On Lecacheux's family of quintic polynomials

By Akinari HOSHI*) and Masakazu KOSHIBA**)

(Communicated by Kenji FUKAYA, M.J.A., Dec. 14, 2020)

Abstract: Kida, Rikuna and Sato [6] developed a classification theory for Brumer's quintic polynomials via Kummer theory arising from associated elliptic curves. We generalize their results to elliptic curves associated to Lecacheux's quintic F_{20}-polynomials instead of Brumer's quintic D_5-polynomials.

Key words: Lecacheux's quintic polynomial; Kummer theory; elliptic curves.

1. Introduction. Let K be a field with $\operatorname{char} K \neq 2$, 5 and C_n be the cyclic group of order n. Let $D_5 \simeq C_5 \rtimes C_2$ be the dihedral group of order 10 and $F_{20} \simeq C_5 \rtimes C_4$ be the Frobenius group of order 20. Let $K(s,t)$ be the rational function field over K with two variables s,t. Brumer's quintic polynomial $\mathrm{Bru}(t,s;X)$ is defined to be

$$(1)\quad \mathrm{Bru}(t,s;X) := X^5 + (t-3)X^4 - (t-s-3)X^3 + (t^2-t-2s-1)X^2 + sX + t \in K(s,t)[X].$$

The polynomial $\mathrm{Bru}(t,s;X)$ is K-generic for D_5, namely (i) the Galois group of $\mathrm{Bru}(t,s;X)$ over $K(s,t)$ is isomorphic to D_5; and (ii) every D_5-Galois extension L/M, $\#M = \infty$, $M \supset K$, can be obtained as $L = \mathrm{Spl}_M(\mathrm{Bru}(b,a;X))$, the splitting field of $\mathrm{Bru}(b,a;X)$ over M, for some $a,b \in M$ (see Jensen, Ledet and Yui [4, Theorem 2.3.5]).

Kida, Rikuna and Sato [6] studied Brumer's quintic $\mathrm{Bru}(t,s;X)$ via Kummer theory arising from elliptic curves. The splitting field $\mathrm{Spl}_{K(s,t)}(\mathrm{Bru}(t,s;X))$ contains the unique quadratic subfield $K(s,t)(\sqrt{d_{t,s}})$ where

$$(2)\quad d_{t,s} := -4s^3 + (t^2-30t+1)s^2 + 2t(3t+1)(4t-7)s - t(4t^4-4t^3-40t^2+91t-4) \in K(s,t).$$

In this paper, we study the case where $K = \mathbf{Q}$. We search elements α and β in $\mathbf{Q}(s,t)$ such that the quadratic subfields of $\mathrm{Spl}_{\mathbf{Q}(s,t)}(\mathrm{Bru}(\beta,\alpha;X))$ and of $\mathrm{Spl}_{\mathbf{Q}(s,t)}(\mathrm{Bru}(t,s;X))$ coincide. According to Kida, Rikuna and Sato [6, Section 2], we restrict ourselves to treat the case $\beta = t$ and consider the equation

$$d_{t,s}u^2 = d_{t,\alpha}.$$

Define

$$d = d_{t,s},\ x = -4d\alpha,\ y = 4d^2u.$$

Then we obtain the associated elliptic curve

$$(3)\quad E_{t,s} : y^2 = x^3 + d(t^2-30t+1)x^2 - 8d^2t(3t+1)(4t-7)x - 16d^3t(4t^4-4t^3-40t^2+91t-4)$$

to Brumer's quintic polynomial $\mathrm{Bru}(t,s;X)$. This elliptic curve $E_{t,s}$ has an isogeny ϕ of degree 5 defined over $\mathbf{Q}(s,t)$. The 5-division polynomial of $E_{t,s}$ (see Silverman [8, Exercise 3.7]) has a quadratic factor $f_2(x)$ (see [1, Section 1]). Take a root θ of $f_2(x) = 0$. Then we obtain a point $A \in E_{t,s}(\overline{\mathbf{Q}(s,t)})$ of order 5 with $x(A) = \theta$. Apply the Vélu formula [10] to $\langle A\rangle$ and take $E^*_{t,s} = E_{t,s}/\langle A\rangle$ as the image of ϕ (see Kida, Rikuna and Sato [6, Section 2]):

$$(4)\quad E^*_{t,s} : y^2 = x^3 + d(t^2-30t+1)x^2 - 8d^2(26t^4-310t^3+327t^2+315t+26)x + 16d^3(68t^6-1120t^5+3804t^4+1760t^3 + 6929t^2+1380t+68).$$

After the specialization $\mathbf{Q}(s,t)^2 \ni (s,t) \mapsto (s',t') \in \mathbf{Q}^2$, we obtain that $\mathrm{Bru}(t',s';X)$, $E_{t',s'}$ and $E^*_{t',s'}$ are defined over $\mathbf{Q}$. After the specialization, for $s,t \in \mathbf{Q}$, we also write $\mathrm{Bru}(t,s;X)$, $E_{t,s}$ and $E^*_{t,s}$ which are defined over $\mathbf{Q}$ (not $\mathbf{Q}(s,t)$). Let $\phi^* : E^*_{t,s} \to E_{t,s}$ be the dual isogeny of ϕ. Then the quotient group $E_{t,s}(\mathbf{Q})/\phi^*(E^*_{t,s}(\mathbf{Q}))$ is finite by weak Mordel–Weil theorem (see [8, Chapter VIII, Section 1]).

Definition 1.1 (Kida, Rikuna and Sato [6, page 694])**.** Let s,t be rational numbers. For each $\mathbf{Q}$-rational point $P = (x(P), y(P)) \in E_{t,s}(\mathbf{Q})$, Brumer's polynomial $\mathrm{Bru}(P;X)$ with respect to P is defined to be

2010 Mathematics Subject Classification. Primary 11G05, 11R20, 12F20, 12G05.

*) Department of Mathematics, Niigata University, Niigata 950-2181, Japan.
**) Graduate School of Science and Technology, Niigata University, Niigata 950-2181, Japan.

doi: 10.3792/pjaa.97.001

$$\mathrm{Bru}(P;X) := \mathrm{Bru}\left(t, \frac{x(P)}{-4d}; X\right)$$

where $\mathrm{Bru}(t,s;X)$ is Brumer's polynomial as in (1) and $d = d_{t,s}$ is given as in (2).

We remark that there exists a rational point $P_0 = (-4ds, 4d^2) \in E_{t,s}(\mathbf{Q})$ and by the definition we have $\mathrm{Bru}(P_0;X) = \mathrm{Bru}(t,s;X)$.

Theorem 1.2 (Kida, Rikuna and Sato [6, Theorem 2.1])**.** *Let s,t be rational numbers. Let $E_{t,s}$ be the elliptic curve as in* (3)*. Let* $\mathrm{Bru}(P;X)$ *be Brumer's polynomial with respect to P as in Definition* 1.1 *with the splitting field* $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Bru}(P;X))$ *over* $\mathbf{Q}$.
(i) *For any* $\mathbf{Q}$*-rational point* $P \in E_{t,s}(\mathbf{Q})$, $\mathrm{Bru}(P;X)$ *is reducible over* $\mathbf{Q}$ *if and only if* $P \in \phi^*(E^*_{t,s}(\mathbf{Q}))$;
(ii) *There exists a bijection between the following two finite sets*

$$\{\textit{subgroup of order } 5 \textit{ in } E_{t,s}(\mathbf{Q})/\phi^*(E^*_{t,s}(\mathbf{Q}))\}$$

and

$$\{\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Bru}(P;X)) \mid P \in E_{t,s}(\mathbf{Q}) \setminus \phi^*(E^*_{t,s}(\mathbf{Q}))\}.$$

The bijection is induced by the correspondence $E_{t,s}(\mathbf{Q}) \ni P \mapsto \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Bru}(P;X))$.

The aim of this paper is to generalize Theorem 1.2 to elliptic curves associated to Lecacheux's quintic F_{20}-polynomial $\mathrm{Lec}(p,r;X)$ instead of Brumer's quintic D_5-polynomial $\mathrm{Bru}(t,s;X)$.

Let $\mathbf{Q}(p,r)$ be the rational function field over $\mathbf{Q}$ with two variables p,r. Lecacheux's quintic polynomial $\mathrm{Lec}(p,r;X)$ is defined to be

$$\text{(5)}\quad \begin{aligned}\mathrm{Lec}(p,r;X) := X^5 &+ \left(r^2(p^2+4) - 2p - \frac{17}{4}\right)X^4 \\ &+ \left(3r(p^2+4) + p^2 + \frac{13}{2}p + 5\right)X^3 \\ &- \left(r(p^2+4) + \frac{11}{2}p - 8\right)X^2 \\ &+ (p-6)X + 1 \in \mathbf{Q}(p,r)[X].\end{aligned}$$

The polynomial $\mathrm{Lec}(p,r;X)$ is known to be $\mathbf{Q}$-generic for F_{20} (see [4, Theorem 2.3.6]).

We will define the elliptic curve $\mathcal{E}_{p,r}$ associated to Lecacheux's polynomial $\mathrm{Lec}(p,r;X)$. Define

$$\text{(6)}\quad \begin{aligned}W_{p,r} := {} & 16(p^2+4)r^3 + 4(p^2+4)r^2 \\ & - 4(19p+41)r - 16p - 199,\end{aligned}$$

$$\begin{aligned}D_{p,r} := {} & \frac{W_{p,r}}{8}((p^4+5p^2+4) \\ & + p(p^2+3)\sqrt{p^2+4}).\end{aligned}$$

The splitting field $\mathrm{Spl}_{\mathbf{Q}(p,r)}(\mathrm{Lec}(p,r;X))$ contains the unique quadratic (resp. quartic) subfield $\mathbf{Q}(p,r)(\sqrt{p^2+4})$ (resp. $\mathbf{Q}(p,r)(\sqrt{D_{p,r}})$) (see Hoshi and Miyake [2, Lemma 7.3 and Lemma 7.4]; $\mathrm{Lec}(p,r;X)$ is $g^{F_{20}}_{p,r}(X)$ in [2]).

We search β such that the quartic subfields of $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p,\beta;X))$ and of $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p,r;X))$ coincide. We consider the equation

$$D_{p,r}u^2 = D_{p,\beta}.$$

Write $D = D_{p,r}$ and $W = W_{p,r}$. Then the above equation becomes

$$Wu^2 = W_{p,\beta}.$$

Define

$$x := 4(p^2+4)W\beta,\ y := 2(p^2+4)W^2u.$$

Then we get the associated elliptic curve

$$\text{(7)}\quad \begin{aligned}\mathcal{E}_{p,r} : y^2 = x^3 &+ (p^2+4)Wx^2 \\ &- 4(19p+41)(p^2+4)W^2x \\ &- 4(p^2+4)^2(16p+199)W^3\end{aligned}$$

to Lecacheux's quintic polynomial $\mathrm{Lec}(p,r;X)$.

The curve $\mathcal{E}_{p,r}$ has an isogeny ν of degree 5 defined over $\mathbf{Q}(p,r)$. We see that the 5-division polynomial of $\mathcal{E}_{p,r}$ (see Silverman [8, Exercise 3.7]) has the quadratic factor $f_2(x)$ (see [1, Section 1]). Take a root θ of $f_2(x) = 0$. Then we obtain a point $A \in \mathcal{E}_{p,r}(\overline{\mathbf{Q}(p,r)})$ of order 5 with $x(A) = \theta$, $\mathcal{E}^*_{p,r} = \mathcal{E}_{p,r}/\langle A\rangle$ as the image of ν and the dual isogeny $\nu^* : \mathcal{E}^*_{p,r} \to \mathcal{E}_{p,r}$ of ν as in (4) (see also Kida, Rikuna and Sato [6, Section 2]):

$$\begin{aligned}\mathcal{E}^*_{p,r} : y^2 = x^3 &+ (p^2+4)Wx^2 \\ &- 4(p^2+4)(52p^2-625p+833)W^2x \\ &+ 4(p^2+4)^2(272p^2-5000p+21713)W^3.\end{aligned}$$

As in the case of Brumer's quintic, after the specialization $\mathbf{Q}(p,r)^2 \ni (p,r) \mapsto (p,r) \in \mathbf{Q}^2$, we also write $\mathrm{Lec}(p,r;X)$, $\mathcal{E}_{p,r}$ and $\mathcal{E}^*_{p,r}$ for $p,r \in \mathbf{Q}$ which are defined over $\mathbf{Q}$ (not $\mathbf{Q}(p,r)$).

Definition 1.3. Let p,r be rational numbers. For each $\mathbf{Q}$-rational point $P = (x(P),y(P)) \in \mathcal{E}_{p,r}(\mathbf{Q})$, Lecacheux's polynomial $\mathrm{Lec}(P;X)$ with respect to P is defined to be

$$\mathrm{Lec}(P;X) := \mathrm{Lec}\left(p, \frac{x(P)}{4(p^2+4)W}; X\right)$$

where $\mathrm{Lec}(p,r;X)$ is Lecacheux's polynomial as in (5) and $W = W_{p,r}$ is given as in (6).

We note that there exists the point $Q_0 = (4r(p^2+4)W, 2(p^2+4)W^2) \in \mathcal{E}_{p,r}(\mathbf{Q})$ and we have $\mathrm{Lec}(Q_0;X) = \mathrm{Lec}(p,r;X)$ by the definition.

The following is the main theorem of this paper:

Theorem 1.4. *Let p, r be rational numbers. Let $\mathcal{E}_{p,r}$ be the elliptic curve as in* (7). *Let $\mathrm{Lec}(P;X)$ be Lecacheux's polynomial with respect to P as in Definition* 1.3 *with the splitting field $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(P;X))$ over* $\mathbf{Q}$.
(i) *For any $\mathbf{Q}$-rational point $P \in \mathcal{E}_{p,r}(\mathbf{Q})$, $\mathrm{Lec}(P;X)$ is reducible over $\mathbf{Q}$ if and only if $P \in \nu^*(\mathcal{E}^*_{p,r}(\mathbf{Q}))$;*
(ii) *There exists a bijection between the following two finite sets*

$$\{\textit{subgroup of order } 5 \textit{ in } \mathcal{E}_{p,r}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{p,r}(\mathbf{Q}))\}$$

and

$$\{\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(P;X)) \mid P \in \mathcal{E}_{p,r}(\mathbf{Q}) \setminus \nu^*(\mathcal{E}^*_{p,r}(\mathbf{Q}))\}.$$

The bijection is induced by the correspondence $\mathcal{E}_{p,r}(\mathbf{Q}) \ni P \mapsto \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(P;X))$.

2. Constructions of $\mathbf{Bru}(t,s;X)$ and $\mathbf{Lec}(p,r;X)$. We recall constructions of Brumer's polynomial $\mathrm{Bru}(t,s;X)$ and Lecacheux's polynomial $\mathrm{Lec}(p,r;X)$ in Lecacheux [7, pages 209–214].

2.1. Construction of $\mathbf{Bru}(t,s;X)$. We consider the elliptic curve:

$$E^*_t : y^2 + (1-t)xy - ty = x^3 - tx^2$$

with 5-torsion points

$$A = (0,0),\ 2A = (t,t^2),\ 3A = (t,0),\ 4A = (0,t).$$

The curve E^*_t is also called Tate normal form (see Husemöller [3, page 93, Definition 4.1]). The j-invariant of E^*_t is $\frac{(t^4-12t^3+14t^2+12t+1)^3}{t^5(t^2-11t-1)}$. There exists the elliptic curve $E_t = E^*_t/\langle A\rangle$ up to isomorphism with the isogeny $\phi : E^*_t \to E_t, X = \frac{t}{x} \mapsto X' = \frac{2(X-2)(X^2+2Xt-1)(2X^2-2Xt-2X+t)}{X(X-1)^2}$ of degree 5. Then by solving this for X, we have $X^5 + (t-3)X^4 + (1 - \frac{1}{4}X' - 2t^2 - \frac{7}{2}t)X^3 + (4t + 3 + 5t^2 + \frac{1}{2}X')X^2 + (-2t^2 - 2 - \frac{1}{4}X' - \frac{5}{2}t)X + t = 0$. Define $s = -2t^2 - 2 - \frac{1}{4}X' - \frac{5}{2}t$. Then the left-hand side of this equation becomes

$$\begin{aligned}\mathrm{Bru}(t,s;x) = x^5 &+ (t-3)x^4 - (t-s-3)x^3 \\ &+ (t^2-t-2s-1)x^2 + sx + t.\end{aligned}$$

We find that the elliptic curve E_t and the elliptic curve $E_{t,s}$ associated to $\mathrm{Bru}(t,s;X)$ as in (3) are isomorphic over some extension field (see also Kida, Rikuna and Sato [6, page 695]). The j-invariants of E_t and of $E_{t,s}$ are the same $\frac{(t^4+228t^3+494t^2-228t+1)^3}{t(t^2-11t-1)^5}$.

2.2. Construction of $\mathbf{Lec}(p,r;X)$. We consider the elliptic curve

$$\begin{aligned}\mathcal{E}^*_p : y^2 - \frac{1}{4}(p^2+4)(x^2+1) \\ = \frac{1}{2}(x^2-px-1)(2x-p)\end{aligned}$$

with 5-torsion points

$$A = (\alpha,\beta), 2A = \left(-\frac{1}{\alpha}, \frac{\beta}{\alpha}\right),$$
$$3A = \left(-\frac{1}{\alpha}, -\frac{\beta}{\alpha}\right), 4A = (\alpha, -\beta)$$

where α and $-1/\alpha$ are roots of $x^2 - px - 1$ and β satisfies

$$\beta^2 = \frac{1}{4}(p^2+4)(\alpha^2+4) = \frac{1}{4}(p^2+4)^{\frac{3}{2}}\alpha.$$

The j-invariant of $\mathcal{E}^*_p$ is $\frac{(p^2-12p+16)^3}{p-11}$. There exists the elliptic curve $\mathcal{E}_p = \mathcal{E}^*_p/\langle A\rangle$ up to isomorphism with the isogeny

$$\begin{aligned}\phi : \mathcal{E}^*_p \to \mathcal{E}_p, x \mapsto r = \tfrac{x+2p}{p^2+4} &+ \tfrac{(p^2+4)(px+2)}{L^2} \\ &+ \tfrac{x(p+2)+(p^2-p+6)}{L} - \tfrac{5p}{2(p^2+4)}\end{aligned}$$

of degree 5 where $L = x^2 - px - 1$. Define $l = -L/(p^2+4)$. Solving the equation for l, we have

$$\begin{aligned}l^5 &+ (r^2(p^2+4) - 2p - \tfrac{17}{4})l^4 \\ &+ (3r(p^2+4) + p^2 + \tfrac{13}{2}p + 5)l^3 \\ &- (r(p^2+4) + \tfrac{11}{2}p - 8)l^2 + (p-6)l + 1 = 0.\end{aligned}$$

The left-hand side of this equation yields $\mathrm{Lec}(p,r;l)$. The elliptic curve $\mathcal{E}_p$ and the associated elliptic curve $\mathcal{E}_{p,r}$ to $\mathrm{Lec}(p,r;X)$ as in (7) are isomorphic over some extension field with the j-invariant $\frac{(p^2+228p+496)^3}{(p-11)^5}$.

3. Proof of Theorem 1.4. The idea of the proof of Theorem 1.4 is to combine the results given in Hoshi and Miyake [2] and Kida, Rikuna and Sato [6]. According to [2, page 1078, Equation (25)], for $p, r \in \mathbf{Q}$, we define $k = \mathbf{Q}(\sqrt{p^2+4})$ and

$$(8) \quad s = -\frac{1}{4}\,(5p + 8r + 2p^2r + (2pr + 5)\sqrt{p^2+4}),$$
$$t = \frac{1}{2}\,(p + \sqrt{p^2+4}).$$

Then it follows that $\mathrm{Spl}_k(\mathrm{Bru}(t, s; X)) = \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p, r; X))$. The associated elliptic curves $E_{t,s}$ and $E^*_{t,s}$ given as in (3) and (4) are defined over k. According to [6, Section 3], we take elliptic curves E_t and E^*_t defined over k by

$$\begin{aligned} E_t : y^2 - (t-1)xy - ty &= x^3 - tx^2 \\ &\quad - 5t(t^2 + 2t - 1)x \\ &\quad - t(t^4 + 10t^3 - 5t^2 + 15t - 1), \\ E^*_t : y^2 - (t-1)xy - ty &= x^3 - tx^2. \end{aligned}$$

The curves $E_{t,s}$ (resp. $E^*_{t,s}$) and E_t (resp. E^*_t) are isomorphic over $F = k(\sqrt{d_{t,s}})$ where $d_{t,s}$ is given in (2) and we take an isogeny $\phi : E_{t,s} \to E^*_{t,s}$ and the dual isogeny $\phi^* : E^*_{t,s} \to E_{t,s}$. We also take an isogeny $\lambda^* : E^*_t \to E_t$ of degree 5. By [6, Theorem 3.1], there exists an injective homomorphism

$$E_{t,s}(k)/\phi^*(E^*_{t,s}(k)) \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{F}/F), \mathrm{Ker}\,\lambda^*(k)).$$

We will prove that there exists an injective homomorphism

$$\mathcal{E}_{p,r}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{p,r}(\mathbf{Q})) \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{F}/F), \mathrm{Ker}\,\lambda^*(k)).$$

We see that the elliptic curves $\mathcal{E}_{p,r}$ and $E_{t,s}$ are isomorphic over k with j-invariant $\frac{(p^2+228p+496)^3}{(p-11)^5}$. Indeed, we may find an isomorphism $f : \mathcal{E}_{p,r} \to E_{t,s}$ which is given explicitly as

$$(x, y) \mapsto (ax + b, uy)$$

where $a, b, u \in k$ are given by

$$\begin{aligned} a &= \frac{1}{8}\,(p^4 + 4p^2 + 2 + p(p^2+2)\sqrt{p^2+4}), \\ b &= \frac{5}{4}\,(p(p^2+2)(p^2+4) \\ &\quad + (p^4 + 4p^2 + 2)\sqrt{p^2+4})W_{p,r}, \\ u &= \frac{1}{16}\,((p^2+2)(p^4+4p^2+1) \\ &\quad + p(p^2+1)(p^2+3)\sqrt{p^2+4}) \end{aligned}$$

with $W_{p,r} = 16(p^2+4)r^3 + 4(p^2+4)r^2 - 4(19p + 41)r - 16p - 199$ given as in (6).

We obtain an isomorphism $f^* : \mathcal{E}^*_{p,r} \to E^*_{t,s}$ defined over k such that the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Ker}\,\nu^* & \longrightarrow & \mathcal{E}^*_{p,r} & \xrightarrow{\nu^*_{/\mathbf{Q}}} & \mathcal{E}_{p,r} & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle f^*_{/k}} & & \downarrow{\scriptstyle f_{/k}} & & \\ 0 & \longrightarrow & \mathrm{Ker}\,\phi^* & \longrightarrow & E^*_{t,s} & \xrightarrow[\phi^*_{/k}]{} & E_{t,s} & \longrightarrow & 0 \\ & & & & \downarrow{\scriptstyle g^*_{/F}} & & \downarrow{\scriptstyle g_{/F}} & & \\ 0 & \longrightarrow & \mathrm{Ker}\,\lambda^* & \longrightarrow & E^*_t & \xrightarrow[\lambda^*_{/k}]{} & E_t & \longrightarrow & 0 \end{array}$$

commutes with exact rows. The j-invariants of $\mathcal{E}^*_{p,r}$ and $E^*_{t,s}$ are the same $\frac{(p^2-12p+16)^3}{p-11}$. Therefore the isomorphism f induces an injection

$$\overline{f} : \mathcal{E}_{p,r}(k)/\nu^*(\mathcal{E}^*_{p,r}(k)) \hookrightarrow E_{t,s}(k)/\phi^*(E^*_{t,s}(k)).$$

By [6, Theorem 3.1] (see also Kida [5, Remark 4.3]), there exists an injective homomorphism

$$\overline{g} : E_{t,s}(k)/\phi^*(E^*_{t,s}(k)) \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{F}/F), \mathrm{Ker}\,\lambda^*(k)).$$

Then we also obtain an injective homomorphism

$$\overline{g} \circ \overline{f} : \mathcal{E}_{p,r}(k)/\nu^*(\mathcal{E}^*_{p,r}(k)) \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{F}/F), \mathrm{Ker}\,\lambda^*(k)).$$

Because the isogeny ν^* is defined over $\mathbf{Q}$, we get

$$\mathcal{E}_{p,r}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{p,r}(\mathbf{Q})) \hookrightarrow \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(\overline{F}/F), \mathrm{Ker}\,\lambda^*(k)).$$

Every point $P = (x(P), y(P)) \in \mathcal{E}_{p,r}(\mathbf{Q})$ defines a Kummer extension

$$L_P = F((\lambda^*)^{-1}(g \circ f(P)))$$

over F. In particular, via (8), we observe that

$$\begin{aligned} L_P &= \mathrm{Spl}_k\Big(\mathrm{Bru}\big(\tfrac{1}{2}(p + \sqrt{p^2+4}), \tfrac{x(f(P))}{-4d}; X\big)\Big) \\ &= \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(P; X)) \end{aligned}$$

where $\mathrm{Lec}(P; X) = \mathrm{Lec}(p, \frac{x(P)}{4(p^2+4)W}; X)$ as in Definition 1.3. Hence the group $\mathcal{E}_{p,r}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{p,r}(\mathbf{Q}))$ classifies the isomorphism classes of $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(P; X))$ with quartic subfield F (see also [6, Section 3]). □

By Theorem 1.4, we have the following result by the multiplication-by-2 map of the elliptic curve $\mathcal{E}_{p,r}$:

Corollary 3.1. *For a* $\mathbf{Q}$*-rational point* $P \in \mathcal{E}_{p,r}(\mathbf{Q})$ *and integer* n *with* $\gcd(n, 5) = 1$, $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(P; X)) = \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}([n]P; X))$ *where* $\mathrm{Lec}(P; X) = \mathrm{Lec}(p, \frac{x(P)}{4(p^2+4)W}; X)$ *as in Definition* 1.3.

In particular, for $P = Q_0 = (4r(p^2+4)W, 2(p^2+4)W^2)$ *and* $n = 2$, *we have* $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p,r;X)) = \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p,R;X))$ *where*

$$\begin{aligned} R &= \tfrac{x([2]Q_0)}{4(p^2+4)W}, \\ W &= 16(p^2+4)r^3 + 4(p^2+4)r^2 \\ &\quad - 4(19p+41)r - 16p - 199, \\ x([2]Q_0) &= 16(p^2+4)^2r^4 + 8(p^2+4)(19p+41)r^2 \\ &\quad + 4(32p^3+398p^2+128p+1592)r \\ &\quad + 16p^3 + 560p^2 + 1622p + 2477. \end{aligned}$$

Remark 3.2. We can also verify that $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p,r;X)) = \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p,R;X))$ in Corollary 3.1 by Hoshi and Miyake [2] via multi-resolvent polynomials. We take multi-resolvent polynomials $F^1_{a,a'}$ and $F^2_{a,a'}$ as in [2, page 1071] where $a = (s,t)$, $a' = (s',t')$. Using [2, page 1078, Method 2], via (8), we obtain that $\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p,r;X)) = \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(p,R;X))$ if and only if $F^1_{a,a'}$ or $F^2_{a,a'}$ has a linear factor over $k = \mathbf{Q}(\sqrt{p^2+4})$. Indeed, we see that $F^2_{a,a'}$ has a linear factor $x + \frac{1+2r}{2}\sqrt{p^2+4} + \frac{p-1}{2}$.

4. Examples of Theorem 1.4. We will give two examples of Theorem 1.4.

Example 4.1 ($p = 1$ and $r = -3$ with $\mathcal{E}_{1,-3}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{1,-3}(\mathbf{Q})) \simeq \mathbf{Z}/5\mathbf{Z}$)**.** We consider the case where $p = 1$ and $r = -3$. The associated isogenous curves are

$$\begin{aligned} \mathcal{E}_{1,-3} &: y^2 = x^3 - 7375x^2 - 2610750000x \\ &\qquad + 68994507812500, \\ \mathcal{E}^*_{1,-3} &: y^2 = x^3 - 7375x^2 - 11313250000x \\ &\qquad - 5450566117187500 \end{aligned}$$

with j-invariants $-\frac{5\cdot 29^3}{2^5}, -\frac{5^2}{2}$ respectively. Their Mordell–Weil groups are

$$\begin{aligned} \mathcal{E}_{1,-3}(\mathbf{Q}) &= \langle P_1, P_2\rangle \simeq \mathbf{Z}^{\oplus 2}, \\ \mathcal{E}^*_{1,-3}(\mathbf{Q}) &= \langle Q_1, Q_2\rangle \simeq \mathbf{Z}^{\oplus 2} \end{aligned}$$

where

$$\begin{aligned} P_1 &= (-53100, 6091750), \\ P_2 &= (88500, 21756250), \\ Q_1 &= (678500, 543906250), \\ Q_2 &= (1452875, 1740500000). \end{aligned}$$

We see $P_2 = Q_0$ where $Q_0 = (4r(p^2+4)W, 2(p^2+4)W^2)$ which corresponds to $\mathrm{Lec}(1,-3;X)$. The isogeny $\nu^* : \mathcal{E}^*_{1,-3} \to \mathcal{E}_{1,-3}$ is given by

$$\begin{aligned} \nu^*(Q_1) &= P_1 - 2P_2, \\ \nu^*(Q_2) &= -P_1 - 3P_2. \end{aligned}$$

Hence the image of ν^* is given by

$$\nu^*(\mathcal{E}^*_{1,-3}) = \langle P_1 - 2P_2, 5P_2\rangle.$$

We conclude that $\mathcal{E}_{1,-3}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{1,-3}(\mathbf{Q})) = \langle \overline{P_2}\rangle \simeq \mathbf{Z}/5\mathbf{Z}$. Thus there exists exactly one isomorphism class of Lecachux's polynomials. We have

$$\begin{aligned} \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(1,-3;X)) &= \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}([n]P_2;X)) \\ &= \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(1, \tfrac{x([n]P_2)}{4(p^2+4)W}; X)) \end{aligned}$$

where $\gcd(n,5) = 1$. For example, for $n = 1, 2, 3, 4$, we have

$$\frac{x([n]P_2)}{4(p^2+4)W} = -3, \frac{-263}{236}, \frac{4849}{39605}, \frac{2034016227}{1036798976}$$

respectively. We can check this example by Sage [9] as in the arXiv version of this paper [1, Example 4.1].

Example 4.2 ($p = 2$ and $r = -15$ with $\mathcal{E}_{2,-15}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{2,-15}(\mathbf{Q})) \simeq (\mathbf{Z}/5\mathbf{Z})^{\oplus 2}$)**.** We consider the case where $p = 2$, $r = -15$. The associated isogenous curves are

$$\begin{aligned} \mathcal{E}_{2,-15} &: y^2 = x^3 - 3362328x^2 - 446557358393568x \\ &\qquad + 4390381057572915584256, \\ \mathcal{E}^*_{2,-15} &: y^2 = x^3 - 3362328x^2 + 1181398581066528x \\ &\qquad - 2432955321125146856888576 \end{aligned}$$

with j-invariants $-\frac{2^6\cdot 239^3}{3^{10}}, \frac{2^6}{3^2}$ respectively. Their Mordell–Weil groups are

$$\begin{aligned} \mathcal{E}_{2,-15}(\mathbf{Q}) &= \langle P_{\mathrm{tor}}\rangle \oplus \langle P_1, P_2, P_3\rangle \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}^{\oplus 3}, \\ \mathcal{E}^*_{2,-15}(\mathbf{Q}) &= \langle Q_{\mathrm{tor}}\rangle \oplus \langle Q_1, Q_2, Q_3\rangle \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}^{\oplus 3} \end{aligned}$$

where

$$\begin{aligned} P_{\mathrm{tor}} &= (-23536296, 0), \\ P_1 &= (\tfrac{1213850592}{121}, \tfrac{32104365187824}{1331}), \\ P_2 &= (12954852, 14669441496), \\ P_3 &= (24185016, 75959770464), \\ Q_{\mathrm{tor}} &= (57159576, 0), \\ Q_1 &= (\tfrac{9662338144}{169}, \tfrac{26786536642000}{2197}), \\ Q_2 &= (58184676, 105083001000), \\ Q_3 &= (\tfrac{15400097496}{121}, \tfrac{1841522732064000}{1331}). \end{aligned}$$

The isogeny $\nu^* : \mathcal{E}^*_{2,-15} \to \mathcal{E}_{2,-15}$ is given by

$$\begin{aligned} \nu^*(Q_{\mathrm{tor}}) &= P_{\mathrm{tor}}, \\ \nu^*(Q_1) &= -P_1 + 2P_2 + 2P_3, \\ \nu^*(Q_2) &= P_{\mathrm{tor}} - 2P_1 - P_2 - P_3, \\ \nu^*(Q_3) &= -2P_1 + 4P_2 - P_3. \end{aligned}$$

Hence we obtain the image

$$\nu^*(\mathcal{E}^*_{2,-15}) = \langle P_{\mathrm{tor}}, P_1 + 2P_2 + 2P_3, 5P_2, 5P_3 \rangle$$

and conclude that $\mathcal{E}_{2,-15}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{2,-15}(\mathbf{Q})) = \langle \overline{P_2}, \overline{P_3} \rangle \simeq (\mathbf{Z}/5\mathbf{Z})^{\oplus 2}$. There exist 6 subgroups of order 5 in $\mathcal{E}_{2,-15}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{2,-15}(\mathbf{Q})) \simeq (\mathbf{Z}/5\mathbf{Z})^{\oplus 2}$ which correspond to the 6 isomorphism classes

$$\begin{aligned}
\mathrm{Lec}(P_2 - 2P_3; X) &= \mathrm{Lec}(2, -\tfrac{6826408529368884683}{114084259282587016}; X),\\
\mathrm{Lec}(P_2 - P_3; X) &= \mathrm{Lec}(2, -\tfrac{5293745}{2271049}; X),\\
\mathrm{Lec}(P_2; X) &= \mathrm{Lec}(2, -\tfrac{131}{136}; X),\\
\mathrm{Lec}(P_2 + P_3; X) &= \mathrm{Lec}(2, \tfrac{157}{529}; X),\\
\mathrm{Lec}(P_2 + 2P_3; X) &= \mathrm{Lec}(2, \tfrac{9701177386741}{7753965979144}; X),\\
\mathrm{Lec}(P_3; X) &= \mathrm{Lec}(2, -\tfrac{19759}{10988}; X),
\end{aligned}$$

with the quartic subfield

$$F = \mathbf{Q}\Big(\sqrt{-233495 - \tfrac{326893}{2}\sqrt{2}}\Big).$$

Since $\mathrm{Lec}(2, -15; X)$ corresponds to the point

$$\begin{aligned}
Q_0 &= (4r(p^2+4)W, 2(p^2+4)W^2)\\
&= (201739680, 2826312394896) = P_{\mathrm{tor}} - P_1 - P_3
\end{aligned}$$

and $\langle \overline{Q_0} \rangle = \langle \overline{P_2 - 2P_3} \rangle$ in $\mathcal{E}_{2,-15}(\mathbf{Q})/\nu^*(\mathcal{E}^*_{2,-15}(\mathbf{Q}))$,

$$\begin{aligned}
\mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(Q_0; X)) &= \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(2, -15; X))\\
&= \mathrm{Spl}_{\mathbf{Q}}(\mathrm{Lec}(P_2 - 2P_3; X)).
\end{aligned}$$

We can check this example by Sage [9] as in the arXiv version of this paper [1, Example 4.2].

Two examples of the degenerate cases $G_{p,r} \simeq D_5$ and C_5 where $G_{p,r} = \mathrm{Gal}(\mathrm{Lec}(p, r; X)/\mathbf{Q})$ are also given in [1, Section 5].

Acknowledgments. The authors thank the referee for helpful comments. This work was partially supported by JSPS KAKENHI Grant Number 19K03418.

References

[1] A. Hoshi and M. Koshiba, On Lecacheux's family of quintic polynomials, arXiv:2003.13458 (the arXiv version of this paper).

[2] A. Hoshi and K. Miyake, On the field intersection problem of solvable quintic generic polynomials, Int. J. Number Theory **6** (2010), no. 5, 1047–1081.

[3] D. Husemöller, *Elliptic curves*, 2nd ed., Graduate Texts in Mathematics, 111, Springer-Verlag, New York, 2004.

[4] C. U. Jensen, A. Ledet and N. Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications, 45, Cambridge University Press, Cambridge, 2002.

[5] M. Kida, On metacyclic extensions, J. Théor. Nombres Bordeaux **24** (2012), no. 2, 339–353.

[6] M. Kida, Y. Rikuna and A. Sato, Classifying Brumer's quintic polynomials by weak Mordell-Weil groups, Int. J. Number Theory **6** (2010), no. 3, 691–704.

[7] O. Lecacheux, Constructions de polynômes génériques à groupe de Galois résoluble, Acta Arith. **86** (1998), no. 3, 207–216.

[8] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106, Springer-Verlag, New York, 1986.

[9] W. A. Stein, *et al.*, Sage: Open Source Mathematical Software (Version 9.0), The Sage Group, http://www.sagemath.org, 2020.

[10] J. Vélu, Isogénies entre courbes elliptiques, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.