51. *Triangles and Elliptic Curves. II*

By Takashi ONO

Department of Mathematics, The Johns Hopkins University, U. S. A.

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1994)

This is a continuation of my preceding paper [1] which will be referred to as (I) in this paper. In (I), to each parameter $t=(a, b, c)$, we associated a pair (E_t, π_t) of an elliptic plane curve and a point on it. In this paper, we shall find an elliptic space curve C in a fibre of the map $t \mapsto E_t$ so that the map $t \mapsto \pi_t$ is an isogeny: $C \to E = E_t$, $t \in C$. As in (I), this paper will contain an assertion on the Mordell-Weil group $E(k)$ when k is a number field.

§1. Space *T*. Let k be a field of characteristic $\neq 2$ and $\bar{k}$ be the algebraic closure of k. Let $l=l(t)$, $m=m(t)$, $n=n(t)$ be independent linear forms on the vector space $\bar{k}^3$. Our parameter space is defined by

(1.1) $$T=\{t \in \bar{k}^3 ; (l^2-m^2)(m^2-n^2)(n^2-l^2) \neq 0\}.$$

For each $t \in T$, put

(1.2) $$P_t=(l^2-n^2)+(m^2-n^2),$$

(1.3) $$Q_t=(l^2-n^2)(m^2-n^2).$$

Then we have

(1.4) $$P_t^2-4Q_t=(l^2-m^2)^2.$$

By the definition of T, we obtain elliptic curves

(1.5) $$\begin{aligned} E_t : y^2 &= x^3+P_t x^2+Q_t x \\ &= x(x-(n^2-l^2))(x-(n^2-m^2)), \quad t \in T. \end{aligned}$$

One verifies easily that

(1.6) $$\pi_t=(n^2, lmn) \in E_t, \quad t \in T.$$

If forms l, m, n have coefficients in k and if $t \in T(k)=T \cap k^3$, then the elliptic curve E_t is defined over k and $\pi_t \in E_t(k)=E_t \cap k^2$.

(1.7) **Example.** If we put $l(t)=(b+a)/2$, $m(t)=(b-a)/2$, $n(t)=c/2$, for $t=(a, b, c) \in T$, then we find ourselves in the situation of (I): $P_t=(a^2+b^2-c^2)/2$, $Q_t=(a+b+c)(a+b-c)(a-b+c)(a-b-c)/16$ and $\pi_t=(c^2/4, c(b^2-a^2)/8)$.

(1.8) **Example.** In §2 we shall meet the simplest situation where $l(t)=a$, $m(t)=b$, $n(t)=c$. In this case, we have $P_t=a^2+b^2-2c^2$, $Q_t=(a^2-c^2)(b^2-c^2)$ and $\pi_t=(c^2, abc)$.

Back to general l, m, n, we shall consider the equivalence relation in T defined by

(1.9) $$t \sim t' \Leftrightarrow E_t=E_{t'}, \quad t, t' \in T.$$

In other words,

(1.10) $$t \sim t' \Leftrightarrow P_t=P_{t'}, \quad Q_t=Q_{t'}, \quad t, t' \in T.$$

Now call t_0 a point in T fixed once for all and consider the class F containing t_0:

(1.11) $$F=\{t \in T ; t \sim t_0\}.$$

Since $E_t = E_{t_0}$ for $t \in F$, the points π_t in (1.6) induces obviously a map:

(1.12) $$\pi : F \to E = E_{t_0}.$$

§2. Structure of *F*. Let t_0 be a point in T fixed once for all. We set $M = l(t_0)^2 - n(t_0)^2$, $N = m(t_0)^2 - n(t_0)^2$.

Notice that $M \neq 0$, $N \neq 0$ and $M \neq N$ in view of (1.1). Furthermore, by (1.2), (1.3), (1.5), (1.9), (1.10), we obtain, for $t \in T$,

(2.1) $$t \in F \Leftrightarrow (l^2 - n^2) + (m^2 - n^2) = M + N \text{ and } (l^2 - n^2)(m^2 - n^2) = MN.$$

The right-hand side of (2.1) amounts to

(2.2) $$(l^2 - n^2, m^2 - n^2) = (M, N) \text{ or } = (N, M).$$

In other words, we have

(2.3) $$\begin{cases} n^2 + M = l^2 \\ n^2 + N = m^2 \end{cases} \text{or} \begin{cases} n^2 + N = l^2 \\ n^2 + M = m^2. \end{cases}$$

In general, for $M, N \in \bar{k}$ such that $M \neq 0$, $N \neq 0$, $M \neq N$, put

(2.4) $$E(M, N) = \{x \in P^3(\bar{k})\ ;\ x_0^2 + Mx_1^2 = x_2^2,\ x_0^2 + Nx_1^2 = x_3^2\}.$$

It is well-known in elementary algebraic geometry that (2.4) is an elliptic curve with the origin $0 = (1, 0, 1, 1)$, defined over k whenever $M, N \in k$ (see, e.g., [2] Chapter 4). Therefore if we denote by $E(M, N)_0$ the affine part of $E(M, N)$, i.e., the subset of $E(M, N)$ consisting of points $x = (x_0, 1, x_2, x_3)$, then we find that

(2.5) $$\Phi F = \{\Phi_t\ ;\ t \in T,\ t \sim t_0\} = E(M, N)_0 \cup E(N, M)_0,$$

with $E(M, N)_0 \cap E(N, M)_0 = \emptyset$, $M = l(t_0)^2 - n(t_0)^2$, $N = m(t_0)^2 - n(t_0)^2$, where we called Φ the matrix in $GL_3(\bar{k})$ determined by

(2.6) $$\Phi_t = = \begin{pmatrix} l(t) \\ m(t) \\ n(t) \end{pmatrix}, \quad t \in T.$$

§3. Map π. Suggested by (2.5), consider an algebraic set C_0 in $\bar{k}^3$ defined by

(3.1) $$C_0 = \Phi^{-1}(E(M, N)_0) = \{t \in \bar{k}^3\ ;\ n^2 + M = l^2,\ n^2 + N = m^2\}.$$

Since C_0 is a subset of F by (2.5) the map π in (1.12) induces a morphism $\pi_0 : C_0 \to E = E_{t_0}$ defined by $\pi_0(t) = \pi_t = (n^2, lmn)$ (cf. (1.6)). Now denote by C the projective completion of C_0:

(3.2) $$C = \{P \in P^3(\bar{k})\ ;\ n^2 + Mx_1^2 = l^2,\ n^2 + Nx_1^2 = m^2\},$$

where $P = (x_0, x_1, x_2, x_3)$, $l = l(x_0, x_2, x_3)$, $m = m(x_0, x_2, x_3)$, $n = n(x_0, x_2, x_3)$. Of course $C \approx E(M, N)$ over $\bar{k}$. The affine morphism π_0 extends to a projective morphism

(3.3) $$\pi^* : C \to E = E_{t_0}$$

so that

(3.4) $$\pi^*(P) = (n^2 x_1,\ lmn,\ x_1^3) \in E \subset P^2(k),$$

with $l = l(x_0, x_2, x_3)$, etc. As an origin of the elliptic curve C we choose $O_C = (e_0, 0, e_2, e_3)$ such that

$$\Phi \begin{pmatrix} e_0 \\ e_2 \\ e_3 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Then we have $\pi^*(O_C) = O_E = (0, 1, 0)$. One verifies easily that $\mathrm{Ker}\,\pi^* \approx \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$. Therefore π^* is an isogeny and we see that the map $\pi : F \to E$ is surjective.

§4. Number fields. Notation being as before, let us assume that the linear forms l, m, n have coefficients in k and the point t_0 belongs to $T(k)$. Then $\Phi \in GL_3(k)$, $M, N \in k$, elliptic curves C, $E = E_{t_0}$ are defined over k and so are the isogeny π^* in (3.3) and the map $\pi : F \to E$ in (1.12).

Assume now that k is a number field; hence $k \subset \bar{\boldsymbol{Q}}$. Then the isogeny $\pi^* : C \to E = E_{t_0}$ and its inverse isogeny $E \to C$ (both defined over k, as easily verified) induce homomorphisms $C(k) \rightleftarrows E(k)$ of finitely generated abelian groups, with finite kernels; hence rank $C(k) = \mathrm{rank}\, E(k)$ and we have

$$[E(k) : \pi^*(C(k))] < +\infty. \tag{4.1}$$

Since $C_0(k) \subset F(k)$, it follows at once from (4.1) that the subgroup of $E(k)$ generated by $\pi(F(k))$ is of finite index in $E(k)$.

Summing up, we obtain

Theorem. *Let k be a number field, l, m, n independent linear forms on $\bar{\boldsymbol{Q}}^3$ with coefficients in k, T the subset of $\bar{\boldsymbol{Q}}^3$ formed by points t such that*

$$(l(t)^2 - m(t)^2)(m(t)^2 - n(t)^2)(n(t)^2 - l(t)^2) \neq 0$$

and E_t, $t \in T$, the elliptic curve in $P^2(\bar{Q})$ defined (affinely) by

$$E_t : y^2 = x(x - (n(t)^2 - l(t)^2))(x - (n(t)^2 - m(t)^2)).$$

For a point $t \in T(k)$, let

$$F = \{t_0 \in T \,;\, E_t = E_{t_0}\},$$

this being an algebraic set defined over k. Let π be the map $F \to E = E_{t_0}$ defined by

$$\pi(t) = (n(t)^2,\ l(t)m(t)n(t)).$$

Then the group generated by the set $\pi(F(k)) \subset E(k)$ is of finite index in the Mordell-Weil group $E(k)$.

References

[1] Ono, T.: Triangles and elliptic curves. Proc. Japan. Acad., **70A**, 106–108 (1994).

[2] ——: Variations on a Theme of Euler. Plenum, New York (to appear).

[3] Silverman, J. H.: The Arithmetic of Elliptic Curves. Springer, New York (1986).