17. *Construction of Elliptic Curves over $Q(t)$ with High Rank: a Preview*

By Tetsuji SHIODA
Department of Mathematics, Rikkyo University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 13, 1990)

1. Introduction. We have recently established a general method for constructing elliptic curves over the rational function field $k(t)$ (k any base field) having relatively high rank (up to 8). Not only can we give the explicit equation of such an elliptic curve, but also we can write down explicit rational points generating the full Mordell-Weil group.

As a preview and as an illustration of this method, we give here an example of an elliptic curve E over $\boldsymbol{Q}(t)$ with the Mordell-Weil group $E(\boldsymbol{Q}(t))$ of rank 8, together with a set of explicit generators.

More precisely, $E(\boldsymbol{Q}(t))$ has the structure of a lattice (the Mordell-Weil lattice), and as such, it is isomorphic to the root lattice of type E_8, and the said generators form "simple roots" in such a lattice.

As we briefly outlined in [2] (see Theorem 7.2), we use the invariants of the Weyl group $W(E_8)$ to define such an elliptic curve. The situation is quite analogous to the theory of algebraic equations. As everyone knows, it is not too easy to solve a given algebraic equation, but it is very easy to write down an algebraic equation with given roots, using the relation of the roots and coefficients of an equation. Now the latter can be viewed as the relation of the fundamental invariants of the symmetric group S_n, or the Weyl group $W(A_r)$ of type A_r ($r=n-1$), to the simple roots of the root system of that type.

The same idea, applied to $E_8, E_7, \cdots$ in place of A_r, yields just as easily, at least in principle, the elliptic curves over $\boldsymbol{Q}(t)$ or $k(t)$, with rank $8, 7, \cdots$, having the "prescribed roots", i.e. the prescribed data for generating rational points.

Actually the analogy can be pursued further. Just as a "general" equation of degree n over $\boldsymbol{Q}$ has the Galois group S_n, so does a "general" elliptic curve over $\boldsymbol{Q}(t)$ of the form (1) below give the Galois extension of $\boldsymbol{Q}$ with Galois group $W(E_8), \cdots$ or more precisely the Galois representation on the Mordell-Weil lattice $E(k(t))$, this time k being the algebraic closure of $\boldsymbol{Q}$, whose image is the full Weyl group (cf. [2], Theorem 7.1). Moreover it seems possible to give explicit examples of such, which we hope to discuss in future.

2. Example. Consider the elliptic curve over $\boldsymbol{Q}(t)$

$$E:\ y^2=x^3+px+q \tag{1}$$

where