Triangles and Elliptic Curves. IV

By Takashi ONO

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

(Communicated by shokichi IYANAGA, M. J. A., May 12, 1995)

This is a continuation of my preceding papers [1], [2], [3], which will be referred to as (I), (II), (III) in this paper. As in (II), (III), to each triple (l, m, n) of independent linear forms on $\bar{k}^3$, k being a field of characteristic not 2 and $\bar{k}$ its algebraic closure, we associate a space

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

Since the condition for $t \in T$ in (0.1) is given by a homogeneous polynomial, we can speak of the subset $P(T)$ of the projective plane

(0.2) $P(T) = \{[t] \in P^2(\bar{k}) ;$
$(l^2 - m^2)(m^2 - n^2)(n^2 - l^2) \neq 0\},$

which is the complement of the complete quadrangle given by six lines $(l^2 - m^2)(m^2 - n^2)(n^2 - l^2) = 0$. Since T is the total space of a bundle whose fibres are (affine parts of) elliptic curves in $P^3(\bar{k})$, it is natural to think of their images under the canonical map $T \to P(T)$ given by $t \mapsto [t]$, the homogeneous coordinates for t. In this paper, we shall study this aspect of the space T and show that there is a close relation between certain family of elliptic curves and a single plane conic, over a given field k of rationality. If X denotes a set of geometric objects, we shall denote by $X(K)$ (or by X_K occasionally) the subset of X which is rational over K.

§1. Basic diagram. Along with the canonical map $P : T \to P(T)'$ ((0,1), (0,2)), we consider the diagram:

$$\begin{array}{ccc} T & \xrightarrow{P} & P(T) \\ p \downarrow & & \downarrow \tilde{p} \\ \Omega & \xrightarrow{r} & \Lambda \end{array} \tag{1.1}$$

where

(1.2) $\Omega = \{\omega = (M, N) \in \bar{k} \times \bar{k} ;$
$MN(M - N) \neq 0\},$

(1.3) $\Lambda = \{\lambda \in \bar{k} ; \lambda \neq 0,1\},$

(1.4) $p(t) = (l^2 - n^2, m^2 - n^2),\ r(\omega) = \dfrac{N}{M},$

(1.5) $\tilde{p}[t] = r(p(t)) = \dfrac{m^2 - n^2}{l^2 - n^2}.$

Since $\bar{k}$ is algebraically closed, p is surjective and hence so is $\tilde{p}$. For an $\omega = (M, N) \in \Omega$, P induces naturally a map

(1.6) $P_\omega : p^{-1}(\omega) \to \tilde{p}^{-1}(r(\omega)).$

Again since $\bar{k}$ is algebraically closed, we see that P_ω is surjective and each fibre is of the form $\{\pm t\}$, $t \in T$; in other words, P_ω is a covering of degree 2. The fibres of p, $\tilde{p}$ are described as follows. For an $\omega = (M, N)$, let

(1.7) $E(\omega) = \{[x] \in P^3(\bar{k}) ;$
$x_0^2 + Mx_1^2 = x_2^2,\ x_0^2 + Nx_1^2 = x_3^2\},$

this being an elliptic curve in $P^3(\bar{k})$ (see e.g., [4] Chap. 4). Deleting four 2-torsion points out of (1.7), we obtain the affine part of (1.7):

(1.8) $E_0(\omega) = \{(x, y, z) \in \bar{k}^3 ; z^2 + M = x^2,$
$z^2 + N = y^2\}.$

From (1.4), (1.8), we have a bijection

(1.9) $p^{-1}(\omega) \xrightarrow{\sim} E_0(\omega),\ \omega \in \Omega,$

given by $t \mapsto (l(t), m(t), n(t)),\ t \in p^{-1}(\omega)$.

On the other hand, for a $\lambda \in \Lambda$, let

(1.10) $c(\lambda) = \{[x, y, z] \in p^2(\bar{k}) ;$
$y^2 - z^2 = \lambda(x^2 - z^2)\},$

this being a nonsingular conic in $p^2(\bar{k})$. Denoting by H the complete quadrangle given by

(1.11) $H = \{[x, y, z] \in p^2(\bar{k}) ;$
$(x^2 - y^2)(y^2 - z^2)(z^2 - x^2) = 0\},$

we have

(1.12) $C(\lambda) \cap H = \{[1,1,1], [-1,1,1],$
$[1, -1,1], [1,1, -1]\}$

which is independent of $\lambda \in \Lambda$.

Deleting these four points from $C(\lambda)$, write

(1.13) $C_0(\lambda) = C(\lambda) - H.$

From (1.5), (1.11), (1.12), (1.13), we have a bijection

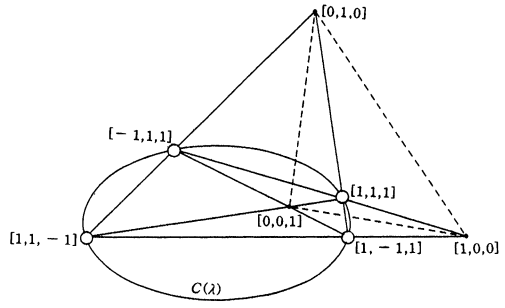
(1.14) $\tilde{p}^{-1}(\lambda) \xrightarrow{\sim} C_0(\lambda)$

given by $[t] \mapsto [l(t), m(t), n(t)]$.

In view of (1.6), (1.9), (1.14), we obtain a covering of degree 2:

(1.15) $\pi_\omega : E_0(\omega) \to C_0\left(\dfrac{N}{M}\right),\ \omega = (M, N) \in \Omega,$

given by $(x, y, z) \mapsto [x, y, z]$.



§2. Rationality. We shall consider what will happen to (1.15) if we restrict our attention to any field k of rationality (of characteristic $\neq 2$). We start with a triple (l, m, n) of independent linear forms defined over k and associate to it the space T defined by (0.1). The diagram (1.1) induces in an obvious way the diagram:

$$\begin{array}{ccc} T(k) & \xrightarrow{P_k} & P(T)(k) \\ p_k \downarrow & & \downarrow \bar{p}_k \\ \Omega(k) & \xrightarrow{r_k} & \Lambda(k) \end{array} \tag{2.1}$$

For an $\omega \in \Omega(k)$, P_k induces naturally a map

$$P_{\omega,k} : p_k^{-1}(\omega) \to \bar{p}_k^{-1}(r_k(\omega)). \tag{2.2}$$

This map is not necessarily surjective, although each fibre consists of two points as before. Along with (1.9), (1.14) and (1.15), we have bijections

$$p_k^{-1}(\omega) \xrightarrow{\sim} E_0(\omega)(k), \quad \omega \in \Omega(k), \tag{2.3}$$

$$\bar{p}_k^{-1}(\lambda) \xrightarrow{\sim} C_0(\lambda)(k), \quad \lambda \in \Lambda(k) \tag{2.4}$$

and a map

$$\pi_{\omega,k} : E_0(\omega)(k) \to C_0\left(\frac{N}{M}\right)(k), \ \omega = (M, N). \tag{2.5}$$

For any $\lambda \in \Lambda(k)$, let

$$\Omega_\lambda(k) = r_k^{-1}(\lambda) = \{\omega = (M, N) \in \Omega(k) ; N = \lambda M\}. \tag{2.6}$$

This set is identified with $k^\times$ by $(M, \lambda M) \leftrightarrow M$ and we denote by $\Omega_\lambda(k)/(k^\times)^2 (\approx k^\times/(k^\times)^2)$ a complete set of representatives of $\Omega_\lambda(k)$ under the action of the group $(k^\times)^2$. Then we have

$$C_0(\lambda)(k) = \bigcup_{\omega \in \Omega_\lambda(k)/(k^\times)^2} \mathrm{Image}(\pi_{\omega,k}), \text{ (disjoint).} \tag{2.7}$$

In fact, (2.5) implies that the right hand side of (2.7) is contained in the left hand side. Conversely, take any point $[t] \in C_0(\lambda)(k)$, with $t \in k^3$. Then $y^2 - z^2 = \lambda(x^2 - z^2)$. Since $[t] = [\rho t]$ for any $\rho \in k^\times$, we may assume that $x^2 - z^2 = M \in k^\times/(k^\times)^2$. Then $y^2 - z^2 = \lambda M$. In other words, $t \in E_0(\omega)(k)$ with $\omega = (M, \lambda M)$, which shows that the left hand side of (2.7) is contained in the right hand side. Finally take a point $[t] \in \mathrm{Im}(\pi_{\omega,k}) \cap \mathrm{Im}(\pi_{\omega',k})$, with $\omega = (M, \lambda M)$, $\omega' = (M', \lambda M') \in \Omega_\lambda(k)/(k^\times)^2$. Then we have $M = \rho^2(x^2 - z^2)$, $M' = \rho'^2(x^2 - z^2)$ for some $\rho, \rho' \in k^\times$. Hence $\omega' = (M', \lambda M') = \rho'^2(x^2 - z^2, y^2 - z^2) = (\rho'^2/\rho^2)(\rho^2(x^2 - z^2), \rho^2(y^2 - z^2)) = (\rho'/\rho)^2 (M, \lambda M) = (\rho'/\rho)^2\omega$. Since ω, ω' are representatives of $\Omega_\lambda(k) \bmod (k^\times)^2$, we must have $\omega = \omega'$, so the union in (2.7) is disjoint, Q.E.D.

Summarizing the arguments, we restate (2.7) as

(2.8) **Theorem.** *Let k be a field of chacteristic not 2. For a $\lambda \in k$, $\lambda \neq 0,1$, let $C(\lambda)$ be the plane conic* (1.10) *and $C_0(\lambda)$ the portion of it given by* (1.13). *For $M \in k^\times/(k^\times)^2$, let $E(M, \lambda M)$ be the space elliptic curve* (1.7) *and $E_0(M, \lambda M)$ the portion of it given by* (1.8). *Then we have*

$$C_0(\lambda)(k) = \bigcup_{M \in \Omega k^\times/(k^\times)^2} P(E_0(M, \lambda M)(k)) \text{ (disjoint),}$$

where P is the canonical map $t \mapsto [t]$, $t \in k^3 - \{0\}$. Furthermore each fibre of P (restricted on $E_0(M, \lambda M)(k)$) consists of two points.

§3. An example. As an illustrative example of (2.8), let us consider the case $k = \boldsymbol{F}_q$, the finite field with q elements, $2 \nmid q$. Since $[k^\times : (k^\times)^2] = 2$, we choose as M elements 1 and r, r being a generator of the cyclic group $k^\times$. Let λ be an element of k such that $\lambda \neq 0,1$. Let χ be the nontrivial quadratic character of $k^\times$, i.e. the character so t hat $\chi(r) = -1$. Since the conic is given by the ternary form:

$$C(\lambda) : \lambda x^2 - y^2 + (1 - \lambda)z^2 = 0, \tag{3.1}$$

we have ([5] p. 145, Th. 2E)

$$\#C(\lambda)(k) = q + 1, \quad \#C_0(\lambda)(k) = q - 3. \tag{3.2}$$

Using character sums, we obtain

$$\#E_0(1, \lambda)(k) = q - 3 + S_1, \quad S_1 = \sum_{x \in k} \chi(x(x + 1)(x + \lambda)), \tag{3.3}$$

$$\#E_0(r, r\lambda)(k) = q - 3 + S_r, \quad S_r = \sum_{x \in k} \chi(x(x + r)(x + r\lambda)). \tag{3.4}$$

Since each fibre of P restricted on $E_0(M, \lambda M)(k)$ consists of two points, we have, by (2.8), (3.3), (3.4),

$$q - 3 = \frac{1}{2}(q - 3 + S_1 + q - 3 + S_r) \tag{3.5}$$

and hence

$$S_1 + S_r = 0, \tag{3.6}$$

a relation which can also be verified directly using $\chi(r) = -1$. Since $\#E(1, \lambda)(k) = \#E_0(1, \lambda)(k) + 4$ and similarly for $E(r, r\lambda)$, we have, from (3.3), (3.4), (3.6),

$$q + 1 - \#E(r, r\lambda)(\boldsymbol{F}_q) \tag{3.7}$$

$$= -(q + 1 - \#E(1, \lambda)(\boldsymbol{F}_q).$$

Therefore, the formula (2.8) may be viewed as a geometric background for typical relations between elliptic curves which are quadratic twists of each other.

References

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

[2] T. Ono: Triangles and elliptic curves. II. Proc. Japan Acad., **70A**, 223–225 (1994).

[3] T. Ono: Triangles and elliptic curves. III. Proc. Japan Acad., **70A**, 311–314 (1994).

[4] T. Ono: Variations on a Theme of Euler. Plenum, New York (1995).

[5] W. M. Schmidt: Equations over Finite Fields. An Elementary Approach. LNM 536, Springer, Berlin, Heidelberg, New York (1976).