Triangles and Elliptic Curves. V

By Takashi ONO

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

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1995)

This is a continuation of my series of papers [4] each of which will be referred to as (I), (II), (III), (IV) in this paper. Let k be a field of characteristic not 2. We shall fix once for all a complete set $\mathcal{M}$ of representatives of $k^\times/(k^\times)^2$. For $M \in \mathcal{M}$ and an element $\lambda \neq 0,1$ of k, consider the set of k-rational points

(0.1) $E(M, \lambda M)(k) = \{p = [x_0, x_1, x_2, x_3];\ x_0^2 + Mx_1^2 = x_2^2,\ x_0^2 + \lambda M x_1^2 = x_3^2\}$

of the elliptic curve $E(M, \lambda M)$ and the bunch of (0.1) taken over $\mathcal{M}$:

(0.2) $\boldsymbol{E}(\lambda; k) = \bigcup_{M\in\mathcal{M}} E(M, \lambda M)(k).$[1)]

Denote by D the set of four points $[1,0, \pm 1, \pm 1]$ in P^3. For each λ, M, the set D is a subgroup of $E(M, \lambda M)(k)$ consisting of points P such that $2P = \mathcal{O} = [1,0,1,1]$; $D \approx \boldsymbol{Z}/2\boldsymbol{Z} \times \boldsymbol{Z}/2\boldsymbol{Z}$. From the definition of $\mathcal{M}$ we find that

(0.3) $E(M, \lambda M)(k) \cap E(M', \lambda M')(k) = D, \quad M \neq M'.$

In other words, the union in (0.2) is "disjoint" up to elements of D.

In this paper, we shall introduce a *surjective* map

(0.4) $c: \boldsymbol{E}(\lambda; k) \to P^1(k)$

which is an analogue of the branched covering of Riemann surfaces. We shall also examine this map for special fields k including some local and global fields in number theory.

§1. Map *c*. For $P = [x_0, x_1, x_2, x_3] \in \boldsymbol{E}(\lambda; k)$ in (0.2), put

(1.1) $\pi(P) = [x_2, x_3, x_0].$

Since each $M \in \mathcal{M}$ is $\neq 0$, $\pi(P)$ is a point in $P^2(k)$. For $\lambda \neq 0,1$ of k, let $C(\lambda)$ be the conic defined by

(1.2) $C(\lambda) = \{[x, y, z] \in P^2(\bar{k});\ y^2 - z^2 = \lambda(x^2 - z^2)\}.$

Clearly π induces a map, written again by π:

(1.3) $\pi: \boldsymbol{E}(\lambda; k) \to C(\lambda)(k).$

Furthermore,

(1.4) π is surjective.

In fact, take any point $Q = [x, y, z] \in C(\lambda)(k)$. If $x^2 = z^2$ then $y^2 = z^2$, so $Q = [\pm 1, \pm 1, 1]$. Therefore there is a point $P = [1,0, \pm 1, \pm 1]$ in D such that $\pi(P) = Q$. If $x^2 \neq z^2$, then there is a unique $M \in \mathcal{M}$ and an element $W \in k^\times$ such that $x^2 - z^2 = w^2 M$ and hence $y^2 - z^2 = w^2 \lambda M$. In other words, we have $\pi(P) = Q$ with $P = [z, w, x, y] \in E(M, \lambda M)(k)$. Q.E.D.

We can verify easily that, for $P, P' \in \boldsymbol{E}(\lambda; k)$,

(1.5) $\pi(P) = \pi(P') \Leftrightarrow P' = P$ or $-P$,

where $-P = [x_0, -x_1, x_2, x_3]$ is the inverse in the abelian group $E(M, \lambda M)(k)$ to which P belongs. Hence the fibre of π consists of two points P, $-P$ except for the case where $2P = \mathcal{O}$, i.e., $P \in D$. In the latter case, π induces on D a bijection: $[1,0, \pm 1, \pm 1] \leftrightarrow [\pm 1, \pm 1, 1] \in C(\lambda)(k)$.

Now consider the point $[1,1,1]$ on $C(\lambda)$ and the line L_∞ defined dy $Z = 0$. Let $[t] = [x, y, z]$ be a point on $C(\lambda)$ and $\sigma[t]$ the intersection of L_∞ and the line joining $[1,1,1]$ and $[t]$ (stereographic projection). When $[t] = [1,1,1]$ we understand by $\sigma[t]$ the point of intersection of L_∞ and the tangent at $[t]$ to $C(\lambda)$. The equation of the line is

(1.6) $(y - z)X + (z - x)Y + (x - y)Z = 0.$

Putting $Z = 0$ in (1.6), we use $[X, Y]$ as the homogeneous coordinates on L_∞ and identify $[X, Y]$ with the non-homogeneous coordinate $u = Y/X$ on $L_\infty = \boldsymbol{P}^1$. Consequently, we have

(1.7) $\sigma[t] = \dfrac{y - z}{x - z} = \lambda \dfrac{x + z}{y + z},$

$[t] = [x, y, z] \in C(\lambda).$

Notice that

(1.8) $\sigma[1,1,-1] = 1,\ \sigma[1,-1,1] = \infty,$

$\sigma[-1,1,1] = 0,\ \sigma[1,1,1] = \lambda.$

On the other hand, let u be a point of L_∞. Then the equation of the line joining u and $[1,1,1]$ is

(1.9) $uX - Y + (1 - u)Z = 0.$

---

1) As usual, we write $X(k)$ or X_k for the k-rational subset of a set X of geometric objects. We also use X for $X(\bar{k})$ occasionally where $\bar{k}$ denotes the algebraic closure of k. E.g., $X = E(M, \lambda M)$ is an elliptic curve in $P^3 = P^3(\bar{k})$ and (0.1) is the subset of k-rational points of X. On the other hand, since the set $\mathcal{M}$ is not necessarily finite, the set $\boldsymbol{E}(\lambda; k)$ in (0.2) is merely the union in the sense of sets.