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