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

$$p=p_0+p_1t+p_2t^2+p_3t^3$$
$$q=q_0+q_1t+q_2t^2+q_3t^3+t^5$$

with

$p_3=-155000$;

$p_2=33420503335873008209/3$;

$q_3=-1737232548737490620365295373 22/27$;

$p_1=-23935043038551120093488038837576 00/9$;

$q_2=29384484208045637330129737450711405278118 00/9$;

$p_0=56910702821267494453067022817596903029679628750/27$;

$q_1=-50331768198142414265423287580156219220650144145986685812 5/81$;

$q_0=30657892173372394597086613398499563737338253375565902284491 25\backslash$
$6302250000/729$.

The Mordell-Weil group $E(\boldsymbol{Q}(t))$ of this elliptic curve is of rank 8, and is generated by the following 8 rational points $P[i]$ $(i=1, \cdots, 8)$ of the form

$$x=(t/u)^2+at+b$$
$$y=(t/u)^3+ct^2+dt+e,$$

where $u=u[i]$ has the prescribed values which are 1, 2, 4, 8, 16, 32, 64, 128 in this example.

With respect to the height pairing defined in [2], these points form a "basis" of the root lattice E_8 in the sense of [1]. There are exactly 240 rational points of the above form, which correspond to the 240 roots of E_8: if a root u is a Z-linear combination of $u[i]$ with coefficients $n[i]$, then there is a unique point P which is the linear combination of $P[i]$ with the same coefficients $n[i]$.

$P[1]$

$x=1869463004949389679072558025/3-(149778401652871t)/3+t^2$,

$y=-4200076456142652747246234145946600411593 75/27$
$+(5608390718541629235386388625t)/3-74889200903935t^2+t^3$

$P[2]$

$x=6417287175824266816726388 25/4-(75997081321517t)/6+t^2/4$,

$y=-4389256831762739993799807131460194983656 25/216$
$+(5775557586950493372919355125t)/24-(75997082561485t^2)/8+t^3/8$

$P[3]$

$x=1885850540115623599727310275/48-(75216966555443t)/24+t^2/16$,

$y=-4255426409208745868997348953213627497468 75/1728$
$+(5657574625056104057550669625t)/192-(75216986393395t^2)/64+t^3/64$

$P[4]$

$x=1914923388164677503770460475/192-(75794622163847t)/96+t^2/64$,

$y=-4354252379199371115673564813198322068843 75/13824$
$+(5744841871325782591338240625t)/1536$
$-(75794939472775t^2)/512+t^3/512$

$P[5]$

$x=6549015415384056448136704 25/256-(76776054280463t)/384+t^2/256$,

$y=-4979118702394812776570570679709345229253125/1769472$
$+(2947301351472416341174772592 5t)/49152$
$-(76777323516175t^2)/2048+t^3/4096$
$P[6]$
$x=225211574796324617556231447 5/3072-(82303054477727t)/1536+t^2/1024,$
$y=-5564690087495737563821328533597325370093 75/884736$
$+(67760264337753444115296186 25t)/98304$
$-(82383782246815t^2)/32768+t^3/32768$
$P[7]$
$x=44520529717261555954063672 75/12288$
$-(118990670549183t)/6144+t^2/4096,$
$y=-15565761043004686986094013461930337113093 75/7077888$
$+(13892966861564145665253162625t)/786432$
$-(120256545050815t^2)/262144+t^3/262144$
$P[8]$
$x=13125368264931800885834272825/16384$
$-(419437994481407t)/24576+t^2/16384,$
$y=-40668741063101780315114166127282581845509375/56623104$
$+(14503587260122167232541039462 5t)/6291456$
$-(438042719065855t^2)/2097152+t^3/2097152$

3. Remarks. (i) The example given above is perhaps the first example ever known of an elliptic curve over $\boldsymbol{Q}(t)$ of rank 8, given with a set of explicit generators of the Mordell-Weil group. For that matter, we are not sure if a similar example, even for rank 6 or 7, has been previously known in the literature.

The detailed accounts of our method will be given in the article "Construction of elliptic curves with high rank via the invariants of the Weyl groups" (in preparation), where we treat also the case of rank 7 or 6, etc.

(ii) Once we have an elliptic curve over $\boldsymbol{Q}(t)$ with rank r, we can specialize t to rational numbers to obtain an infinite family of elliptic curves defined over $\boldsymbol{Q}$ with rank at least r, for all t in $\boldsymbol{Q}$ with only finitely many exception, by a result due to Néron, Tate and Silverman (cf. [3]). For our example of rank 8, we have 8 $\boldsymbol{Q}$-rational points on each specialized curve which are independent for almost all t in $\boldsymbol{Q}$. Further, with respect to the canonical height on $E_t(\boldsymbol{Q})$, the (partial) regulator of these points has the asymptotic behavior

$$\lim \det(\langle P_t[i], P_t[j]\rangle/h(t))=1/2^8$$

as the height $h(t)$ of t goes to infinity.

(iii) Though our construction method is simple, to carry out the computation we need a reasonably smart computer. We wish to thank A. Furukawa for his help in computation.

Added in Proof. The reason why the coefficients in the given example are so huge is as follows: first, the analogy of our method with the theory of algebraic equations, mentioned in the introduction, will explain that it is

natural to a certain extent; second, the initial data here ($u[1]=1, \cdots, u[8]=128$) are so chosen to satisfy the non-degeneracy condition stated in [2], Theorem 7.2. The first reason is inevitable, but we have recently improved the non-degeneracy condition, which allows one to produce examples with much smaller digits. This will be included in the paper in preparation.

References

[1] Bourbaki, N.: Groupes et Algèbres de Lie. Chap. 4, 5 et 6, Hermann, Paris (1968).
[2] Shioda, T.: Mordell-Weil lattices and Galois representation. I, II, III. Proc. Japan Acad., **65**A, 268–271; 296–303 (1989).
[3] Silverman, J.: The Arithmetic of Elliptic Curves. Springer-Verlag, New York-Berlin-Heidelberg-Tokyo (1986).