i, q_j]$, by means of *elimination method*. Comparing the two expressions, we obtain the relations of p_i and q_j as the fundamental invariants of $W(E_r)$, as stated in Theorem (E_r).

Step 5. Finally we note that the non-degeneracy assumption such as $\delta_0(u) \neq 0$ in the theorems is equivalent to the assumption (#) in the Step 2 that $f: S_\lambda \to \boldsymbol{P}^1$ has no reducible fibres other than $f^{-1}(\infty)$.

Then, specializing $(u_1, \cdots, u_r)$ to some rational values in $\boldsymbol{Q}^r$ such that $\delta_0(u) \neq 0$, we complete the proof.

For the case (A_2) and (D_4), we can skip or reverse some of the above steps and verify the theorem in a more elementary way.

REMARK. This method of the proof will make it clear that we can replace $\boldsymbol{Q}$ by any field of characteristic 0 in the statement of the theorems, or even by one of characteristic p, provided that p is different from a small number of prime numbers which come into the denominators of some expression in the course of the proof. The primes to be avoided are the following:

$p = 2, 3$	in case (A_2) or (D_4)
$p = 2, 3, 5, 7$	in case (E_6)
$p \leqq 11$ or $p = 29, 1229$	in case (E_7)

$$p \leqq 19 \text{ or } p = 41, 61, 199 \qquad \text{in case } (E_8).$$

5. Case (A_2).

We begin with the case (A_2), where the elliptic curve $E=E_\lambda$ is given by

$$(5.1) \qquad y^2 = x^3+p_0x+q_0+t^2$$
$$\lambda = (p_0, q_0) \in \boldsymbol{A}^2$$

Letting b_1, b_2, b_3 be the roots of $x^3+p_0x+q_0=0$, we have

$$(5.2) \qquad \begin{cases} p_0 = b_1b_2+b_2b_3+b_3b_1 & (b_1+b_2+b_3=0) \\ q_0 = -b_1b_2b_3 . \end{cases}$$

The assumption (#) is that

$$(5.3) \qquad b_1, b_2, b_3 \text{ are distinct,}$$

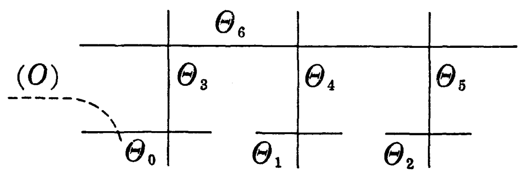
which is equivalent to the condition:

$$(5.3)' \qquad \Delta_0 = 4p_0^3+27q_0^2 \neq 0 .$$

Step 1. The elliptic surface $f: S_\lambda \to \boldsymbol{P}^1$ has a singular fibre of type IV* at $t=\infty$:

$$(5.4) \qquad f^{-1}(\infty) = \Theta_0+\Theta_1+\Theta_2+2(\Theta_3+\Theta_4+\Theta_5)+3\Theta_6 ,$$

where the irreducible components Θ_i are smooth rational curves with self-intersection number -2 intersecting other components as in the figure below. We always choose Θ_0 to be the unique component meeting the zero-section (O).



$m_\infty = 7$
$m_\infty^{(1)} = 3$

Step 2. Let us check the "Step 5" first.

LEMMA 5.1. *There are no reducible fibres of* $f: S_\lambda \to \boldsymbol{P}^1$ *other than* $f^{-1}(\infty)$ *under the assumption* (5.3).

PROOF. The discriminant of (5.1) is

$$\Delta = 4p_0^3+27(q_0+t^2)^2 = \Delta_0+54q_0t^2+27t^4 .$$

By (5.3)′, Δ has either 4 simple roots ($p_0 \neq 0$) or 2 double roots ($p_0=0$). Hence the singular fibre $f^{-1}(v)$ at $v \neq \infty$ is either of type I_1 or II (a rational curve with a node or cusp) (cf. [**K**], [**N2**], [**T1**]), hence irreducible. q.e.d.

It follows from (4.10), (4.11) that the rank of $E(K)$ is $r=2$ and $\det T=m_\infty^{(1)}=3$. Hence $E(K)$ is torsion-free (3 is square-free) and we have $E(K)^\circ \cong A_2$ and $E(K)\cong A_2^*$ by the general theory. But we see this more directly below.

Step 3. Now we look at the 3 obvious points of $E(K)$:

$$P_i=(b_i, t) \qquad (i=1, 2, 3). \tag{5.5}$$

Since they are collinear, lying on the line $y=t$, we have

$$P_1+P_2+P_3=0 \tag{5.6}$$

by the definition of the group law on E.

Let us see how the section (P_i) intersects the singular fibre $f^{-1}(\infty)$. At any rate, a section meets the smooth part $f^{-1}(\infty)^\#$, and

$$f^{-1}(\infty)^\# = \Theta_0^\# \cup \Theta_1^\# \cup \Theta_2^\# \cong \boldsymbol{G}_a \times \boldsymbol{Z}/3\boldsymbol{Z} \tag{5.7}$$

where $\Theta_i^\#$ is Θ_i minus the points meeting other Θ_j and corresponds to the coset $\boldsymbol{G}_a \times \bar{i}$ $(i=0, 1, 2)$.

LEMMA 5.2. *All the* 3 *sections* (P_i) *intersect the same non-identity component of* $f^{-1}(\infty)$, Θ_1 *or* Θ_2.

PROOF. In terms of the ∞-model of (5.1) (cf. (4.13)), we have $P_i=(b_i s^2, s^2)$, which passes the singular point $(0, 0)$ of the cuspidal cubic $Y^2=X^3$ at $s=0$. The latter is the fibre $f'^{-1}(\infty)$, where we denote by $f': S'\to \boldsymbol{P}^1$ the associated Weierstrass fibration; namely, S' is the normal surface obtained from S by collapsing all the non-identity components $\bigcup_{i\geq 1}\Theta_i$ in $f^{-1}(\infty)$. Thus each (P_i) in S must meet either Θ_1 or Θ_2.

Suppose, for instance, that (P_1) meets Θ_1 and (P_2) meets Θ_2. Then P_3 would meet Θ_0 by (5.6) and (5.7), a contradiction. Hence all the P_i $(i=1, 2, 3)$ meet one and the same component. q.e.d.

Step 4. Let us rename Θ_1 as the component meeting all P_i.

LEMMA 5.3. *Let*

$$sp_\infty : E(K) \longrightarrow f^{-1}(\infty)^\# = \boldsymbol{G}_a \times \boldsymbol{Z}/3$$

be the specialization homomorphism. Then we have

$$sp_\infty(P_i) = \left(-\frac{b_i}{2}, \bar{1}\right) \qquad (i=1, 2, 3). \tag{5.8}$$

PROOF. To compute the $\boldsymbol{G}_a$-component of $sp_\infty(P_i)$, it is enough to compute $sp_\infty(Q)$ for $Q=3P_i\in E(K)^\circ$. This can be done directly by using the addition formula (5.9) below, but we proceed in a slightly different way.

In general, if $P_i=(x_i, y_i)$ $(i=1, 2)$ are two points of E, the sum $P=P_1+P_2$ has the coordinates x, y given by

$$(5.9)\qquad \begin{cases} x=-x_1-x_2+m^2, & m=(y_1-y_2)/(x_1-x_2), \\ y=-y_1-m\,(x-x_1). \end{cases}$$

Applying this to $Q_1=P_2-P_3\in E(K)^\circ$, we have

$$\begin{cases} x(Q_1)=-(b_2+b_3)+\{2/(b_2-b_3)\}^2\cdot t^2 \\ y(Q_1)=-3b_1/(b_2-b_3)\cdot t-\{2/(b_2-b_3)\}^3\cdot t^3 . \end{cases}$$

Rewriting these in terms of the coordinates X, Y of the ∞-model (4.13), we have

$$sp_\infty(Q_1)=(X/Y)|_{s=0}=-(b_2-b_3)/2 .$$

Similarly, for $Q_2=P_3-P_1\in E(K)^\circ$, we have

$$sp_\infty(Q_2)=-(b_3-b_1)/2 .$$

By (5.6), we have $Q_1=P_1+2P_2$ and $Q_2=-2P_1-P_2$ so that $3P_1=-(Q_1+2Q_2)$. Hence

$$sp_\infty(3P_1)=(b_2-b_3)/2+(b_3-b_1)=-3b_1/2 .$$

This proves that the $\boldsymbol{G}_a$-component of $sp_\infty(P_1)$ is $-b_1/2$, as asserted. q.e.d.

COROLLARY 5.4. *The 3 sections (P_i) $(i=1, 2, 3)$ are disjoint from each other and also from the zero section (O).*

PROOF. Clearly (P_i) and (P_j) $(i\neq j)$ do not meet at $t\neq\infty$, because $b_i\neq b_j$ by assumption. Further they cannot meet at ∞ by (5.8). It is easy to see that (P_i) and (O) are disjoint. q.e.d.

LEMMA 5.5. *The value of the pairing $\langle P_i, P_j\rangle$ is as follows:*

$$(5.10)\qquad \langle P_i, P_j\rangle=\begin{cases} 2/3 & (i=j) \\ -1/3 & (i\neq j). \end{cases}$$

In particular, $\det(\langle P_i, P_j\rangle)_{i,j\leq 2}=1/3$.

PROOF. This follows from (4.4), (4.5) and Corollary 5.4, since we have $\mathrm{contr}_\infty(P_i, P_j)=4/3$. The latter is in the table (4.17) for $i=j$, and we have the same value for $i\neq j$ because all sections P_i pass the same component Θ_1 in the singular fibre $f^{-1}(\infty)$ of type IV*. q.e.d.

Now the rational points (or sections) $Q_1, Q_2\in E(K)^\circ$, given in the proof of Lemma 5.3, have Gram matrix

$$(5.11)\qquad (\langle Q_i, Q_j\rangle)_{i,j\leq 2}=\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}.$$

This clearly shows the isomorphism of lattices:

$$E(K)^{\circ} \cong A_2 \qquad \text{and} \qquad E(K) \cong A_2^*, \tag{5.12}$$

proving also that $\{Q_1, Q_2\}$ and $\{P_1, P_2\}$ give the generators of the Mordell-Weil lattices $E(K)^{\circ}$ and $E(K)$. Note that $\pm P_i$ $(i=1, 2, 3)$ correspond to the 6 minimal vectors of A_2^* and P_i-P_j $(i\neq j)$ to the 6 minimal vectors (the 6 "roots") of A_2.

This completes the analysis of the case (A_2), and in particular, the proof of Theorem (A_2).

6. Case (D_4).

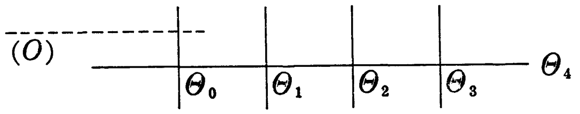
We consider the elliptic curve $E=E_\lambda$

$$\begin{aligned} y^2 &= x^3+x(p_0-t^2)+q_0+q_1t+q_2t^2 \\ \lambda &= (p_0, q_0, q_1, q_2)\in \boldsymbol{A}^2 . \end{aligned} \tag{6.1}$$

Step 1. The associated elliptic surface $f: S_\lambda\to \boldsymbol{P}^1$ has a singular fibre of type I_0^* at $t=\infty$:

$$f^{-1}(\infty) = \Theta_0+\Theta_1+\Theta_2+\Theta_3+2\Theta_4 \tag{6.2}$$

where we use the similar notation as before; see the figure below.



$m_\infty = 5$
$m_\infty^{(1)} = 4$

Step 2. Until Step 5, we assume that $(\#)$ f has no reducible fibres other than $f^{-1}(\infty)$. Then we have by (4.10) and (4.11)

$$r = 8-(5-1) = 4, \qquad \det T = m_\infty^{(1)} = 4 .$$

This implies that the Mordell-Weil group $E(K)$ is torsion-free of rank 4 such that $\det E(K)^{\circ}=4$. (Indeed, if n is the order of $E(K)_{tor}$, then n^2 must divide 4. Hence $n=1$ or 2. If $n=2$, then $E(K)^{\circ}$ would be an even unimodular lattice of rank 4, a contradiction.) It follows that (under the assumption $(\#)$)

$$E(K)^{\circ} \cong D_4 \qquad \text{and} \qquad E(K) \cong D_4^* . \tag{6.3}$$

In particular, the minimal norm of $E(K)$ is 1 and the number of the minimal sections is 24.

The minimal sections are characterized as follows:

LEMMA 6.1. *Let $P\in E(K)$, $P\neq O$. Then we have $\langle P, P\rangle=1$ if and only if (P) is disjoint from (O) and Θ_0. In terms of the coordinates $P=(x, y)$, this is* *so if and only if*

$$(6.4) \qquad x = at+b, \qquad y = dt+e \qquad (a, b, d, e \in k).$$

Thus there exist exactly 24 *rational points of this form.*

PROOF. We have

$$\langle P, P\rangle = 2+2(PO)-\mathrm{contr}_\infty(P)$$

and, for the singular fibre of type I_0^*,

$$(6.5) \qquad \mathrm{contr}_\infty(P) = \begin{cases} 0 & \text{if } (P) \text{ meets } \Theta_0 \\ 1 & \text{otherwise.} \end{cases}$$

Hence the first assertion holds. Next, by (4.12), $P=(x, y)$ is of the form (cf. [**S1**, Lemma 3.1] or [**S3**, Proposition 5.1]):

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

If (P) does not meet Θ_0 (i.e. it meets Θ_i for some $i=1$, 2 or 3), then it passes the cusp (0, 0) of the cuspidal cubic at $t=\infty$ (cf. the arguments given for the case (A_2)), and hence we have $g=h=0$. Moreover, we have $c=0$ from the equation (6.1), hence P is of the form (6.4). The converse is easily verified.

q.e.d.

Step 3. Next let us consider the specialization map:

$$sp_\infty\colon E(K) \longrightarrow f^{-1}(\infty)^\#\,.$$

Since the singular fibre $f^{-1}(\infty)$ is of type I_0^*, its smooth part is

$$(6.6) \qquad f^{-1}(\infty)^\# = \cup_{i=0}^3 \Theta_i^\# \cong \boldsymbol{G}_a\times(\boldsymbol{Z}/2)^{\oplus 2}\,.$$

If $\Theta_i^\#$ corresponds to the coset $\boldsymbol{G}_a\times\theta$, then write $[\Theta_i]=\theta\in(\boldsymbol{Z}/2)^{\oplus 2}$.

LEMMA 6.2. *The* 24 *rational points* $(at+b, ct+d)$ *are grouped into the* 3 *sets of* 8 *points, corresponding to* $a=0$, 1 *or* -1. *The* 8 *points in each set pass through the same irreducible component* Θ_i, *so we can label* Θ_i *so that* $\Theta_1, \Theta_2, \Theta_3$ *correspond to* $a=0, 1, -1$. *Then we have*

$$(6.7) \qquad sp_\infty(P) = \begin{cases} (d, [\Theta_1]) & \text{if } a=0 \\ (-d/2, [\Theta_i]) & \text{if } a=\pm 1 \ (i\geqq 2)\,. \end{cases}$$

PROOF. Let us analyse the condition for $P=(at+b, *)$ to belong to $E(K)$. It is necessary and sufficient for this that

$$(6.8) \qquad (at+b)^3+(at+b)(p_0-t^2)+(q_0+q_1t+q_2t^2)$$

is a square in $k[t]$. The coefficient of t^3 must vanish, so we have

$$a^3-a=0, \qquad \text{i.e.,} \quad a=0,\ 1 \text{ or } -1.$$

First consider the case $a=0$. Then (6.8) is a square if and only if b is a root of the quartic equation

$$h(X)=(X^3+p_0X+q_0)(X-q_2)+q_1^2/4=0. \tag{6.9}$$

For any such b, $P=(b, dt+e)$ belongs to $E(K)$ if and only if

$$d^2=-b+q_2, \qquad e^2=b^3+p_0b+q_0, \qquad 2de=q_1, \tag{6.10}$$

and hence there are exactly 2 choices of (d, e). (The case $d=e=0$ does not occur, because then P becomes a torsion point of order 2.) Thus we obtain 8 points of the form $(b, dt+e)$, provided that 4 roots of (6.9) are distinct.

The case $a=1$ or -1 can be treated in the same way, and we obtain (at most) 8 points each, of the form $(\pm t+b, dt+e)$.

Since the number of minimal vectors in D_4^* is 24, the $3\cdot 8=24$ points so obtained must be all distinct. In particular, $h(X)$ must have 4 distinct roots $b_1, \cdots, b_4$ under (#).

Next we see that the 8 points for each value of a pass through the same irreducible component Θ_i (some $i\geqq 1$), by checking that their differences intersect the identity component Θ_0 at $t=\infty$. For instance, we have by the addition formula (5.9)

$$X(P_1-P_2)|_{s=0}=1/(d_1-d_2)^2, \qquad Y(P_1-P_2)|_{s=0}=1/(d_1-d_2)^3$$

for $P_i=(b_i, d_it+e_i)$, in terms of the ∞-model (cf. (4.13)). This shows first that P_1-P_2 intersects Θ_0 at $t=\infty$ and that

$$sp_\infty(P_1-P_2)=d_1-d_2\neq 0. \tag{6.11}$$

In other words, P_1 and P_2 intersect the same component, say Θ_j ($j\geqq 1$), at distinct points.

Similarly it is easy to check that two sections corresponding to different values of $a=0,\ 1,\ -1$ meet the different components of $f^{-1}(\infty)$. Hence we may suppose that the 3 components $\Theta_1, \Theta_2, \Theta_3$ correspond to $a=0,\ 1,\ -1$.

Finally, to prove the formula (6.7), we have only to compute $sp_\infty(2P)\in \boldsymbol{G}_a$ (note that $2P\in E(K)^\circ$). By the addition formula again, we see easily

$$sp_\infty(2P)=2d/(1-3a^2),$$

which implies (6.7). q.e.d.

COROLLARY 6.3. *For $P_i=(b_i, d_it+e_i)\in E(K)$ ($i=1, \cdots, 4$), the Gram matrix $(\langle P_i, P_j\rangle)$ is equal to the identity matrix of degree 4. Hence $P_1, \cdots, P_4$ are independent and they generate a subgroup of index 2 in $E(K)$. If Q is any rational* *point of the form* $(\pm t+b', d't+e')$, *then* P_1, P_2, P_3 *and* Q *generate the full Mordell-Weil group* $E(K)$.

PROOF. By the above lemma, the sections (P_i) are disjoint from each other and also from the zero section. We can compute $\langle P_i, P_j\rangle$ by (4.4), (4.5) and (6.5), noting that $\mathrm{contr}_\infty(P_i, P_j)=1$ for all i, j since all P_i pass through the same Θ_1. Hence the first assertion. Then $\det(\langle P_i, P_j\rangle)=1$, and since we know $\det(E(K))=1/4$, P_i generates a subgroup of index 2 in $E(K)$. Finally Q is not in this subgroup, since $\langle P_i, Q\rangle\equiv 1/2 \pmod 1$. Hence the last assertion. q.e.d.

Step 4. Let P_i $(i=1, \cdots, 4)$ be as in Corollary 6.3. Since b_i are the 4 roots of $h(X)=0$ in (6.9), the relation of the roots and coefficients give

$$\text{(6.12)}\qquad \begin{cases} b_1+\cdots+b_4=q_2 \\ b_1b_2+\cdots=p_0 \\ b_1b_2b_3+\cdots=p_0q_2-q_0 \\ b_1b_2b_3b_4=q_1^2/4-q_0q_2\,. \end{cases}$$

Using the relation $b_i=-d_i^2+q_2$ in (6.10), we can rewrite (6.12) as the relations of d_i. By a simple computation (which is *not* so tedious because it leads very naturally to the fundamental invariants of the Weyl group $W(D_4)$; cf. [**B**]), we have:

$$\text{(6.13)}\qquad \begin{cases} \sum_i d_i^2=3q_2 \\ \sum_{i<j}d_i^2d_j^2=p_0+3q_2^2 \\ \sum_{i<j<k}d_i^2d_j^2d_k^2=q_0+p_0q_2+q_2^3 \\ d_1d_2d_3d_4=\varepsilon q_1/2 \qquad (\varepsilon=\pm 1). \end{cases}$$

Step 5. Now we reverse the above arguments. Take arbitrary $d_1, \cdots, d_4$ such that (##) $d_1^2, \cdots, d_4^2$ are distinct. Then define q_2, p_0, q_0 and q_1 by (6.13). Letting $\lambda=(p_0, q_0, q_1, q_2)$, consider the elliptic curve E_λ and the elliptic surface S_λ defined by (6.1). Define also b_i, e_i by

$$b_i=-d_i^2+q_2, \qquad e_i=\varepsilon d_jd_kd_l \ (=q_1/2d_i \text{ if } d_i\neq 0)\,.$$

Then

$$P_i=(b_i, d_it+e_i) \qquad (i=1, \cdots, 4)$$

give 4 rational points of E_λ over $k_0(t)$, $k_0=\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0, \cdots, q_2)$, such that $sp_\infty(P_i)=(d_i, [\Theta_1])$. The Mordell-Weil lattice $E(K)$ will be isomorphic to D_4^*, once the condition (#) (that $f: S_\lambda\to\boldsymbol{P}^1$ has no reducible fibres other than $f^{-1}(\infty)$) is verified.

LEMMA 6.4. *The two conditions* (#) *and* (##) *are equivalent. In other words,* *there are no reducible fibres of* $f: S_\lambda \to \boldsymbol{P}^1$ *other than* $f^{-1}(\infty)$, *precisely when* $d_1^2, \cdots, d_4^2$ *are distinct.*

PROOF. We have seen in Steps 2 and 3 that the condition (#) implies that $b_1, \cdots, b_4$ are distinct, and the latter is equivalent to the condition (##). Let us show the converse: (##)⇒(#).

Assume for a moment that $d_1, \cdots, d_4$ are algebraically independent over $\boldsymbol{Q}$. Then $p_0, \cdots, q_2$ are so too, in which case it is obvious that f has no other reducible fibres at $t \neq \infty$. Then the narrow Mordell-Weil lattice $E_\lambda(K)^\circ$ is isomorphic to D_4 by (6.3).

Recall that the narrow Mordell-Weil lattice is isomorphic (up to the sign) to the orthogonal complement L of the trivial sublattice in $NS(S_\lambda)$. The 24 "roots" $Q \in E(K)^\circ \cong D_4$ define the 24 elements $D(Q)=(Q)-(O) \in NS(S_\lambda)$ such that

$$(6.14) \qquad (D\cdot D) = -2, \qquad (D\cdot(O)) = (D\cdot\Theta_i) = 0 \quad (\text{all } i \geqq 0).$$

Observe that $\{Q\}=\{\pm P_i \pm P_j \mid 1 \leqq i<j \leqq 4\}$, $\{P_i\}$ being as before. Now we specialize $d_1, \cdots, d_4$ in such a way that they still satisfy (##), then we still get 24 divisor classes $D=(Q)-(O)$ in $NS(S_\lambda)$ satisfying (6.14), using the 4 points $P_i=(b_i, d_i t+e_i)$. Therefore there is no room for the non-identity components $\Theta_{v,j}$ for $v \neq \infty$ (note $\Theta_{v,j}$ will satisfy (6.14) too). Thus there is no reducible singular fibres other than $f^{-1}(\infty)$. (Compare the arguments involving the "E_8-frame" in [**S4**]; here we implicitly considered the "D_4-frame".) q.e.d.

Finally, taking $(d_1, \cdots, d_4)$ in $\boldsymbol{Q}^4$ satisfying (##) and applying the above argument, we complete the proof of Theorem (D_4).

7. Preliminaries for the cases (E_r).

First we recall basic facts on the root lattices E_6, E_7 and E_8; we refer to [**B**, Ch. 6], [**CS**, Ch. 4] or [**M**, Ch. 4] for the details.

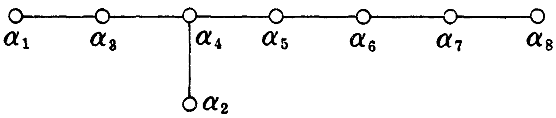
(i) The most fundamental of these three lattices is the root lattice E_8. It is characterized as the unique positive-definite even integral unimodular lattice of rank 8. The minimal norm is 2, and there are 240 minimal vectors ("roots") in E_8, which form the root system of type E_8 in the Euclidean space $E_8 \otimes \boldsymbol{R} = \boldsymbol{R}^8$. Any root spans a sublattice $\cong A_1$, and its orthogonal complement in E_8 defines the root lattice E_7, whose isomorphism class is independent of the choice of A_1. It has det=2 and 126 minimal vectors ("roots") of norm 2. Similarly, the orthogonal complement in E_8 of any sublattice isomorphic to A_2 defines the root lattice E_6, which is unique up to isomorphism. It has det=3 and 72 minimal vectors of norm 2.

(ii) The dual lattice L^* of a lattice L is the subgroup of $L \otimes \boldsymbol{Q}$ consisting of those elements x such that $\langle x, y\rangle \in \boldsymbol{Z}$ for all $y \in L$. We have $\det L = [L^* : L]$ for any integral lattice L. The root lattice E_8 is self-dual, since it is unimodular. The dual lattice E_7^* of E_7 has $\det = 1/2$ and 56 minimal vectors of norm $3/2$, and $[E_7^* : E_7] = 2$. The dual lattice E_6^* of E_6 has $\det = 1/3$ and 54 minimal vectors of norm $4/3$, and $[E_6^* : E_6] = 3$.

(iii) The automorphism group of E_8, $\mathrm{Aut}(E_8)$, is equal to the Weyl group $W(E_8)$, which is of order $2^{14}3^5 5^2 7$ and contains -1_8, with the quotient group $W(E_8)/\{\pm 1\}$ having a simple subgroup of index 2. Similarly we have $\mathrm{Aut}(E_7) = W(E_7)$, which is of order $2^{10}3^4 5\cdot 7$ and contains -1 such that $W(E_7)/\{\pm 1\}$ is a simple group. For E_6, we have $\mathrm{Aut}(E_6) = W(E_6)\cdot\{\pm 1\}$, $W(E_6)$ being of order $2^7 3^4 5$ and not containing -1; further $W(E_6)$ has a simple subgroup of index 2. According to the ATLAS, these simple groups are $U_4(2) \cong S_4(3)$, $S_6(2)$ and $O_8^+(2)$ for E_6, E_7 and E_8 respectively.

The Weyl group $W(E_r)$ acts transitively on the set of roots in E_r as well as on the set of minimal vectors in E_r^*, except that, in case $r=6$, $W(E_6)$ has 2 orbits there.

(iv) Now let $\{\alpha_1, \cdots, \alpha_r\}$ be a basis (or a system of simple roots) of E_r, which has the familiar Dynkin diagram:



For E_6 or E_7, ignore those α_j with $j > 6$ or 7.

If we denote by $\{\alpha_j \mid 1 \leqq j \leqq m\}$ all the "positive roots" of E_r, i.e., those roots which can be written as a linear combination of $\alpha_1, \cdots, \alpha_r$ with non-negative integral coefficients (cf. [**B**, tables at the end of Ch. 6]), then $\pm\alpha_j$ give all the roots of E_r. Thus $n = 2m$ is equal to the number of the roots, i.e., $n = 240$, 126 or 72 for $r = 8$, 7 or 6.

(v) Now choose a basis $\{u_1, \cdots, u_r\}$ of the dual lattice E_r^* consisting of minimal vectors. The Gram matrix of E_r^* is then given by

$$I_r = (\langle u_i, u_j\rangle)_{1\leq i,j\leq r} \qquad (r = 8, 7, 6)\,.$$

Let us denote by $\{u_i \mid 1 \leqq i \leqq N\}$ all the minimal vectors of E_r^*; thus $N = 240$, 56 or 54 according as $r = 8$, 7 or 6. We arrange $\{u_i\}$ so that they coincide with $\{\pm u_i \mid 1 \leqq i \leqq N/2\}$.

(vi) The symmetric algebra of E_r^* is identified with the polynomial ring $\boldsymbol{Z}[u_1, \cdots, u_r]$. Writing u_i and α_j as a $\boldsymbol{Z}$-linear combination of $u_1, \cdots, u_r$, we regard them as elements of $\boldsymbol{Z}[u_1, \cdots, u_r]$.

Definition 7.1. We define the following polynomial in X with coefficients in $\boldsymbol{Z}[u_1, \cdots, u_r]$:

$$\Phi_{E_r}(X) = \Pi_{i=1}^{N}(X-u_i) = \Pi_{i=1}^{N/2}(X^2-u_i^2), \tag{7.1}$$

which will be called the *universal polynomial of type* E_r.

Letting

$$\varepsilon_\nu = \nu\text{-th elementary symmetric function of } u_1, \cdots, u_N \tag{7.2}$$

$$\varepsilon'_\nu = \nu\text{-th elementary symmetric function of } u_1^2, \cdots, u_{N/2}^2, \tag{7.3}$$

we have $\varepsilon_\nu=0$ for ν odd and $\varepsilon_{2\nu}=(-1)^\nu\varepsilon'_\nu$. Obviously, we have

$$\Phi_{E_r}(X) = X^N + \sum_{\nu=1}^{N/2}\varepsilon_{2\nu}X^{N-2\nu}. \tag{7.4}$$

The coefficients ε_ν are invariant under $W(E_r)$ as polynomials in $u_1, \cdots, u_r$.

(vii) The structure of the ring of $W(E_r)$-invariants in $\boldsymbol{Q}[u_1, \cdots, u_r]$ is well-known. It is a graded polynomial ring generated by r homogeneous elements of weights

$$\begin{cases} 2, 8, 12, 14, 18, 20, 24, 30 & (r=8) \\ 2, 6, 8, 10, 12, 14, 18 & (r=7) \\ 2, 5, 6, 8, 9, 12 & (r=6). \end{cases} \tag{7.5}$$

(viii) As a by-product of the proof of Theorem (E_r) given in the next sections, we can prove that, for $r=8$ or 7, ε_w with w ranging over the weights in (7.5) form a set of *fundamental invariants* of $W(E_r)$. In other words, we obtain:

THEOREM 7.2.

$$\boldsymbol{Q}[u_1, \cdots, u_8]^{W(E_8)} = \boldsymbol{Q}[\varepsilon_2, \varepsilon_8, \varepsilon_{12}, \varepsilon_{14}, \varepsilon_{18}, \varepsilon_{20}, \varepsilon_{24}, \varepsilon_{30}] \tag{7.6}$$

$$\boldsymbol{Q}[u_1, \cdots, u_7]^{W(E_7)} = \boldsymbol{Q}[\varepsilon_2, \varepsilon_6, \varepsilon_8, \varepsilon_{10}, \varepsilon_{12}, \varepsilon_{14}, \varepsilon_{18}] \tag{7.7}$$

(ix) For the case of E_6, we slightly modify the notation as follows. We can choose $u_1, \cdots, u_6$ so that $\langle u_i, u_j\rangle \equiv 1/3 \pmod 1$ for all $i, j \leqq 6$, and arrange $\{u_i\}$ so that the same congruence holds for all $i, j \leqq N/2=27$. Thus $\{u_i \mid 1\leqq i\leqq 27\}$ and $\{-u_i \mid 1\leqq i\leqq 27\}$ give the 2 orbits mentioned in (iii). We redefine ε_ν as the ν-th elementary symmetric function of $u_1, \cdots, u_{27}$. Let

$$\begin{aligned} \Psi_{E_6}(X) &= \Pi_{i=1}^{27}(X-u_i) \\ &= X^{27} + \sum_{\nu=1}^{27}(-1)^\nu\varepsilon_\nu X^{27-\nu}. \end{aligned} \tag{7.8}$$

Note that ε_ν are invariant under $W(E_6)$, since $\{u_1, \cdots, u_{27}\}$ is stable under $W(E_6)$. We have

$$\Phi_{E_6}(X) = \Psi_{E_6}(X)\Psi_{E_6}(-X), \tag{7.9}$$

so we rename the *universal polynomial of type* E_6 to mean this newly defined polynomial $\Psi_{E_6}(X)$ of degree 27.

With this modified notation, we can state:

THEOREM 7.3.

$$\boldsymbol{Q}[u_1, \cdots, u_6]^{W(E_6)} = \boldsymbol{Q}[\varepsilon_2, \varepsilon_5, \varepsilon_6, \varepsilon_8, \varepsilon_9, \varepsilon_{12}]. \tag{7.10}$$

REMARK 7.4. The fundamental invariants of the Weyl group $W(E_r)$ seem to have been studied by many authors (e.g. [**F**] for E_6, [**Br**] for E_7), but we have not found in the literature such a simple statement as above. This comes out automatically in our approach via the Mordell-Weil lattices (see the proof of Theorem 8.3, 9.3 or 10.3).

(x) Using the minimal vectors (roots) in E_r instead of those in E_r^*, we can define similar polynomial:

$$\Pi_{j=1}^{n}(X-\alpha_j) \in \boldsymbol{Z}[u_1, \cdots, u_r][X] \tag{7.11}$$

of degree $n=240$, 126 or 72 for $r=8$, 7 or 6; for $r=8$, this is the same as Φ_{E_8}. The coefficients of (7.11) are again invariant under $W(E_r)$. In particular, the constant term

$$\delta_0(u) = \Pi_{i=1}^{n}\alpha_j = \pm(\Pi_{j=1}^{n/2}\alpha_j)^2 \tag{7.12}$$

is an important invariant, playing the role of the difference product or the discriminant, which appears in the statement of Theorem (E_r). It is known that the Jacobian determinant of any sets of fundamental invariants of $W(E_r)$ with respect to $u_1, \cdots, u_r$ is equal to $\Pi_{j=1}^{n/2}\alpha_j$, up to a constant.

8. Case (E_8).

Let us consider the elliptic curve $E=E_\lambda$

$$\begin{aligned} y^2 &= x^3+x(\textstyle\sum_{i=0}^{3}p_it^i)+(\sum_{i=0}^{3}q_it^i+t^5) \\ \lambda &= (p_0, p_1, p_2, p_3, q_0, q_1, q_2, q_3) \in \boldsymbol{A}^8. \end{aligned} \tag{8.1}$$

As before, let $K=k(t)$ be the rational function field over an algebraically closed field k containing p_i and q_j.

Step 1. The elliptic surface $f: S_\lambda \to \boldsymbol{P}^1$ has an irreducible singular fibre of type II at $t=\infty$:

$$f^{-1}(\infty) = \Theta_0 \qquad \text{(a rational curve with a cusp)} \tag{8.2}$$

$$f^{-1}(\infty)^\# = \Theta_0^\# \cong \boldsymbol{G}_a \qquad \text{(the additive group)}. \tag{8.3}$$

Step 2. Assume that (#) f has no reducible fibres at all. This is certainly the case if λ is generic (over the prime field) or if λ is sufficiently general. Then we have $E(K)=E(K)^{\circ}$, which has rank $r=8$ and det $=1$ by (4.10) and (4.11). Hence the Mordell-Weil lattice $E(K)$ is an even unimodular lattice of rank 8, and as such, it is isomorphic to the root lattice E_8:

$$E(K)=E(K)^{\circ}\cong E_8\,. \tag{8.4}$$

It has 240 roots (minimal vectors of norm 2). Since

$$\langle P,P\rangle=2+2(PO)\geqq 2 \qquad \text{for any } P\in E(K), \qquad P\neq 0\,,$$

P is a minimal section if and only if $(PO)=0$. By (4.12), we have:

LEMMA 8.1. *Under the assumption* $(\#)$, *there are exactly* 240 *rational points* $P=(x,y)$ *in* $E(K)$ *of the form:*

$$x=gt^2+at+b, \qquad y=ht^3+ct^2+dt+e\,, \tag{8.5}$$

with some constants $a, b, \cdots, g, h$ *in* k.

Step 3. Consider the specialization homomorphism:

$$sp_{\infty}\colon E(K)\longrightarrow f^{-1}(\infty)^{\#}\cong \boldsymbol{G}_a\,. \tag{8.6}$$

LEMMA 8.2. *If* P *is given by* (8.5), *then* $g\neq 0$, $h\neq 0$, *and*

$$sp_{\infty}(P)=g/h\,. \tag{8.7}$$

PROOF. In terms of the ∞-model (cf. (4.13)), P is written as

$$X=g+as+bs^2, \qquad Y=h+cs+ds^2+es^3\,.$$

Hence the section (P) meets $f^{-1}(\infty)$ at $(X,Y)=(g,h)$, which must be different from the singular point $(0,0)$ of the curve $Y^2=X^3$. Hence both g and h are $\neq 0$, and we have

$$sp_{\infty}(P)=(X/Y)|_{s=0}=g/h\,. \qquad \text{q.e.d.}$$

Step 4. Now we assume that λ is generic over $\boldsymbol{Q}$, i.e., $p_0,\cdots,q_3$ are algebraically independent over $\boldsymbol{Q}$, and let k be the algebraic closure of $\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0,\cdots,q_3)$. Then the condition $(\#)$ holds, and hence we have $E_{\lambda}(K)\cong E_8$ by (8.4). We choose a basis $\{P_1,\cdots,P_8\}$ of $E_{\lambda}(K)$ with Gram matrix $(\langle P_i,P_j\rangle)=I_8$, and label the 240 points P_i $(1\leqq i\leqq 240)$ in the same way as in §7 (v). Letting

$$u_i=sp_{\infty}(P_i)\in k\,, \tag{8.8}$$

we define the polynomial

$$\Phi(X,\lambda)=\Pi_{i=1}^{240}(X-u_i)\in \boldsymbol{Q}(\lambda)[X]\,. \tag{8.9}$$

It has coefficients in $\boldsymbol{Q}(\lambda)$ because $\{u_i\}$ is stable under $\mathrm{Gal}(k/\boldsymbol{Q}(\lambda))$. Since sp_∞ is a homomorphism, $\Phi(X, \lambda)$ will coincide with the universal polynomial of type E_8 defined by (7.1), once we see that $u_1, \cdots, u_8$ are algebraically independent over $\boldsymbol{Q}$. At any rate, the coefficients $\pm\varepsilon_\nu$ of $\Phi(X, \lambda)$ are contained in $\boldsymbol{Z}[u_1, \cdots, u_{240}]^{\mathfrak{S}_{240}} \subset \boldsymbol{Z}[u_1, \cdots, u_8]^{W(E_8)}$.

THEOREM 8.3. *Assume that $\lambda=(p_0, \cdots, q_3)$ is generic over $\boldsymbol{Q}$. Then the polynomial $\Phi(X, \lambda)$ has the coefficients in the polynomial ring $\boldsymbol{Z}[\lambda]=\boldsymbol{Z}[p_0, \cdots, q_3]$. The elements $u_1, \cdots, u_8$ are algebraically independent over $\boldsymbol{Q}$, and we have*

$$\boldsymbol{Q}[u_1, \cdots, u_8]^{W(E_8)} = \boldsymbol{Q}[p_0, \cdots, q_3]\,, \tag{8.10}$$

which also coincides with $\boldsymbol{Q}[\varepsilon_2, \varepsilon_8, \varepsilon_{12}, \varepsilon_{14}, \varepsilon_{18}, \varepsilon_{20}, \varepsilon_{24}, \varepsilon_{30}]$. In other words, both $\{p_0, \cdots, q_3\}$ and $\{\varepsilon_2, \cdots, \varepsilon_{30}\}$ form the fundamental invariants of the Weyl group $W(E_8)$. The explicit relation between them is given by the formulas (2.25) *of Theorem* (E_8).

THEOREM 8.4. *Under the same assumption, the polynomial $\Phi(X, \lambda)$ is irreducible over the rational function field $\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0, \cdots, q_3)$. The splitting field of $\Phi(X, \lambda)$ over $\boldsymbol{Q}(\lambda)$*

$$\mathcal{K} = \boldsymbol{Q}(\lambda)(u_1, \cdots, u_{240}) \tag{8.11}$$

is a Galois extension of $\boldsymbol{Q}(\lambda)$ with the Galois group

$$\mathrm{Gal}(\mathcal{K}/\boldsymbol{Q}(\lambda)) = W(E_8) \quad (\textit{the Weyl group of type } E_8) \tag{8.12}$$

and it is a purely transcendental extension of the prime field $\boldsymbol{Q}$:

$$\mathcal{K} = \boldsymbol{Q}(u_1, \cdots, u_8)\,. \tag{8.13}$$

THEOREM 8.5. *For λ generic, the specialization map*

$$sp_\infty : E_\lambda(k(t)) \longrightarrow k$$

is an injective homomorphism, whose image $\sum_{i=0}^{8}\boldsymbol{Z}u_i$ is a submodule of rank 8 *in $\mathcal{K}=\boldsymbol{Q}(u_1, \cdots, u_8)$ with $W(E_8)$-action. In particular, each minimal section P is uniquely determined by $u=sp_\infty(P)$.*

More explicitly, for each root u of the equation $\Phi(X, \lambda)=0$, there is a unique rational point $P=P(u)$ of $E_\lambda(k(t))$ with $sp_\infty(P)=u$. It is of the form (8.5), i.e., *$P=(x, y)$ with*

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

in which $g, h, a, \cdots, e$ are determined by u as follows:

$$\begin{cases} g = u^{-2}, \qquad h = u^{-3} \\ a, b, c, d, e \in \boldsymbol{Q}[u_1, \cdots, u_8][u^{-1}] \cap \boldsymbol{Q}(\lambda)(u)\,. \end{cases} \tag{8.14}$$

These results (and Theorems 7.2, (7.6)) will be proven almost at the same time.

PROOF OF THEOREM 8.3. Let us analyse the condition for the point (8.5) to belong to $E(K)$, by means of the elimination method. For that purpose, we substitute (8.5) into the equation (8.1) and look at the coefficients of t^m for $m=6, 5, \cdots, 0$. Then we get 7 polynomial relations among $a, b, \cdots, g, h$ over $\boldsymbol{Q}[p_0, \cdots, q_3]$:

$$(8.15)_1 \qquad h^2 = g^3$$

$$(8.15)_2 \qquad 2ch = 1+3ag^2+p_3g$$

$$(8.15)_3 \qquad c^2+2dh = 3a^2g+3bg^2+p_2g+p_3a$$

$$(8.15)_4 \qquad 2cd+2eh = a^3+6abg+p_1g+p_2a+p_3b+q_3$$

$$(8.15)_5 \qquad d^2+2ce = 3a^2b+3b^2g+p_0g+p_1a+p_2b+q_2$$

$$(8.15)_6 \qquad 2de = 3ab^2+p_0a+p_1b+q_1$$

$$(8.15)_7 \qquad e^2 = b^3+p_0b+q_0 .$$

Now, we set $u=g/h$ in view of (8.7). Then, by $(8.15)_1$, we have

$$g = u^{-2}, \qquad h = u^{-3} .$$

The next 3 relations $(8.15)_2, \cdots, (8.15)_4$ determine c, d, e as elements of $\boldsymbol{Q}[p_0, \cdots, q_3][u, u^{-1}, a, b]$. Substitute these into the remaining 3 relations, and we get 3 relations among u, a, b over $\boldsymbol{Q}[p_0, \cdots, q_3]$. Then, eliminating a and b from them, we obtain a monic polynomial of degree 240 in u with coefficients in $\boldsymbol{Q}[p_0, \cdots, q_3]$.

In carrying out the elimination process sketched above (and also for constructing numerical examples), it is useful to note that we are dealing with a weighted homogeneous equation. Namely we have

x	y	t	p_0	p_1	p_2	p_3	q_0	q_1	q_2	q_3	a	b	c	d	e	g	h	u
10	15	6	20	14	8	2	30	24	18	12	4	10	3	9	15	−2	−3	1

where the second row gives the weight of the letter above.

Let us introduce the homogeneous elements of weight 0:

$$(8.16) \qquad \begin{cases} A = a/u^4, \quad B = b/u^{10}, \quad C = c/u^3, \quad D = d/u^9, \quad E = e/u^{15}, \\ P_i = p_i/u^{20-6i}, \quad Q_i = q_i/u^{30-6i} \quad (i=0, 1, 2, 3). \end{cases}$$

Then $(8.15)_2, \cdots, (8.15)_4$ imply

$$(8.17) \qquad C, D, E \in \boldsymbol{Q}[P_0, \cdots, Q_3][A, B]$$

(for instance, $C=(1+3A+P_3)/2$, etc.). Substituting these into $(8.15)_5, \cdots, (8.15)_7$, we obtain 3 relations of B over $\boldsymbol{Q}[P_0, \cdots, Q_3][A]$ of the form:

$$B^2+f_2(A)\cdot B+f_4(A)=0 \tag{8.18}$$

$$f_1'(A)\cdot B^2+f_3'(A)\cdot B+f_5'(A)=0 \tag{8.19}$$

$$B^3+f_2''(A)\cdot B^2+f_4''(A)\cdot B+f_6''(A)=0\,, \tag{8.20}$$

where $f_d(A), \cdots$ are polynomials of degree d in A over $\boldsymbol{Q}[P_0, \cdots, Q_3]$. Under (8.18), the last two are equivalent to the following:

$$h_2(A)\cdot B+h_4(A)=0 \tag{8.19$'$}$$

$$h_3(A)\cdot B+h_5(A)=0\,. \tag{8.20$'$}$$

Eliminating B from (8,19)$'$, (8.20)$'$ and (8.18), we obtain two relations of A over $\boldsymbol{Q}[P_0, \cdots, Q_3]$ of degree 8 and 7:

$$A^8+\cdots=0, \qquad (310+P_3)\cdot A^7+\cdots=0\,. \tag{8.21}$$

In particular, we see that A is integral over $\boldsymbol{Q}[P_0, \cdots, Q_3]$, and so are B, C, D, E, by (8.18) and (8.17). Next we eliminate A from (8.21) to obtain a relation $R=0$ among $P_0, \cdots, Q_3$. In other words, R is the resultant of two relations in (8.21). On the other hand, let L be the resultant of $h_2(A)$ and $h_4(A)$ appearing in (8.19)$'$. Then we have

$$R=\text{const.}\ L^2\cdot F \tag{8.22}$$

where F is a polynomial in $\boldsymbol{Z}[P_0, \cdots, Q_3]$ with the constant term 1. Writing $P_0, \cdots, Q_3$ in terms of $p_0, \cdots, q_3$ and u by (8.16), and multiplying u^{240} to F, we finally obtain a monic relation of u over $\boldsymbol{Z}[p_0, \cdots, q_3]$:

$$\Phi(u)=u^{240}+60p_3u^{238}+1764p_3^2u^{236}+\cdots=0\,. \tag{8.23}$$

Conversely, for any root u of (8.23), we have a common root A of (8.21), which uniquely determines B satisfying (8.18), $\cdots$, (8.20), and also C, D, E by (8.17). Hence we obtain, for a given u, at least one set of $g, h, a, \cdots, e$ satisfying all the relations of (8.15), and thus a rational point P of the form (8.5) such that $sp_\infty(P)=u$. Noting that $\Phi(X)$ is separable (which can be checked by specialzing p_i and q_j to numerical values), we see that $\Phi(X)$ divides $\Phi(X, \lambda)$ defined by (8.9). Therefore, comparing the degree, we conclude that

$$\Phi(X)=\Phi(X, \lambda)\,. \tag{8.24}$$

This proves the first assertion in Theorem 8.3.

Next we compare the coefficients of X^d in (8.24) for $d=2, 8, 12, 14, 18, 20, 24, 30$, which are the weights of the fundamental invariants of the Weyl group $W(E_8)$ (cf. (7.5)). Then we find the following explicit formulas:

$$(8.25)\qquad \begin{cases} \varepsilon_2 = 60p_3, \\ \varepsilon_8 = 720p_2+478170p_3^4, \\ \varepsilon_{12} = 15120q_3+\cdots, \\ \varepsilon_{14} = 79200p_1+\cdots, \\ \varepsilon_{18} = 2620800q_2+\cdots, \\ \varepsilon_{20} = 11040480p_0+\cdots, \\ \varepsilon_{24} = 419237280q_1+\cdots, \\ \varepsilon_{30} = 65945880000q_0+\cdots, \end{cases}$$

where $\cdots$ stands for a sum of terms in p_i or q_j of lower weights.

Obviously it follows that

$$(8.26)\qquad \boldsymbol{Q}[\varepsilon_2, \cdots, \varepsilon_{30}] = \boldsymbol{Q}[p_3, p_2, q_3, p_1, q_2, p_0, q_1, q_0].$$

This shows first that $\varepsilon_2, \cdots, \varepsilon_{30}$ are algebraically independent over $\boldsymbol{Q}$, since p_i, q_j are so by assumption, and second that they form the fundamental invariants of $W(E_8)$ because they have the right weights. For the same reason, $p_0, \cdots, q_3$ form the fundamental invariants, which proves (8.10). It is by now clear that $u_1, \cdots, u_8$ are algebraically independent over $\boldsymbol{Q}$.

Writing out the part $\cdots$ of (8.25) and letting $\varepsilon_{2\nu}=(-1)^\nu\varepsilon'_\nu$, we obtain the formula expressing p_i, q_j in terms of ε'_d ($d=1, 4, \cdots, 15$), which is nothing but the formula (2.25) of Theorem (E_8). To emphasize the dependence of p_i, q_j upon $u_1, \cdots, u_8$, we write it here in the form:

$$(8.27)\qquad p_i = I_{20-6i}(u_1, \cdots, u_8), \qquad q_i = I_{30-6i}(u_1, \cdots, u_8),$$

where I_w stands for an invariant of weight w for the Weyl group $W(E_8)$. Thus we have proven Theorem 8.3 (and (7.6) of Theorem 7.2).

PROOF OF THEOREM 8.4. For the splitting field $\mathcal{K}$ of $\Phi(X, \lambda)$ over $\boldsymbol{Q}(\lambda)$, we have

$$\mathcal{K} = \boldsymbol{Q}(p_0, \cdots, q_3)(u_1, \cdots, u_{240}) = \boldsymbol{Q}(u_1, \cdots, u_8)$$

by (8.27), since all u_i are $\boldsymbol{Z}$-linear combination of $u_1, \cdots, u_8$. Next, taking the field of fractions in both sides in (8.10), we have

$$(8.28)\qquad \boldsymbol{Q}(u_1, \cdots, u_8)^{W(E_8)} = \boldsymbol{Q}(p_0, \cdots, q_3).$$

By Galois theory, it is then immediate that $\boldsymbol{Q}(u_1, \cdots, u_8)$ is a Galois extension of $\boldsymbol{Q}(p_0, \cdots, q_3)$ with Galois group $W(E_8)$. Moreover this Galois group acts transitively on the 240 roots u_i of the polynomial $\Phi(X, \lambda)$, since the Weyl group $W(E_8)$ acts transitively on the "roots" of E_8. This proves the irreducibility of Φ over $\boldsymbol{Q}(p_0, \cdots, q_3)$. Thus we have proven Theorem 8.4.

PROOF OF THEOREM 8.5. First of all, the specialization map sp_∞ is injective, because $u_1, \cdots, u_8$ are linearly independent over $\boldsymbol{Q}$ (they are even algebraically independent).

To prove other assertion, we use the notation in the proof of Theorem 8.1. Take a root u of $\Phi(X, \lambda)=0$ and define P_i, Q_i by (8.16) using this u. As noted before, we have a common root A of (8.21), which is obviously integral over $\boldsymbol{Q}[P_0, \cdots, Q_3]$. On the other hand, applying the Euclid algorithm to the 2 relations in (8.21), we obtain a relation of degree 1 in A (one step before getting the resultant R). This means that A is in the quotient field of $\boldsymbol{Q}[P_0, \cdots, Q_3]$. Hence A belongs to the normalization of the ring $\boldsymbol{Q}[P_0, \cdots, Q_3]$, which is contained in $V=\boldsymbol{Q}[u_1, \cdots, u_8][u^{-1}]$. Thus $a=u^4\cdot A$ belongs to V.

Similarly, B is integral over $\boldsymbol{Q}[P_0, \cdots, Q_3][A]$ by (8.18), hence over $\boldsymbol{Q}[P_0, \cdots, Q_3]$, and it belongs to $\boldsymbol{Q}(P_0, \cdots, Q_3)(A)=\boldsymbol{Q}(P_0, \cdots, Q_3)$ by (8.19)'. Hence we have $B\in V$ and $b=u^{10}\cdot B\in V$. By (8.17) and (8.16), we see also c, d, $e\in V$.

This completes the proof of Theorem 8.5.

Step 5. It follows from Theorem 8.5 that the specialization map sp_∞ is a group isomorphism of $E_\lambda(k(t))$ to $\sum_{i=1}^{8}\boldsymbol{Z}u_i$ for λ generic, and we can introduce the lattice structure on the latter to make sp_∞ a lattice isomorphism. In particular, we have

$$(8.29) \qquad (\langle P_i, P_j\rangle) = (\langle u_i, u_j\rangle) = I_8 .$$

Now we observe that the condition ($\#$) in Step 2 is equivalent to the non-vanishing of the invariant δ_0 in Theorem (E_8). Indeed, if ($\#$) holds, then the Mordell-Weil lattice $E(K)$ is E_8 so that it has 240 roots P, and $sp_\infty(P)\neq 0$ by (8.7). Since δ_0 is the constant term of $\Phi(X, \lambda)=\Phi_{E_8}(X)$ (cf. the end of §7), we have $\delta_0\neq 0$. Conversely, if there is a reducible fibre for $f: S_\lambda\to \boldsymbol{P}^1$, the non-identity components give rise to zeros of $\Phi(X)$, hence $\delta_0=0$ (cf. [**S4**]).

Now we specialize the generic $u=(u_1, \cdots, u_8)$ to $u^\circ=(u_1^\circ, \cdots, u_8^\circ)$ in $\boldsymbol{Q}^8$ such that $\delta_0(u^\circ)\neq 0$. (For the notion of specialization, we refer to [**W2**].) Then $\lambda=(p_0, \cdots, q_3)$ specializes to $\lambda^\circ=(p_0^\circ, \cdots, q_3^\circ)$ in $\boldsymbol{Q}^8$, which is uniquely determined from u° by (8.27) or by (2.25). The Mordell-Weil lattice $E_\lambda(K)$ specializes to $E_{\lambda^\circ}(K)$, and the 240 roots $\{P_i \mid 1\leqq i\leqq 240\}$ in the former specialize to $\{P_i^\circ\}$ in the latter. Each P_i° is a $\boldsymbol{Q}(t)$-rational point of E_{λ° of the form (8.5):

$$x = (u_i^\circ)^{-2}t^2+\cdots, \qquad y = (u_i^\circ)^{-3}t^3+\cdots,$$

as it is obtained from a $\boldsymbol{Q}(u_1, \cdots, u_8)(t)$-rational point P_i of E_λ (given by Theorem 8.5) under the specialization of $(u_1, \cdots, u_8)$ to $(u_1^\circ, \cdots, u_8^\circ)\in\boldsymbol{Q}^8$.

On the other hand, recall that we have

$$\langle P_i, P_j\rangle = 1-(P_iP_j),$$

since there are no reducible fibres. By the invariance of the intersection number under specialization (cf. [W2]), we have therefore

$$(8.30) \qquad (\langle P_i^\circ, P_j^\circ\rangle)_{i,j\leq 8} = (\langle P_i, P_j\rangle)_{i,j\leq 8} = I_8.$$

Thus we have shown that, given any $u^\circ \in \boldsymbol{Q}^8$ such that $\delta_0(u^\circ)\neq 0$, we can define an elliptic curve $E=E_{\lambda^\circ}$ defined over $\boldsymbol{Q}(t)$, having the 8 generators $\{P_i^\circ\}$ of the Mordell-Weil group $E(\boldsymbol{Q}(t))$ of rank 8, satisfying (8.30). Further, if $\delta_1(u^\circ)\neq 0$, then all u_i° $(1\leqq i\leqq 240)$ are distinct, and the proof of Theorem 8.5 (and 8.3) gives the algorithm to uniquely determine the rational point P_i° for each u_i°.

This completes the proof of Theorem (E_8) stated in §2.

9. Case $(\boldsymbol{E}_7)$.

The remaining cases (E_7) and (E_6) are similar to the case (E_8), and indeed, the formulation of the results and the proof can be given in a surprisingly parallel way. It should be noticed that the crucial step using the elimination argument is considerably simpler here.

In this section, we treat the case (E_7).

Thus we consider the elliptic curve $E=E_\lambda$

$$(9.1) \qquad \begin{gathered} y^2 = x^3+x(p_0+p_1t+t^3)+(\textstyle\sum_{i=0}^4 q_it^i) \\ \lambda = (p_0, p_1, q_0, q_1, q_2, q_3, q_4) \in \boldsymbol{A}^7. \end{gathered}$$

As before, $K=k(t)$ is the rational function field over an algebraically closed field k containing p_i and q_j.

Step 1. The elliptic surface $f: S_\lambda \to \boldsymbol{P}^1$ has a reducible singular fibre of type III at $t=\infty$:

$$(9.2) \qquad f^{-1}(\infty) = \Theta_0+\Theta_1, \qquad (\Theta_0\cdot\Theta_1) = 2,$$

where Θ_0, Θ_1 are smooth rational curves tangent at the unique point of their intersection. The associated algebraic group is:

$$(9.3) \qquad f^{-1}(\infty)^\# = \Theta_0^\# \cup \Theta_1^\# \cong \boldsymbol{G}_a \times \boldsymbol{Z}/2.$$

Step 2. Assume that (#) f has no reducible fibres other than $f^{-1}(\infty)$. This is certainly the case if λ is generic or sufficiently general. Then the narrow Mordell-Weil lattice $E(K)^\circ$ has rank $r=7$ and $\det = 2$ by (4.10) and (4.11). Hence it is isomorphic to the root lattice E_7, because its opposite lattice is the orthogonal complement of Θ_1 (a "root") in E_8^-, where E_8^- is itself the orthogonal complement of $\langle (O), F\rangle$ in $NS(S_\lambda)$ (cf. §7 (i) and Step 2 in case (E_8)). In general, we call such an E_8^- the "E_8-frame" of a rational elliptic surface with a section (O) (cf. [**S4**]). Thus we have

$$E(K) \cong E_7^*, \qquad E(K)^\circ \cong E_7. \tag{9.4}$$

There are 56 minimal sections of $E(K)$ of norm 3/2. Recalling that

$$\langle P, P\rangle = 2+2(PO)-\begin{cases} 0 & (P\Theta_0)=1 \\ 1/2 & \text{otherwise,}\end{cases}$$

for any $P\in E(K)$, $P\neq O$ (see (4.17)), P is a minimal section if and only if $(PO)=0$ and $(P\Theta_1)=1$. Then we have:

LEMMA 9.1. *Under the assumption* (#), *there are exactly* 56 *rational points* $P=(x, y)$ *in* $E(K)$ *of the form:*

$$x = at+b, \quad y = ct^2+dt+e \quad (a, b, \cdots, e\in k). \tag{9.5}$$

PROOF. Using (4.12), argue as in Lemma 6.1. q.e.d.

Step 3. Consider the specialization homomorphism:

$$sp_\infty\colon E(K) \longrightarrow f^{-1}(\infty)^\# \cong \boldsymbol{G}_a\times \boldsymbol{Z}/2. \tag{9.6}$$

LEMMA 9.2. *If P is given by* (9.5), *then*

$$sp_\infty(P) = (-c, \bar{1}). \tag{9.7}$$

PROOF. We have to show that the $\boldsymbol{G}_a$-component $sp'_\infty(P)$ of $sp_\infty(P)$ is equal to $-c$, for which it suffices to see that $sp_\infty(Q)=-2c$ for $Q=2P\in E(K)^\circ$. By the addition formula (5.9) (or its variant: the duplication formula), this can be easily verified (cf. the proof of (6.17) of Lemma 6.2). q.e.d.

Step 4. Now we assume that λ is generic over $\boldsymbol{Q}$, i.e., $p_0, \cdots, q_4$ are algebraically independent over $\boldsymbol{Q}$, and let k be the algebraic closure of $\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0, \cdots, q_4)$. Then the condition (#) holds, and hence we have $E_\lambda(K)\cong E_7^*$ by (9.4). We choose a basis $\{P_1, \cdots, P_7\}$ of $E_\lambda(K)$ with Gram matrix $(\langle P_i, P_j\rangle)=I_7$, and arrange the 56 points P_i $(1\leqq i\leqq 56)$ in the same way as in §7 (v). Letting

$$u_i = sp'_\infty(P_i) = -c_i \in k, \tag{9.8}$$

we define the polynomial

$$\Phi(X, \lambda) = \Pi_{i=1}^{56}(X-u_i) \in \boldsymbol{Q}(\lambda)[X]. \tag{9.9}$$

As in the case (E_8), this will coincide with the universal polynomial of type E_7 defined by (7.1), provided that $u_1, \cdots, u_7$ are algebraically independent over

$\boldsymbol{Q}$. Note $\Phi(-X, \lambda)=\Phi(X, \lambda)$.

THEOREM 9.3. *Assume that* $\lambda=(p_0, \cdots, q_4)$ *is generic over* $\boldsymbol{Q}$. *Then the polynomial* $\Phi(X, \lambda)$ *has the coefficients in the polynomial ring* $\boldsymbol{Z}[p_0, \cdots, q_4]$. *The elements* $u_1, \cdots, u_7$ *are algebraically independent over* $\boldsymbol{Q}$, *and we have*

$$\begin{aligned} \boldsymbol{Q}[u_1, \cdots, u_7]^{W(E_7)} &= \boldsymbol{Q}[p_0, p_1, q_0, \cdots, q_4], \\ &= \boldsymbol{Q}[\varepsilon_2, \varepsilon_6, \varepsilon_8, \varepsilon_{10}, \varepsilon_{12}, \varepsilon_{14}, \varepsilon_{18}]. \end{aligned} \tag{9.10}$$

Thus both $\{p_0, \cdots, q_4\}$ *and* $\{\varepsilon_2, \cdots, \varepsilon_{18}\}$ *form the fundamental invariants of the Weyl group* $W(E_7)$. *The explicit relation between them is given by the formulas* (2.21) *of Theorem* (E_7).

THEOREM 9.4. *Under the same assumption, the polynomial* $\Phi(X, \lambda)$ *is irreducible over the rational function field* $\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0, \cdots, q_4)$. *The splitting field of* $\Phi(X, \lambda)$ *over* $\boldsymbol{Q}(\lambda)$

$$\mathcal{K} = \boldsymbol{Q}(\lambda)(u_1, \cdots, u_{56}) \tag{9.11}$$

is a Galois extension of $\boldsymbol{Q}(\lambda)$ *with the Galois group*

$$\mathrm{Gal}(\mathcal{K}/\boldsymbol{Q}(\lambda)) = W(E_7) \quad (\textit{the Weyl group of type } E_7) \tag{9.12}$$

and it is a purely transcendental extension of $\boldsymbol{Q}$:

$$\mathcal{K} = \boldsymbol{Q}(u_1, \cdots, u_7). \tag{9.13}$$

THEOREM 9.5. *For* λ *generic, the composed map*

$$sp'_\infty = pr_1 \circ sp_\infty : E_\lambda(k(t)) \longrightarrow \boldsymbol{G}_a(k) \times \boldsymbol{Z}/2 \longrightarrow \boldsymbol{G}_a(k) = k \tag{9.14}$$

is an injective homomorphism, whose image $\sum_{i=1}^7 \boldsymbol{Z}u_i$ *is a submodule of rank 7 in* $\mathcal{K}=\boldsymbol{Q}(u_1, \cdots, u_7)$ *with* $W(E_7)$*-action. In particular, each minimal section* P *is uniquely determined by* $u=sp'_\infty(P)(=-c)$.

More explicitly, for each root c *of the equation* $\Phi(X, \lambda)=0$, *there is a unique rational point* $P=(x, y)$ *of* $E_\lambda(k(t))$ *such that*

$$x = at+b, \qquad y = ct^2+dt+e,$$

where a, b, d, e *are determined by* c *as follows:*

$$\begin{cases} a = c^2-q_4 \\ d = d(c) \in \boldsymbol{Q}[u_1, \cdots, u_7] \cap \boldsymbol{Q}(\lambda)(c) \\ b = -a^3+2cd-q_3 \\ e = (3a^2b-d^2+p_1a+q_2)/(2c), \end{cases} \tag{9.15}$$

$d(c)$ being certain rational function of c with coefficients in $\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0, \cdots, q_4)$

which is also expressed as a polynomial in $u_1, \cdots, u_7$.

PROOF OF THEOREM 9.3. As before, we substitute (9.5) into (9.1) and look at the coefficients of t^m for $m=4, 3, \cdots, 0$. Then we get 5 relations among $a, b, \cdots, e$ over $\boldsymbol{Q}[p_0, \cdots, q_4]$:

$$\begin{cases} c^2 = a+q_4 \\ 2cd = a^3+b+q_3 \\ d^2+2ce = 3a^2b+p_1a+q_2 \\ 2de = 3ab^2+p_0a+p_1b+q_1 \\ e^2 = b^3+p_0b+q_0\,. \end{cases} \tag{9.16}$$

By the first 3 relations, a, b, e are determined as elements of $\boldsymbol{Q}[p_0, \cdots, q_4][c, c^{-1}, d]$, as in (9.15). Substituting these into the last 2 relations, we get 2 monic relations of d over $\boldsymbol{Z}[p_0, \cdots, q_4][c]$ of degree 3 and 4:

$$d^3+\cdots=0, \qquad d^4+\cdots=0\,. \tag{9.17}$$

Then, eliminating d from them, we obtain a monic polynomial of degree 56 in c with coefficients in $\boldsymbol{Z}[p_0, \cdots, q_4]$:

$$\Phi(c) = c^{56}-36q_4c^{54}+594q_4^2c^{52}+(72q_3-6084q_4^3)c^{50}+\cdots=0\,. \tag{9.18}$$

Note, as before, that we have the weighted homogeneity, the weights being given in this case by

(9.19)

x	y	t	p_0	p_1	q_0	q_1	q_2	q_3	q_4	a	b	c	d	e
6	9	4	12	8	18	14	10	6	2	2	6	1	5	9

Now, for any root c of (9.18), we have a common root d of (9.17), which uniquely determines a, b, e by the formulas in (9.15). Hence, for each c, there is at least one rational point P of the form (9.5). As before, this implies:

$$\Phi(X) = \Phi(X, \lambda)\,. \tag{9.20}$$

This proves the first assertion in Theorem 9.1.

Next we compare the coefficients of X^d in (9.20) for $d=2, 6, 8, 10, 12, 14, 18$, which are the weights of the fundamental invariants of the Weyl group $W(E_7)$ (cf. (7.5)). Then we find the following:

$$
(9.21) \qquad \begin{cases} \varepsilon_2 = -36q_4, \\ \varepsilon_6 = 72q_3 - 6084q_4^3, \\ \varepsilon_8 = 60p_1 - 1800q_3q_4 + 43875q_4^4, \\ \varepsilon_{10} = -504q_2 + \cdots, \\ \varepsilon_{12} = -540p_0 + \cdots, \\ \varepsilon_{14} = 3828q_1 + \cdots, \\ \varepsilon_{18} = -29496q_0 + \cdots, \end{cases}
$$

where $\cdots$ stands for a sum of terms in p_i or q_j of lower weights.

Hence we have

$$
(9.22) \qquad \boldsymbol{Q}[\varepsilon_2, \cdots, \varepsilon_{18}] = \boldsymbol{Q}[q_4, q_3, p_1, q_2, p_0, q_1, q_0].
$$

which proves (9.10), together with the algebraic independence of $u_1, \cdots, u_7$ over $\boldsymbol{Q}$.

Letting $\varepsilon_{2\nu} = (-1)^\nu \varepsilon'_\nu$, we obtain from (9.21) the formula expressing p_i, q_j in terms of ε'_d ($d=1, 3, \cdots 9$), which is nothing but the formula (2.21) of Theorem (E_7). In particular, we can write

$$
(9.23) \qquad p_i = I_{12-4i}(u_1, \cdots, u_7), \qquad q_j = I_{18-4j}(u_1, \cdots, u_7),
$$

where I_w denotes an invariant of weight w for the Weyl group $W(E_7)$. Thus we have proven Theorem 9.3 (and (7.7) of Theorem 7.2).

Theorems 9.4 and 9.5 can be proven exactly in the same way as before, so we omit the proof.

Step 5. It follows from Theorem 9.5 that the specialization map sp'_∞ is a group isomorphism of $E_\lambda(k(t))$ to $\sum_{i=1}^7 \boldsymbol{Z}u_i$ for λ generic, and we can introduce the lattice structure on the latter to make sp'_∞ a lattice isomorphism. In particular, we have

$$
(9.25) \qquad (\langle P_i, P_j \rangle) = (\langle u_i, u_j \rangle) = I_7.
$$

Now we observe that the condition (#) in Step 2 is equivalent to the non-vanishing of the invariant δ_0 in Theorem (E_7). Indeed, if (#) holds, then the narrow Mordell-Weil lattice $E(K)^\circ$ is E_7 so that it has 126 roots P, and we have $sp_\infty(P) \neq 0$ by the same proof as (8.7). Since δ_0 is the product of these (cf. the end of §7), we have $\delta_0 \neq 0$. Conversely, if there is a reducible fibre for $f: S_\lambda \to \boldsymbol{P}^1$ other than $f^{-1}(\infty)$, then its non-identity components, say Θ, give rise to the roots $(\Theta \cdot \Theta) = -2$ of the "E_7-frame" in $NS(S_\lambda)$, which implies $\delta_0 = 0$ (cf. [**S4**]). The condition $\delta_0 \neq 0$ is also equivalent to the smoothness of the affine surface defined by (9.1).

Now we specialize the generic $u = (u_1, \cdots, u_7)$ to $c = (c_1, \cdots, c_7)$ in $\boldsymbol{Q}^7$ such that $\delta_0(c)\neq 0$. Then $\lambda=(p_0, \cdots, q_4)$ specializes to $\lambda^\circ=(p_0^\circ, \cdots, q_4^\circ)\in \boldsymbol{Q}^7$, which is uniquely determined from c by (9.23) or by (2.21). The Mordell-Weil lattice $E_\lambda(K)$ specializes to $E_{\lambda^\circ}(K)$, and the 56 minimal vectors $\{P_i \mid 1\leqq i\leqq 56\}$ in the former specialize to $\{P_i^\circ\}$ in the latter. Each P_i° is a $\boldsymbol{Q}(t)$-rational point of E_{λ° of the form (9.5), as it is obtained from a $\boldsymbol{Q}(u_1, \cdots, u_7)(t)$-rational point P_i of E_λ (given by Theorem 9.5) under the specialization of $(u_1, \cdots, u_7)$ to $(c_1, \cdots, c_7)$ $\in \boldsymbol{Q}^7$.

On the other hand, we have

$$\langle P_i, P_j\rangle = 1/2-(P_iP_j),$$

since $f^{-1}(\infty)$ is the only reducible fibre. By the invariance of the intersection number under specialization, we have therefore

$$(\langle P_i^\circ, P_j^\circ\rangle)_{i,j\leq 7} = (\langle P_i, P_j\rangle)_{i,j\leq 7} = I_7 . \tag{9.26}$$

Thus we have shown that, given any $c\in \boldsymbol{Q}^7$ such that $\delta_0(c)\neq 0$, we can define an elliptic curve $E=E_{\lambda^\circ}$ defined over $\boldsymbol{Q}(t)$, having the 7 generators $\{P_i^\circ\}$ of the Mordell-Weil group $E(\boldsymbol{Q}(t))$ of rank 7, satisfying (9.26). Further, if $\delta_1(c)$ $\neq 0$, then all c_i $(1\leqq i\leqq 56)$ are distinct, and the proof of Theorem 9.3 (and 9.1) gives the algorithm to uniquely determine the rational point P_i° for each c_i.

This completes the proof of Theorem (E_7) stated in §2.

10. Case $(\boldsymbol{E}_6)$.

Finally we consider the case (E_6).

The elliptic curve $E=E_\lambda$ is given by

$$\begin{gathered} y^2 = x^3+x(p_0+p_1t+p_2t^2)+(q_0+q_1t+q_2t^2+t^4) \\ \lambda = (p_0, p_1, p_2, q_0, q_1, q_2) \in \boldsymbol{A}^6 . \end{gathered} \tag{10.1}$$

As before, $K=k(t)$ is the rational function field over an algebraically closed field k containing p_i and q_j.

Step 1. The elliptic surface $f: S_\lambda\to \boldsymbol{P}^1$ has a reducible singular fibre of type IV at $t=\infty$:

$$f^{-1}(\infty) = \Theta_0+\Theta_1+\Theta_2 , \tag{10.2}$$

where Θ_0, Θ_1, Θ_2 are smooth rational curves meeting transversally at the unique point of their intersection. The associated algebraic group is:

$$f^{-1}(\infty)^\# = \Theta_0^\#\cup\Theta_1^\#\cup\Theta_2^\# \cong \boldsymbol{G}_a\times \boldsymbol{Z}/3 . \tag{10.3}$$

Step 2. Assume that $(\#)$ f has no reducible fibres other than $f^{-1}(\infty)$. This is certainly the case if λ is generic or sufficiently general. Then the narrow Mordell-Weil lattice $E(K)^{\circ}$ has rank $r=6$ and $\det=3$ by (4.10) and (4.11). Hence it is isomorphic to the root lattice E_6, because its opposite lattice is the orthogonal complement of $T_{\infty}=\langle\Theta_1, \Theta_2\rangle\cong A_2^-$ in the E_8-frame E_8^- in $NS(S_\lambda)$ (cf. §7 (i) and Step 2 in case (E_7)). Therefore we have

$$E(K)\cong E_6^*,\qquad E(K)^{\circ}\cong E_6\,. \tag{10.4}$$

There are 54 minimal sections of $E(K)$ of norm 4/3. Recall that

$$\langle P, P\rangle = 2+2(PO)-\begin{cases} 0 & (P\Theta_0)=1 \\ 2/3 & \text{otherwise,}\end{cases}$$

for any $P\in E(K)$, $P\neq O$ (see (4.5) and (4.17)). Hence P is a minimal section if and only if $(PO)=0$ and $(P\Theta_i)=1$ for $i=1$ or 2.

LEMMA 10.1. *Under the assumption* (#), *there are exactly* 27 *rational points* $P=(x, y)$ *in* $E(K)$ *of the form:*

$$x = at+b,\qquad y=t^2+dt+e\quad (a, b, d, e\in k)\,, \tag{10.5}$$

and the corresponding sections (P) *intersect one and the same component of* $f^{-1}(\infty)$, *say* Θ_1.

PROOF. The first assertion is shown in the same way as Lemma 9.1. Now take P, P' as in (10.5). By the addition formula (5.9), we see that $P-P'$ passes through the identity component Θ_0 (so that $P-P'$ belongs to $E(K)^{\circ}$), which proves the second assertion. q.e.d.

Step 3. Consider the specialization homomorphism:

$$sp_{\infty}\colon E(K)\longrightarrow f^{-1}(\infty)^{\#}\cong \boldsymbol{G}_a\times \boldsymbol{Z}/3\,. \tag{10.6}$$

LEMMA 10.2. *If P is given by* (10.5), *then*

$$sp_{\infty}(P) = (-a/2, \bar{1})\,. \tag{10.7}$$

The proof is similar to that of Lemma 9.1, and will be omitted.

Step 4. Now we assume that λ is generic over $\boldsymbol{Q}$, i.e., $p_0, \cdots, q_2$ are algebraically independent over $\boldsymbol{Q}$, and let k be the algebraic closure of $\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0, \cdots, q_2)$. Then the condition (#) holds, and hence we have $E_\lambda(K)\cong E_6^*$ by (10.4). We choose a basis $\{P_1, \cdots, P_6\}$ of $E_\lambda(K)$ with Gram matrix $(\langle P_i, P_j\rangle)=I_6$, and arrange the 54 points P_i $(1\leqq i\leqq 54)$ in the same way as in §7 (ix). Letting

$$u_i = -2\cdot sp'_{\infty}(P_i) = a_i\in k\,, \tag{10.8}$$

we define the polynomial

$$\Psi(X, \lambda) = \Pi_{i=1}^{27}(X-u_i) \in \boldsymbol{Q}(\lambda)[X]\,. \tag{10.9}$$

As before, this will coincide with the universal polynomial of type E_6 defined by (7.8), provided that $u_1, \cdots, u_6$ are algebraically independent over $\boldsymbol{Q}$.

THEOREM 10.3. *Assume that $\lambda=(p_0, \cdots, q_2)$ is generic over $\boldsymbol{Q}$. Then the polynomial $\Psi(X, \lambda)$ has the coefficients in the polynomial ring $\boldsymbol{Z}[p_0, \cdots, q_2]$. The elements $u_1, \cdots, u_6$ are algebraically independent over $\boldsymbol{Q}$, and we have*

$$\begin{aligned} \boldsymbol{Q}[u_1, \cdots, u_6]^{W(E_6)} &= \boldsymbol{Q}[p_0, p_1, p_2, q_0, q_1, q_2]\,, \\ &= \boldsymbol{Q}[\varepsilon_2, \varepsilon_5, \varepsilon_6, \varepsilon_8, \varepsilon_9, \varepsilon_{12}]\,. \end{aligned} \tag{10.10}$$

Thus both $\{p_0, \cdots, q_2\}$ and $\{\varepsilon_2, \cdots, \varepsilon_{12}\}$ form the fundamental invariants of the Weyl group $W(E_6)$. The explicit relation between them is given by the formulas (2.15) of Theorem (E_6).

THEOREM 10.4. *Under the same assumption, the polynomial $\Psi(X, \lambda)$ is irreducible over the rational function field $\boldsymbol{Q}(\lambda)=\boldsymbol{Q}(p_0, \cdots, q_2)$. The splitting field of $\Psi(X, \lambda)$ over $\boldsymbol{Q}(\lambda)$*

$$\mathcal{K} = \boldsymbol{Q}(\lambda)(u_1, \cdots, u_{27}) \tag{10.11}$$

is a Galois extension of $\boldsymbol{Q}(\lambda)$ with the Galois group

$$\mathrm{Gal}\,(\mathcal{K}/\boldsymbol{Q}(\lambda)) = W(E_6) \qquad (\textit{the Weyl group of type } E_6) \tag{10.12}$$

and it is a purely transcendental extension of $\boldsymbol{Q}$:

$$\mathcal{K} = \boldsymbol{Q}(u_1, \cdots, u_6)\,. \tag{10.13}$$

THEOREM 10.5. *For λ generic, the composed map*

$$sp'_\infty = pr_1 \circ sp_\infty \colon E_\lambda(k(t)) \longrightarrow \boldsymbol{G}_a(k) \times \boldsymbol{Z}/3 \longrightarrow \boldsymbol{G}_a(k) = k \tag{10.14}$$

is an injective homomorphism, whose image $\sum_{i=0}^{6} \boldsymbol{Z}u_i/2$ is a submodule of rank 6 in $\mathcal{K}=\boldsymbol{Q}(u_1, \cdots, u_6)$ with $W(E_6)$-action. In particular, each minimal section P is uniquely determined by $sp'_\infty(P)(=-a/2)$.

More explicitly, for each root a of the equation $\Psi(X, \lambda)=0$, there is a unique rational point $P=(x, y)$ of $E_\lambda(k(t))$ such that

$$x = at+b, \qquad y = t^2+dt+e\,,$$

where b, d, e are determined by a as follows:

$$
(10.15) \qquad \begin{cases} b = \beta_a(u_1, \cdots, u_6) \in \boldsymbol{Q}[u_1, \cdots, u_6] \cap \boldsymbol{Q}(\lambda)(a) \\ d = (a^3 + p_2 a)/2 \\ e = (3a^2 b - d^2 + p_1 a + p_2 b + q_2)/2 . \end{cases}
$$

Here $\beta_a(u_1, \cdots, u_6)$ is a certain rational function of a with coefficients in $\boldsymbol{Q}(\lambda) = \boldsymbol{Q}(p_0, \cdots, q_2)$ which is also expressed as a polynomial in $u_1, \cdots, u_6$.

PROOF OF THEOREM 10.3. As before, we substitute (10.5) into (10.1) and look at the coefficients of t^m for $m=3, \cdots, 0$. Then we get 4 relations among $a, b, \cdots, e$ over $\boldsymbol{Q}[p_0, \cdots, q_2]$:

$$
(10.16) \qquad \begin{cases} 2d = a^3 + p_2 a \\ d^2 + 2e = 3a^2 b + p_1 a + p_2 b + q_2 \\ 2de = 3ab^2 + p_0 a + p_1 b + q_1 \\ e^2 = b^3 + p_0 b + q_0 . \end{cases}
$$

By the first 2 relations, d, e are determined as in (10.15). Substituting these into the remaining relations in (10.16), we get 2 relations of b over $\boldsymbol{Z}[p_0, \cdots, q_2][a]$ of degree 3 and 2:

$$
(10.17) \qquad b^3 + \cdots = 0, \qquad ab^2 + \cdots = 0 .
$$

Then, eliminating b, we obtain a monic relation $\Psi(a)=0$ of degree 27 in a with coefficients in $\boldsymbol{Z}[p_0, \cdots, q_2]$: explicitly, we have

$$
\begin{aligned}
(10.18) \qquad \Psi(X) = {} & X^{27} + 12p_2 X^{25} + 60p_2^2 X^{23} \\
& -48p_1 X^{22} + (96q_2 + 168p_2^3) X^{21} + \cdots \\
& +(480p_0 + 294p_2^4 + 528p_2 q_2) X^{19} \\
& -(1344q_1 + 1008p_1 p_2^2) X^{18} + \cdots \\
& +(17280q_0 + 4768p_0 p_2^2 - 1248q_2^2 \\
& \quad +1200p_2^3 q_2 + 608p_1^2 p_2 + 252p_2^6) X^{15} + \cdots .
\end{aligned}
$$

The weights in this case are defined as follows:

(10.19)

x	y	t	p_0	p_1	p_2	q_0	q_1	q_2	a	b	d	e
4	6	3	8	5	2	12	9	6	1	4	3	6

The rest of the proof is completely analogous to that of Theorem 8.3 or 9.3, and it can be safely omitted.

Also Theorems 10.4 and 10.5 can be proven exactly in the same way as before.

Step 5. It remains to check that the condition (#) in Step 2 is equivalent to $\delta_0 \neq 0$ in Theorem (E_6), but again this can be verified by the same method. (These conditions are also equivalent to the smoothness of the affine surface defined by (10.1).)

Finally we specialize the generic $u=(u_1, \cdots, u_6)$ to some $a=(a_1, \cdots, a_6)$ in $\boldsymbol{Q}^6$ such that $\delta_0(a) \neq 0$. Then we obtain an elliptic curve E defined over $\boldsymbol{Q}(t)$, having the 6 explicit generators $\{P_i^\circ\}$ of the Mordell-Weil group $E(\boldsymbol{Q}(t))$ of rank 6, such that the Gram matrix $(\langle P_i^\circ, P_j^\circ \rangle)=I_6$. Further, if $\delta_1(a) \neq 0$, then all a_i $(1 \leqq i \leqq 27)$ are distinct, and the proof of Theorem 10.1 gives the algorithm to uniquely determine the rational point P_i° for each a_i.

This completes the proof of Theorem (E_6).

REMARK 10.6. As we have seen above, the cases for E_6 and E_7 can be treated exactly in the same way as the case for E_8, and thus, for the purpose of just proving Theorem (E_6) or (E_7), the last two sections could have been spared by pointing out the analogy.

However, we have chosen to give the detailed formulation in each case, allowing some repetition. The reason for this is as follows. We think that each pair of Theorems 8.3 and 8.4, 9.3 and 9.4, 10.3 and 10.4, constitutes the fundamental theorems for the algebraic equations of type E_r for $r=8, 7, 6$, which are comparable to the classical theory of the generic algebraic equations (cf. Introduction). As such, these results will have ample applications (see e.g. [**S4**] for an application to the deformation of singularities). Moreover, for $r=6$ or 7, they are closely related to the algebraic equation for the 27 lines on a cubic surface or the 28 double tangents to a plane quartic curve, and our results based on the Mordell-Weil lattices will throw some new light on these classical topics, which we hope to discuss in some other occasion (cf. [**S6**]).

REMARK 10.7. We have greatly benefited from the recent progress of a personal computer, which enables a mathematician like me without too much knowledge of computer to use it for the useful purpose. We have used it both in carrying out the elimination process in the cases (E_r) and in constructing numerical examples.

It should be noted that our method is safe against the possible errors caused by a computer or a software (we have encountered some bugs, indeed), because we have a safety check: after all, a rational point obtained must satisfy the equation of a given elliptic curve! For instance, take Example (E_8) in § 3 and check whether or not the coordinates (x, y) of the points P_i satisfy the equation $y^2=x^3+\cdots$ given there. If we made any mistake in the course of computing the fundamental invariants of the Weyl group or in determining the rational points P_i, there would be little chance for such a point to satisfy the given equation.

Acknowledgements. I would like to thank Professor J-P. Serre for many valuable comments on my work on the Mordell-Weil lattices. I would like to dedicate this paper to Professor G. Shimura whose philosophy to seek for significant algebraic equations or extensions has greatly influenced me in the present work.

Addendum (June 12, 1991).

I) Some of questions mentioned at the end of the Introduction have since been settled.
Page 676, Paragraph (2): For the Galois representations of type E_6, E_7, E_8, see the article [**S6**, §6-7].
Page 677, Paragraph (4): Indeed, this is the case. We now have an effective version of Néron's construction; see [**S7**].

II) I would like to thank Professor N. Elkies who has kindly made several comments on this paper in his letter dated July 25, 1990. With his permission, let me include here some of his remarks which might be helpful to other readers. (A few minor points have been incorporated in the text).
a) The reader should be aware of "the consistent use of the same notation for a vector (such as a root or dual root vector) in the space containing a root system, and the inner product of that vector with a generic vector in the same space". It is expected that the reader will get used to it, since this is a useful point of view.
b) Page 695, Lemma 6.2: "This partition of 24 minimal vectors of D_4 into three sets of 8 is the well-known partition of the twenty-four units in the Hurwitz quaternions into the three cosets of the normal subgroup $\{\pm 1, \pm i, \pm j, \pm k\}$, each forming an orthogonal frame for $\boldsymbol{R}^4$."
c) Page 700, paragraph (ix): "I suspect that the facts about E_6^* that permit this construction will not be familiar to many readers of this paper; at any rate they were new to me. But it's easy to derive them directly from the fact that E_6 is a root lattice of discriminant 3: the inner product gives rise to a nondegenerate $((1/3\,\boldsymbol{Z})/\boldsymbol{Z})$-valued quadratic form on $E_6^*/E_6 \cong \boldsymbol{Z}/3$; the short vectors of E_6^* must all be in the two nontrivial classes of E_6^*/E_6, and divided equally between them. The Weyl group permutes each of the two classes because it is generated by reflections $u \leftrightarrow u-(\alpha, u)\alpha \equiv u \bmod E_6$. Provided u and u' are in the same class mod E_6, $(u, u') \bmod 1$ is independent of the choice of u, u' and is either 1/3 or 2/3, but the latter cannot occur, for then if u_1, u_2, u_3 are any minimal vectors of E_6^* in the same class mod E_6 we would have $(u_i, u_j)=\delta_{ij}-1/3$ whence $u_1+u_2+u_3=0$, so the minimal vectors would span only a rank-2 sublattice of E_6^*, which is ridiculous."

References

[Br] C. Bramble, A collineation group isomorphic with the group of the double tangents of the plane quartic, Amer. J. Math., XL (1918), 351-365.

[B] N. Bourbaki, Groupes et Algèbres de Lie, Chap. 4, 5 et 6, Hermann, Paris, 1968.

[CS] J. Conway and N. Sloane, Sphere Packings, Lattices and Groups, Grundlehren Math. Wiss., **290**, Springer, 1988.

[F] J. Frame, The classes and representations of the groups of 27 lines and 28 bitangents, Annali di Mat. Ser. IV, **32** (1951), 83-119.

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

[M] Ju. Manin, Cubic Forms, 2nd ed., North-Holland, 1986.

[N1] A. Néron, Propriétés arithmétiques de certaines familles de courbes algébriques, Proc. Intern. Math. Congr. Amsterdam 1954, vol. III, 481-488.

[N2] A. Néron, Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. I. H. E. S., **21** (1964).

[OS] K. Oguiso and T. Shioda, The Mordell-Weil lattice of a rational elliptic surface, Comment. Math. Univ. St. Pauli, **40** (1991), 83-99.

[S1] T. Shioda, Mordell-Weil lattices and Galois representation, I, II, III, Proc. Japan Acad., **65**A (1989), 267-271, 296-299, 300-303.

[S2] T. Shioda, Construction of elliptic curves over $\boldsymbol{Q}(t)$ with high rank: a preview, Proc. Japan Acad., **66**A (1990), 57-60.

[S3] T. Shioda, Mordell-Weil lattices and sphere packings, to appear in Amer. J. Math..

[S4] T. Shioda, Mordell-Weil lattices of type E_8 and deformation of singularities, in Prospects in Complex Geometry, SLN, **1468** (1991), 177-202.

[S5] T. Shioda, On the Mordell-Weil lattices, Comment. Math. Univ. St. Pauli, **39** (1990), 211-240.

[S6] T. Shioda, Theory of Mordell-Weil lattices, to appear in Proc. ICM 1990, Kyoto.

[S7] T. Shioda, An infinite family of elliptic curves over $\boldsymbol{Q}$ with large rank via Néron's method, to appear in Invent. Math..

[Si] J. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, 1986.

[T1] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, Lecture Notes in Math., **476** (1975), 33-52.

[T2] J. Tate, Variation of the canonical height of a point depending on a parameter, Amer. J. Math., **105** (1983), 287-294.

[W1] A. Weil, Abstract versus classical algebraic geometry, Proc. Intern. Math. Congr. Amsterdam 1954, vol. III, 550-558; Collected Papers, vol. II, Springer-Verlag, 1980, 180-188.

[W2] A. Weil, Foundations of Algebraic Geometry, AMS, 1962.

Tetsuji SHIODA

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Tokyo
Japan