Some explicit integral polynomials with Galois group $W(E_8)$

Dedicated to Professor J-P. Serre

By Tetsuji SHIODA[*),**)]

(Communicated by Heisuke HIRONAKA, M.J.A., Sept. 14, 2009)

Abstract: We construct some explicit Galois extensions of $\mathbf{Q}$ (or integral polynomials) with Galois group $W(E_8)$ via Mordell-Weil lattices.

Key words: Weyl group; Galois group; Mordell-Weil lattices.

1. Introduction. In our previous work [6], we have studied the Galois representaions and the algebraic equations of exceptional type E_r $(r = 6, 7, 8)$ arising from Mordell-Weil lattices (MWL). In particular, we have established the construction theorem of infinitely many (linearly disjoint) Galois extensions of $\mathbf{Q}$ whose Galois group is isomorphic to the Weyl group $W(E_r)$, plus the proof that every extension of $\mathbf{Q}$ with Galois group $W(E_r)$ is obtained in that way (see Theorems 7.1 and 7.2 of [6]). Furthermore we have exhibited an explicit example of such for $r = 6$ and $r = 7$ [6, Examples 7.4 and 7.6], but the case $r = 8$ was omitted there, since some necessary information about the maximal subgroups of the Weyl group $W(E_8)$ was not available that time.

More recently, Jouve-Kowalski-Zywina [3] and Várilly-Alvarado-Zywina [9] have constructed some explicit $W(E_8)$-extensions of $\mathbf{Q}$. The former is based on the simple algebraic group of type E_8 and the characterisitic polynomial of its adjoint representation, while the latter uses the del-Pezzo surfaces of degree one.

Now the purpose of this note is to write down an explicit example of integral polynomial whose splitting field is a $W(E_8)$-extension of $\mathbf{Q}$ by the method of [6], which is entirely parallel to the case of $r = 6, 7$ mentioned above and whose construction seems to be more natural and somewhat simpler than those given by [3] or [9]. See §2 for the statements. For the proof (§3), we have only to apply the group-theoretic lemma on $W(E_8)$ obtained by [3] (Lemma 3.1 below), to the old data we examined nearly two decades ago. A few remarks are given in §4.

We refer to [2, Ch. 4] for the basic facts on the root lattice E_8 and the Weyl group $W(E_8)$; we simply recall that it has order $2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$ and it is almost a simple group; we have $W(E_8) = 2.O_8^+(2).2$ with the notation of Atlas [1] where $O_8^+(2)$ is a simple group. For Mordell-Weil lattices, we refer to [5].

I would like to dedicate this paper to Professor J-P. Serre who helped me in treating this type of problems in [6], which leads to the present paper.

2. An explicit example. Consider the elliptic curve $E/\mathbf{Q}(t)$ defined by

$$(2.1)\quad y^2 = x^3 + (1 + t + t^2 + t^3)\, x + 1 + t + t^2 + t^3 + t^5.$$

Let $\bar{\mathbf{Q}}$ be an algebraic closure of $\mathbf{Q}$. Then the Mordell-Weil lattice $E(\bar{\mathbf{Q}}(t))$ is isomorphic to the root lattice E_8, and there are exactly 240 rational points $P = (x(t), y(t))$, corresponding to the 240 roots of E_8, which are of the form:

$$(2.2)\quad x(t) = v^2t^2 + at + b,\ y(t) = v^3t^3 + ct^2 + dt + e$$

$(v, a, \ldots, e \in \bar{\mathbf{Q}})$. The quantity v satisfies an algebraic equation of degree 240 with integer coefficients $\Psi(v) = 0$, which is explicitly given as $\Psi(v) = F(v^2)$ with a polynomial $F(X) \in \mathbf{Z}[X]$ of degree 120 below.

We prove the following

Proposition 2.1. *The Galois representation*

$$\rho : Gal(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(E(\bar{\mathbf{Q}}(t))) \cong \mathrm{Aut}(E_8) = W(E_8)$$

is surjective.

Proposition 2.2. *Let $\mathcal{K}$ be the splitting field of the polynomial $\Psi(v)$ of degree 240. Then $\mathcal{K}/\mathbf{Q}$ is a Galois extension with Galois group $W(E_8)$.*

2010 Mathematics Subject Classification. Primary 11S05, 12F12, 14J27.

*) Research Institute for Mathematical Sciences, Kyoto University, Kitashirakawa Oiwake-cho, Sakyo-ku, Kyoto 606-8502, Japan.

**) Department of Mathematics, Rikkyo University, 3-34-1 Nishi-Ikebukuro, Toshima-ku, Tokyo 171-8501, Japan.

doi: 10.3792/pjaa.85.118

(2.3) $F(X)$

$$
\begin{aligned}
&= 1 + 60\,X + 1764\,X^2 + 33880\,X^3 + 478890\,X^4 \\
&+ 5327856\,X^5 + 48793140\,X^6 + 380483064\,X^7 \\
&+ 2598324795\,X^8 + 15932785020\,X^9 \\
&+ 89749362936\,X^{10} + 473980028160\,X^{11} \\
&+ 2387129524492\,X^{12} + 11610734817520\,X^{13} \\
&+ 54946822132728\,X^{14} + 253570184893640\,X^{15} \\
&+ 1139170471812505\,X^{16} + 4966863067888332\,X^{17} \\
&+ 20975997259257420\,X^{18} + 85751930578096488\,X^{19} \\
&+ 338777493097323270\,X^{20} \\
&+ 1286110326634556720\,X^{21} \\
&+ 4645243511039448812\,X^{22} \\
&+ 15781295779679038440\,X^{23} \\
&+ 49982542358210104135\,X^{24} \\
&+ 147131229010289262732\,X^{25} \\
&+ 404490375319591401040\,X^{26} \\
&+ 1051866512316875968008\,X^{27} \\
&+ 2627876995725411369560\,X^{28} \\
&+ 6344305570523224297840\,X^{29} \\
&+ 14520529565511555036172\,X^{30} \\
&+ 29688209277164999351080\,X^{31} \\
&+ 46109411843449203201495\,X^{32} \\
&+ 11874604308325191705300\,X^{33} \\
&- 30452071214048924433244 4\,X^{34} \\
&- 17105076074942263054276 00\,X^{35} \\
&- 65643732862172620229726 26\,X^{36} \\
&- 20640733068869514203178928\,X^{37} \\
&- 55485376072870265785653512\,X^{38} \\
&- 12879371307148972920602 3952\,X^{39} \\
&- 25774374278394981377949 3007\,X^{40} \\
&- 44246997536649454324553 1996\,X^{41} \\
&- 65505277692161352414071 7120\,X^{42} \\
&- 88447210722247535652156 8192\,X^{43} \\
&- 12805755957774303584653 07604\,X^{44} \\
&- 22327470939684184754687 36712\,X^{45} \\
&- 37096634512516500885282 16368\,X^{46} \\
&- 27876421711104355549244 45112\,X^{47} \\
&+ 10836668436242566282618 846201\,X^{48} \\
&+ 58617803145640098757603 141084\,X^{49} \\
&+ 16990117464551970161031 5084748\,X^{50} \\
&+ 36461936339585116525155 6074640\,X^{51} \\
&+ 62176081744259218874311 2149958\,X^{52} \\
&+ 85399699595475283912327 9092256\,X^{53} \\
&+ 93640307951485929035349 2992584\,X^{54} \\
&+ 81324298939942765427653 2027720\,X^{55} \\
&+ 56190160125725076756896 0750119\,X^{56} \\
&+ 13533674553485379304376 6886324\,X^{57} \\
&- 13590566540228718307363 77392248\,X^{58} \\
&- 64631963690929207574362 26504288\,X^{59} \\
&- 19274666150603339082780 988303322\,X^{60} \\
&- 43000266962344916776074 492071304\,X^{61} \\
&- 73878522660917308900155 611253488\,X^{62} \\
&- 93075326288055274100372 536594400\,X^{63} \\
&- 64536984699047964526813 581514542\,X^{64} \\
&+ 49300929293800996462069 228076464\,X^{65} \\
&+ 25286015965624245209267 5829367640\,X^{66} \\
&+ 48972511982630070359341 8835619104\,X^{67} \\
&+ 66048803116795842115599 5175713950\,X^{68} \\
&+ 68571214717040961543008 6676252264\,X^{69} \\
&+ 55168352695751047676214 5457969296\,X^{70} \\
&+ 28851267218177618529121 2516963736\,X^{71} \\
&- 74267572398719223747581 053086990\,X^{72} \\
&- 50090391596843962059203 1943919824\,X^{73} \\
&- 91054998448480854010225 8882764384\,X^{74} \\
&- 12069688736172132451950 49682159960\,X^{75} \\
&- 13886293081814467967087 22329894566\,X^{76} \\
&- 15693548447169242827536 40688567888\,X^{77} \\
&- 18237074756601707417526 27186852960\,X^{78} \\
&- 20488645114288287057847 72599553992\,X^{79} \\
&- 20351662785672331855152 68622860248\,X^{80} \\
&- 16874336273847373953026 66916386904\,X^{81}
\end{aligned}
$$

$$- 1115482759086740014512839085137184\,X^{82}$$
$$- 526761122020931966446367902077448\,X^{83}$$
$$- 585778648799393756054504186793 90\,X^{84}$$
$$+ 250069449965626638272171839412808\,X^{85}$$
$$+ 387136100056401973048117693037508\,X^{86}$$
$$+ 357325360560127756205870421947760\,X^{87}$$
$$+ 211364951183975868623079248436736\,X^{88}$$
$$+ 514186277248226946372341123 45296\,X^{89}$$
$$- 467738653934118744874242211411132\,X^{90}$$
$$- 717745534745000930784056206180 56\,X^{91}$$
$$- 538294658054476625645705334803 00\,X^{92}$$
$$- 230621395973051025402027211479 28\,X^{93}$$
$$+ 181610088533428638393897939 1048\,X^{94}$$
$$+ 113809696458089621452140867045 20\,X^{95}$$
$$+ 885536836200186293522568634820 1\,X^{96}$$
$$+ 350882311948395822379655302609 2\,X^{97}$$
$$+ 698584814104495914238234637808\,X^{98}$$
$$- 706078710984494230280625007 28\,X^{99}$$
$$- 981800556683347475495524341 82\,X^{100}$$
$$+ 139069087931147919858901980 96\,X^{101}$$
$$+ 612926366776909800536055203 92\,X^{102}$$
$$+ 401961206524742790546396411 44\,X^{103}$$
$$+ 178551819170392256499519280 83\,X^{104}$$
$$+ 633449306664507019256741478 0\,X^{105}$$
$$+ 227878741256845877459023889 6\,X^{106}$$
$$+ 737551796202189011654576888\,X^{107}$$
$$+ 432931186611007826071544506\,X^{108}$$
$$+ 429301341790049890169381 68\,X^{109}$$
$$+ 538259733452669451411924\,X^{110}$$
$$- 849592431713619927676092 0\,X^{111}$$
$$- 101833461610703030850412 7\,X^{112}$$
$$+ 300905188142683299657 00\,X^{113}$$
$$+ 679863686062085630984 64\,X^{114}$$
$$+ 589594315627301560499 2\,X^{115}$$
$$- 448019811798352498176\,X^{116}$$
$$- 280668086084640358400\,X^{117}$$
$$- 3365783326104268800\,X^{118}$$
$$+ 1750559212171657216\,X^{119}$$
$$+ 313989595009449984\,X^{120}.$$

3. Proof. Let $G = Im(\rho)$ be the image of ρ which is a subgroup of $W(E_8)$. By [6, §7] and [7, §8]) (cf. §4 below for a brief review), G is also isomorphic to the Galois group $\mathrm{Gal}(\mathcal{K}/\mathbf{Q})$, and we can view G as a subgroup of $\mathcal{S}_{240}$, the permutation group of the 240 roots of Ψ. [The two embeddings of G are compatible, since we have a natural inclusion of $W(E_8)$ into $\mathcal{S}_{240}$ which results from the ''generic'' case.] In this situation, we claim that $G = W(E_8)$.

For the polynomial $\Psi(X) = F(X^2) \in \mathbf{Z}[X]$, let $\Psi_p(X) = \Psi(X)(mod\ p)$ for a prime number p and we consider the decomposition of $\Psi_p(X) \in \mathbf{Z}/p\mathbf{Z}[X]$ into irreducible polynomials.

Taking $p = 5$, for example, we find that $\Psi_p(X)$ is a product of 16 distinct irreducible polynomials of degree 15, as is easily checked with a computer. We express this fact by saying that Ψ_p has the cycle type $(15)^{16}$.

Similarly, for $p = 7, 11, 13, 17$, we check that the cycle type is respectively given as follows:

$$(3)^8(12)^{18},\ (15)^{16},\ (20)^{12},\ (4)^2(8)^{29}.$$

Thus the Galois group G contains some elements having these cycle types.

Now we quote the following lemma from [3], which is reformulated in the same form as [6, Lemma 7.5] for the case $r = 6, 7$:

Lemma 3.1 (Jouve-Kowalski-Zywina)**.** *Let C_1 (resp. C_2) be the conjugacy class, which is unique, of an element in $W(E_8)$ with cycle type $(15)^{16}$ (resp. $(4)^2(8)^{29}$). Suppose that a subgroup H of $W(E_8)$ has the property that $H \cap C_i \neq \emptyset$ for $i = 1, 2$, then $H = W(E_8)$.*

Obviously it implies our claim that $G = W(E_8)$, which completes the proof of both Propositions 2.1 and 2.2.

4. Remarks.

4.1. Background: the generic situation. For the reader's convenience, we briefly recall the general set-up from [6, §6] as the background of the proof given above.

Let

$$(4.1) \qquad E_\lambda : y^2 = x^3 + \left(\sum_{i=0}^{3} p_i t^i\right)x + \sum_{j=0}^{3} q_j t^j + t^5$$

$$\lambda = (p_0, \dots, q_3) \in \mathbf{A}^8. \tag{4.2}$$

Assume that λ is generic, i.e. p_i, q_j are algebraically independent over $\mathbf{Q}$, and let k be the algebraic closure of $\mathbf{Q}(\lambda)$. It is known that the generic Galois representation

$$\rho_\lambda : Gal(k/\mathbf{Q}(\lambda)) \to \mathrm{Aut}(E(k(t))) \cong W(E_8)$$

is surjective and that the smallest Galois extension $\mathcal{K}_\lambda$ of $\mathbf{Q}(\lambda)$ such that $E(\mathcal{K}_\lambda(t)) = E(k(t))$ is equal to the splitting field of the universal polynomial of type E_8 of degree 240 $\Phi_{E_8}(u, \lambda) \in \mathbf{Q}[\lambda][u]$. See [6, §6] and [7, §8] for the proof and the definition of the universal polynomial of type E_r. In particular, the Galois group $Gal(\mathcal{K}_\lambda/\mathbf{Q}(\lambda))$ is isomorphic to $W(E_8)$ which acts transitively on the 240 roots of $\Phi_{E_8}(u, \lambda) = 0$.

4.2. Special cases. By applying Hilbert's irreducibility theorem [4] to the generic situation above, we obtain infinitely many $W(E_8)$-extensions of $\mathbf{Q}$ [6, Theorem 7.1]: for *most* choice of $\lambda_0 \in \mathbf{Q}^8$, the specialization $\lambda \to \lambda_0$ gives rise to such an extension.

Now the theme of the present note to make a *specific* choice of $\lambda_0 \in \mathbf{Q}^8$ for which this holds. The propositions in §2 assert that if we choose $\lambda_0 = (1, \dots, 1)$ (i.e. if all coefficients p_i, q_j of (4.1) are specialized to 1), then the specialized extension of $\mathbf{Q}$ does have the full Galois group $W(E_8)$. The polynomial $\Psi(v)$ in Proposition 2.2 is obtained from the universal polynomial $\Phi_{E_8}(u, \lambda)$ under the same specialization $\lambda \to \lambda_0$, except that we replace u by $v = 1/u$:

$$\Psi(v) = \Phi_{E_8}(u, \lambda_0)/u^{240}. \tag{4.3}$$

It is possible to derive the polynomial $\Psi(v)$ directly from the equations (2.1) and (2.2): first substitute (2.2) into (2.1) to obtain an identity in t of the form:

$$\phi_0 + \phi_1 t + \cdots + \phi_5 t^5 = 0 \ (\phi_i \in \mathbf{Q}[v, a, \dots, e])$$

and then eliminate $e, \dots, a$ from the simultaneous relations $\phi_0 = \cdots = \phi_5 = 0$ to obtain the equation $\Psi(v) = 0$. [In fact, the universal polynomial $\Phi_{E_8}(u, \lambda)$ is obtained in the same way starting from the generic equation (4.1) and (2.2) with $v = 1/u$; see the proof of [7, Theorem 8.3]].

If we consider the ideal $I = (\phi_0, \cdots, \phi_5)$ in the polynomial ring $\mathbf{Q}[v, a, \dots, e]$ and take its Gröbner basis (with respect to suitable ordering), then we obtain the relation $\Psi(v) = 0$, plus the polynomial expressions of $a, \dots, e$ in terms of v. For this approach, compare [8].

4.3. Other examples. Observe that the method described above allows one to produce as many explicit examples of integral polynomials and extensions with Galois group $W(E_8)$ as one wants. For example, starting from the elliptic curve $E'/\mathbf{Q}(t)$ with the equation:

$$y^2 = x^3 + \left(2 + t + t^2 + t^3\right) x + 1 + t + t^2 + t^3 + t^5, \tag{4.4}$$

we get also such a polynomial $\Psi'(v)$. We leave it as an excercise to check that the cycle type for $p = 11$ is $(4)^2(8)^{29}$, while that for $p = 43$ is $(15)^{16}$ in this case. By Lemma 3.1, we obtain another $W(E_8)$-extension which is distinct from the one given in §2.

4.4. Correction of [6, Theorem 7.3]. We take this opportunity to make a correction in our article [6]. In Theorem 7.3 (a formal analogue of Tate's conjecture), we asserted the equivalence of three conditions (i), (ii), (iii) stated there. But we want to cancel the condition (iii) from the statement.

Ackowledgements. We thank E. Kowalski (ETH, Zürich) for useful discussion about the recent article [3]. We thank the referee for careful reading of the paper and also for checking the computations.

References

[1] J. H. Conway *et al., Atlas of finite groups*, Oxford Univ. Press, Eynsham, 1985.

[2] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, Springer-Verlag, Berlin-New York, 1988, 2nd ed., 1993, 3rd ed., 1999.

[3] F. Jouve, E. Kowalski and D. Zywina, An explicit integral polynomial whose splitting field has Galois group $W(E_8)$, Journal de théorie des nombres de Bordeaux **20** (2008), no. 3, 761–782.

[4] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, Vieweg, Braunschweig, 1989.

[5] T. Shioda, On the Mordell-Weil lattices, Comment. Math. Univ. St. Paul. **39** (1990), no. 2, 211–240.

[6] T. Shioda, Theory of Mordell-Weil lattices, in *Proceedings of the International Congress of Mathematicians, Vol.* I, II (*Kyoto, 1990*), Math. Soc. Japan, Tokyo, 1991, pp. 473–489.

[7] T. Shioda, Construction of elliptic curves with high rank via the invariants of the Weyl groups, J. Math. Soc. Japan **43** (1991), no. 4, 673–719.

[8] T. Shioda, Gröbner basis, Mordell-Weil lattices and deformation of singularities, RIMS-1661, Kyoto Univ. (Preprint).

[9] A. Várilly-Alvarado and D. Zywina, Arithmetic E_8 lattices with maximal Galois action. (Preprint). `http://arxiv.org/abs/0803.3063`