PRINCIPAL QUARTIC EXTENSIONS AND ELLIPTIC CURVES

Kevin Mugo

PRINCIPAL QUARTIC EXTENSIONS AND ELLIPTIC CURVES

KEVIN MUGO

150 N. University St. Department of Mathematics
Purdue University
W. Lafayette, IN 47905
U.S.A
kevin.mugo@gmail.com

Abstract. We associate to an S_4 extension, M/K, a Brauer-Severi variety, whose K-rational points correspond to quartic polynomials of the form $u^4 + Au + B$ with splitting field M. The condition that M/K is generated by such a polynomial is a necessary and sufficient condition for $M \subseteq K(E[4])$ for some elliptic curve E/K. We point out a flaw in the related work of Holden, provide numerical examples, and describe a family of elliptic curves with the same mod 4 representation.

1. Introduction

1.1. **Notation.** Let K be a number field, and fix an extension M/K with $\mathrm{Gal}(M/K) \cong S_4$. Choose L/K such that $K \subseteq L \subseteq M$, $[L : K] = 4$, and the normal closure of L in $\overline{K}$ is M and let $\Delta_{L/K}$ denote the discriminant of L/K. The quartic extension L/K, can be realised as $K(\alpha)$, where α is a root of an irreducible quartic polynomial defined over K, whose splitting field is M.

A *principal*, quartic polynomial defined over K, is one of the form $u^4 + A\,u + B$ with $A, B \in K$ and $AB \neq 0$. If $L = K(\alpha)$ where α is a root of a principal quartic polynomial, we say L/K is a principal, quartic extension.

For $a, b \in K^\times$, let (a, b) denote the quaternion algebra on two generators i, j with defining relations

$$i^2 = a, \quad j^2 = b, \quad ij = -ji$$

We identify (a, b) with its equivalence class in $\mathrm{Br}_2(K)$, the 2-part of the Brauer group of K (See [6, Ch.3] for the definition of the Brauer group).

1.2. **Overview.** In section 2, we give a criterion for determining when M/K is generated by a principal quartic. In section 3, we apply this criterion to the problem of deciding when an S_4 extension is contained in the 4-torsion point field of an elliptic curve.

2010 *Mathematics Subject Classification.* 11D09; 11D25.
Key words and phrases. Elliptic Curves; 4-torsion; quartic polynomials.

2. A Brauer-Severi Variety

We show that each principal, quartic, extension L/K, with normal closure M/K, corresponds to a K-rational point on a variety.

Proposition 2.1. *The following are equivalent:*

1. *M is a splitting field of a principal quartic, $p(u) := u^4 + Au + B \in K[u]$.*
2. *M is a splitting field of $q(x) := x^4 - s_1x^3 + s_2x^2 - s_3x + s_4 \in K[x]$, with roots $\{x_1, x_2, x_3, x_4\}$ and the following variety has a K-rational point.*

$$\Gamma_{q(x)} = \left\{ (a:b:c:d) \in \mathbb{P}^3 \;\middle|\; \begin{array}{l} \sum_{i=1}^{4}(a + bx_i + cx_i^2 + dx_i^3) = 0 \\ \sum_{i=1}^{4}(a + bx_i + cx_i^2 + dx_i^3)^2 = 0 \end{array} \right\}$$

Proof. (1) $\Longrightarrow$ (2)
Let M be the splitting field of $r(u) = u^4 + Au + B$ with roots $\{u_1, u_2, u_3, u_4\}$, then $(0:1:0:0) \in \Gamma_{p(u)}(K)$.

(2) $\Longrightarrow$ (1)
Let $(a:b:c:d) \in \Gamma_{q(x)}(K)$ and set $u_i = a + bx_i + cx_i^2 + dx_i^3$. Consider $p(u) = \prod_{i=1}^{4}(u - u_i)$. The coefficients of $p(u)$ can be expressed solely in terms of the K-rational coefficients: $a, b, c, d, s_1, s_2, s_3, s_4$. Moreover, the respective coefficients of the cubic and quadratic terms are:

$$\sum_{i=1}^{4} u_i \quad \text{and} \quad \frac{(\sum_{i=1}^{4} u_i)^2 - \sum_{i=1}^{4} u_i^2}{2}$$

both of which are zero by assumption. It follows that $r(u)$ is of the form $u^4 + Au + B \in K[u]$.

It remains to show that M is the splitting field of $p(u)$. For each i, $K(u_i) \subseteq K(x_i)$ and in fact, we will show an equality of fields $K(x_i) = K(u_i)$. Observe that

$$S_3 \cong \mathrm{Gal}(M/K(x_i)) \subseteq \mathrm{Gal}(M/K(u_i)) \subseteq \mathrm{Gal}(M/K) \cong S_4$$

so that $[K(x_i) : K(u_i)] = 1, 2$ or 4.

If $[K(x_i) : K(u_i)] = 4$ then $u_i \in K$. Hence $b = c = d = 0$ and $u_i = a$. Since $\sum_{i=1}^{4} u_i = 0$ then $a = 0$ as well but $(a:b:c:d) = (0:0:0:0)$ is not a projective point.

If $[K(x_i) : K(u_i)] = 2$ then $\mathrm{Gal}(M/K(u_i))$ is a subgroup of S_4, of index 2, containing a subgroup isomorphic to S_3, but this is impossible. We conclude that $K(x_i) = K(u_i)$ and that M is a splitting field of $p(u)$. □

Example 2.1. (1) Let $L = \mathbb{Q}(\alpha)$ where α is a root of $q(x) = x^4 - x^3 + 2x^2 + x - 1$, and M is the splitting field of $q(x)$.
$(0:2:-2:1) \in \Gamma_{q(x)}(\mathbb{Q})$ corresponds to the quartic $p(u) := u^4 + 60u + 52$ which generates $M/\mathbb{Q}$ and therefore $L = \mathbb{Q}(\beta)$, for some root β of $p(u)$. The extension $L/\mathbb{Q}$ is therefore principal over $\mathbb{Q}$.

(2) Let $M/\mathbb{Q}$ be the splitting field of $q(x) = x^4 - x^3 + 2x^2 - 1$. $\Gamma_{q(x)}(\mathbb{Q}) = \emptyset$ and therefore any quartic extension $L \subseteq M$, will not be principal.

With the exception of certain degenerate cases, the variety $\Gamma_{q(x)}$, is birationally equivalent to a conic, and is therefore a Brauer-Severi variety.

Corollary 2.1. *Let M be the splitting field of $q(x) = x^4 - s_1x^3 + s_2x^2 - s_3x + s_4 \in K[x]$, with roots $\{x_1, x_2, x_3, x_4\}$ and define*

$$A(q) = 3s_1^2 - 8s_2$$
$$B(q) = -6s_3s_1^3 + 2s_2^2s_1^2 - 12s_4s_1^2 + 28s_2s_3s_1 - 8s_2^3 - 36s_3^2 + 32s_2s_4.$$

(1) *If $A(q) \cdot B(q) = 0$, $\Gamma_{q(x)}$ has a K-rational point.*
(2) *If $A(q) \cdot B(q) \neq 0$,*

$$\Gamma_{q(x)} \simeq \left\{ (X : Y : Z) \in \mathbb{P}^2 \;\middle|\; A(q)\, X^2 + B(q)\, Y^2 + C(q)\, Z^2 = 0 \right\}$$

Proof. Let $\sigma_n = \sum_{j=1}^{4} x_j^n$ denote the n-th power sum.

(1) If $A(q) = 0$,

$$(\sigma_1 : -\sigma_0 : 0 : 0) \in \Gamma_{q(x)}(K).$$

If $B(q) = 0$ and $A(q) \neq 0$,

$$\left(\begin{vmatrix} \sigma_1 & \sigma_2 \\ \sigma_2 & \sigma_3 \end{vmatrix} : - \begin{vmatrix} \sigma_0 & \sigma_2 \\ \sigma_1 & \sigma_3 \end{vmatrix} : \begin{vmatrix} \sigma_0 & \sigma_1 \\ \sigma_1 & \sigma_2 \end{vmatrix} : 0 \right) \in \Gamma_q(K).$$

(2) Make the following definitions:

$$D(q) = \frac{\begin{vmatrix} \sigma_0 & \sigma_2 \\ \sigma_1 & \sigma_3 \end{vmatrix}}{A(q)}, \qquad E(q) = \frac{\begin{vmatrix} \sigma_0 & \sigma_3 \\ \sigma_1 & \sigma_4 \end{vmatrix}}{A(q)},$$

$$F(q) = \frac{\begin{vmatrix} \sigma_0 & \sigma_1 & \sigma_3 \\ \sigma_1 & \sigma_2 & \sigma_4 \\ \sigma_2 & \sigma_3 & \sigma_5 \end{vmatrix}}{B(q)}, \qquad C(q) = \frac{\begin{vmatrix} \sigma_0 & \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_1 & \sigma_2 & \sigma_3 & \sigma_4 \\ \sigma_2 & \sigma_3 & \sigma_4 & \sigma_5 \\ \sigma_3 & \sigma_4 & \sigma_5 & \sigma_6 \end{vmatrix}}{A(q) \cdot B(q)}.$$

Under the linear change of variables

$$\begin{bmatrix} W \\ X \\ Y \\ Z \end{bmatrix} = \begin{bmatrix} 1 & \sigma_1/\sigma_0 & \sigma_2/\sigma_0 & \sigma_3/\sigma_0 \\ & 1 & D(q) & E(q) \\ & & 1 & F(q) \\ & & & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix}$$

we have the following identities:

$$\sum_{i=1}^{4}\left(a+b\,x_i+c\,x_i^2+d\,x_i^3\right)=\begin{bmatrix}\sigma_0\\ \sigma_1\\ \sigma_2\\ \sigma_3\end{bmatrix}^T\begin{bmatrix}a\\ b\\ c\\ d\end{bmatrix}=\sqrt{\sigma_0}\,W=2\,W \tag{2.1}$$

$$\begin{aligned}\sum_{i=1}^{4}\left(a+b\,x_i+c\,x_i^2+d\,x_i^3\right)^2&=\begin{bmatrix}a\\ b\\ c\\ d\end{bmatrix}^T\begin{bmatrix}\sigma_0&\sigma_1&\sigma_2&\sigma_3\\ \sigma_1&\sigma_2&\sigma_3&\sigma_4\\ \sigma_2&\sigma_3&\sigma_4&\sigma_5\\ \sigma_3&\sigma_4&\sigma_5&\sigma_6\end{bmatrix}\begin{bmatrix}a\\ b\\ c\\ d\end{bmatrix}\\ &=\sigma_0\,W^2+A(q)\,X^2+B(q)\,Y^2+C(q)\,Z^2\end{aligned} \tag{2.2}$$

Setting both (2.1) and (2.2) equal to zero yields,

$$\Gamma_{q(x)}\simeq\left\{(X:Y:Z)\in\mathbb{P}^2\;\middle|\;A(q)\,X^2+B(q)\,Y^2+C(q)\,Z^2=0\right\}$$

□

Remark 2.1. By definition $A(q)\cdot B(q)\cdot C(q)$ equals the discriminant of $q(x)$, and therefore

$$A(q)\cdot B(q)\cdot C(q)\equiv\Delta_{L/K}\bmod(K^\times)^2$$

Proposition 2.2. *Let M/K be an S_4 extension, the normal closure of a quartic extension L/K. Choose $q(x)=x^4-s_1x^3+s_2x^2-s_3x+s_4\in K[x]$ to be any polynomial that generates M/K and form the coefficients:*

$$\begin{aligned}A(q)&=3s_1^2-8s_2\\ B(q)&=-6s_3s_1^3+2s_2^2s_1^2-12s_4s_1^2+28s_2s_3s_1-8s_2^3-36s_3^2+32s_2s_4\end{aligned}$$

If $A(q)\cdot B(q)\neq 0$, then M/K is a principal extension if and only if the class of $(-\Delta_{L/K}B(q),-A(q)B(q))$ is trivial in $Br_2(K)$.

Proof. If $A(q).B(q)\neq 0$ then by Corollary 2.1

$$\Gamma_{q(x)}\simeq\left\{(X:Y:Z)\in\mathbb{P}^2\;\middle|\;A(q)\,X^2+B(q)\,Y^2+C(q)\,Z^2=0\right\}$$

M/K is principal iff the quadratic form $Q:=A(q)X^2+B(q)Y^2+C(q)Z^2$ represents 0.

By definition, the Hasse invariant of Q, $\omega(Q)$, is the class of

$$(A(q),B(q))\otimes(A(q),C(q))\otimes(B(q),C(q))$$

in $\mathrm{Br}_2(K)$.
For ease of notation, let A,B,C denote $A(q),B(q),C(q)$ respectively. Recall by Remark 2.1, $ABC=\mathrm{disc}(q(x))\equiv\Delta_{L/K}\bmod(K^\times)^2$. Using the linearity condition

$$(a,b)\otimes(a,c)=(a,bc).$$

and the identities

$$(a,-a)=(a,1)=(a,1-a)=1$$

in $\mathrm{Br}_2(K)$, we obtain:

$$\begin{aligned}
\omega(Q) &= (A,B)\otimes(A,C)\otimes(B,C)\\
&= (A,-AB)\otimes(AB,C)\\
&= (-\Delta_{L/K},-AB)\otimes(A,-AB)\otimes(AB,C)\otimes(AB,-AB)\otimes(-\Delta_{L/K},-AB)\\
&= (-\Delta_{L/K}A,-AB)\otimes(AB,-ABC)\otimes(-\Delta_{L/K},-AB)\\
&= (-BC,-AB)\otimes(AB,-\Delta_{L/K})\otimes(-\Delta_{L/K},-AB)\\
&= (-BC,-AB)\otimes(-1,-\Delta_{L/K})\\
&= (-BC,-AB)\otimes(AB,-AB)\otimes(-1,-\Delta_{L/K})\\
&= (-\Delta_{L/K}B,-AB)\otimes(-1,-\Delta_{L/K})
\end{aligned}$$

The quadratic ternary form, Q, has a non-trivial zero when $\omega(Q)=(-1,-ABC)$ (See [5, p. 121]). Hence Q has a non-trivial zero if and only if

$$(-\Delta_{L/K}B(q),-A(q)B(q))=1.$$

□

Remark 2.2. It is easily verified that $\omega(Q)$ is independent of the choice of $q(x)$, but rather depends solely on L/K. That is, if $L=K(\alpha)=K(\beta)$, and α,β are roots of $q(x),q'(x)$, respectively, with associated quadratic forms Q,Q', then $\omega(Q)=\omega(Q')$. Notationally we write ω in place of $\omega(Q)$.

In the proof of Proposition 2.2 we have established:

Corollary 2.2. *Let L/K be a quartic extension. L/K is a principal quartic extension if and only if $\omega\otimes(-1,-\Delta_{L/K})=1$.*

3. Application to Elliptic Curves

The connection between elliptic curves and principal quartic extensions, stems from the following result that we establish in [7, Corollary 4] (Cf. [1, Equation 6.6]).

Theorem 3.1. *Let E/K be an elliptic curve with invariant $j_0\neq 0,1728$. The unique S_4 field extension $M\subseteq K(E[4])$ is the splitting field of the quartic polynomial $p(u):=u^4+\dfrac{32}{j_0}u+\dfrac{4}{j_0}$.*

Therefore if $M\subseteq K(E[4])$, M/K is generated by a principal quartic. The converse also holds:

Corollary 3.1. *$M\subseteq K(E[4])$ if and only if M/K is the splitting field of a principal quartic polynomial $p(u)\in K[u]$.*

Proof. For the sufficiency, let M/K, be the splitting field of u^4+Au+B with roots u_1,u_2,u_3,u_4. Note that $AB\neq 0$, since M/K is an S_4 extension. M/K is the splitting field of

$$p(u)=\prod_{i=1}^{4}\left(u-\frac{Au_i}{8B}\right)=u^4+\frac{32}{j_0}u+\frac{4}{j_0}$$

where $j_0 = \frac{2^{14}B^3}{A^4}$. Furthermore $j_0 \neq 1728$, since the discriminant of $p(u)$ is non-zero. The elliptic curve

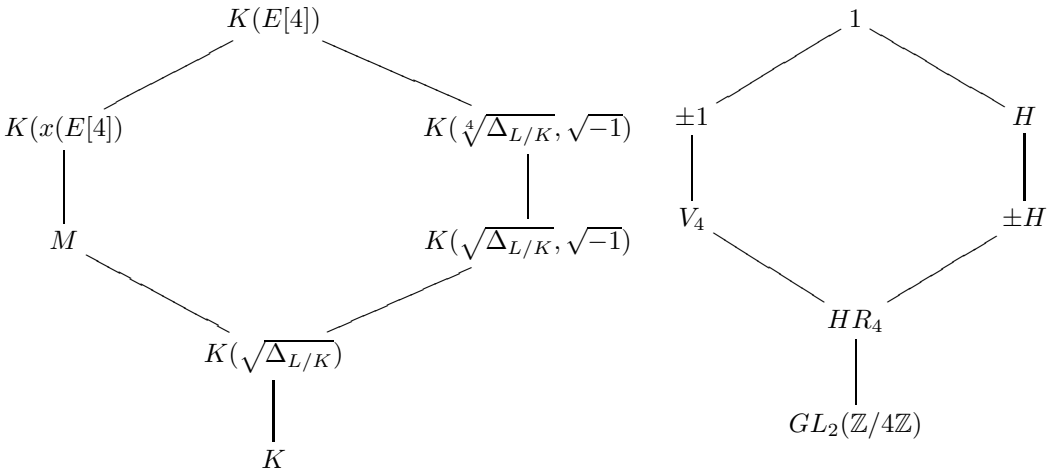
$$E : y^2 = x^3 + \frac{3j_0}{1728 - j_0}x + \frac{2j_0}{1728 - j_0}$$

has invariant j_0 and therefore $M \subseteq K(E[4])$. □

In Corollary 2.2, we saw that L/K is principal if $\omega \otimes (-1, -\Delta_{L/K})$ is trivial. If $L \subseteq M \subseteq K(E[4])$, we have the following stronger result:

Theorem 3.2. *Let $M \subseteq K(E[4])$. If $Gal(K(E[4])/K) \cong GL_2(\mathbb{Z}/4\mathbb{Z})$ then $\omega = (-1, -\Delta_{L/K}) = 1$.*

Proof. We have the following lattice of fixed subfields of $K(E[4])$ and their corresponding Galois groups (See [1, 5.5] for the definition of the groups H and R_4).



The Brauer classes ω and $(-1, -\Delta_{L/K})$ can be interpreted as obstructions to the following embedding problems.

- The obstruction to the embedding problem:

  $$1 \longrightarrow \mu_2 \longrightarrow D_4 \longrightarrow \mathrm{Gal}(K(\sqrt{\Delta_{L/K}}, \sqrt{-1}) \cong V_4 \longrightarrow 1$$

  is $(-1, -\Delta_{L/K})$. (See ([3, Prop. 3.10]).
  The field extension $K(\sqrt[4]{\Delta_{L/K}}, \sqrt{-1})/K$ with Galois group D_4, is a solution to this embedding problem and thus $(-1, -\Delta_{L/K}) = 1$.
- The obstruction to the embedding problem:

  $$1 \longrightarrow \mu_2 \longrightarrow 2 \cdot A_4 \longrightarrow \mathrm{Gal}(M/K(\sqrt{\Delta_{L/K}})) \cong A_4 \longrightarrow 1$$

  is ω. (See ([2]). Here $2 \cdot A_4$ denotes the double cover of A_4.
  The field extension $K(x(E[4])/K(\sqrt{\Delta_{L/K}})$ with Galois group $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}) \cong 2 \cdot A_4$ is a solution to this embedding problem and thus $\omega = 1$.

□

3.1. **Elliptic Curves Arising from Mod 4 Representations.** In [4], Holden states a criterion for determining when $M \subseteq K(E[4])$ for some elliptic curve E/K. Unfortunately, the main result is incorrect as stated. In particular Theorem 6, where it is stated that two quartics generate the same extension M/K if and only if both quartics have the same invariant I and the same invariant J, is false. Indeed two distinct quartics may generate the same S_4 extension, M/K, despite having different invariants I and J.

For instance, Holden asserts that the splitting field $M/\mathbb{Q}$ for $q(x) := x^4 - x^3 + x^2 + x - 1$ is not contained in the field $\mathbb{Q}(E[4])$ for any $E/\mathbb{Q}$. However, this is definitely incorrect. Using the substitution

$$x \to u := -2 + 3x - x^2 + 2x^3,$$

we find the principal quartic $u^4 + 103u - 109$ generates M. By Corollary 3.1, M is contained in $\mathbb{Q}(E[4])$ for the elliptic curve $E : y^2 = x^3 - 432948x - 349609151$.

In Table 3.1, we list 12 S_4 extensions, $M/\mathbb{Q}$, which Holden in [4], claims do not come from elliptic curves. We find that 7 of the 12 examples do come from elliptic curves. The first and second columns, list the discriminant of the polynomial, and the generating polynomial of the $M/\mathbb{Q}$ extension. The third column gives a principal quartic generating the same S_4 extension. The fourth column gives the minimal model of the corresponding elliptic curve $E/\mathbb{Q}$, where $[a, b]$ are coefficients of the Weierstrass equation $y^2 = x^3 + ax + b$.

TABLE 1. Examples of Principal and Non-Principal S_4 Extensions

$\Delta_{L/\mathbb{Q}}$	$q(x)$	$p(u)$	$E/\mathbb{Q}$
257	$x^4 + x^2 - x + 1$	None	
-331	$x^4 - x^3 + x^2 + x - 1$	$u^4 + 103u - 109$	[-432948, -349609151]
-491	$x^4 - x^3 - x^2 + 3x - 1$	$u^4 + 29u - 47$	[-276924, -73529705]
592	$x^4 + 2x^2 - 2x + 1$	$u^4 - 4u + 4$	[-444, -2738]
697	$x^4 - x^3 + 2x^2 - x + 2$	None	
-731	$x^4 - x^3 + 2x^2 - 1$	None	
761	$x^4 - x^3 + x^2 + 2x + 1$	None	
788	$x^4 - x^3 + 2x^2 - 2x + 2$	$u^4 - 5344u + 88064$	[-3252864, -2111131982]
-848	$x^4 - x^2 - 2x + 1$	$u^4 - 16u + 19$	[3021, 5618]
892	$x^4 - x^3 - x^2 + 2$	$u^4 - 8u + 79$	[-52851, -4674526]
-976	$x^4 - 2x^3 + 3x^2 - 1$	$u^4 + 864u - 1053$	[-2379, -320006]
985	$x^4 - x^3 + 2x^2 - 3x + 2$	None	

It is natural to ask what proportion of S_4 extensions, are contained in the 4-torsion point field of an elliptic curve. Determining the asymptotic density of these octahedral field extensions is still an open question, but using an extensive database of quartic polynomials found at the website

`ftp://megrez.math.u-bordeaux.fr/pub/numberfields/`

we plotted the function

$$\pi(T) = \frac{\#\left\{M/K \,\middle|\, \mathrm{Gal}(M/K) \simeq S_4, L/K \text{ is principal, } \left|\Delta_{L/K}\right| \leqslant T\right\}}{\#\left\{M/K \,\middle|\, \mathrm{Gal}(M/K) \simeq S_4, \ \left|\Delta_{L/K}\right| \leqslant T\right\}}$$

for $0 < T \leqslant 10^7$ and for $K = \mathbb{Q}$ and obtained Figure 1.

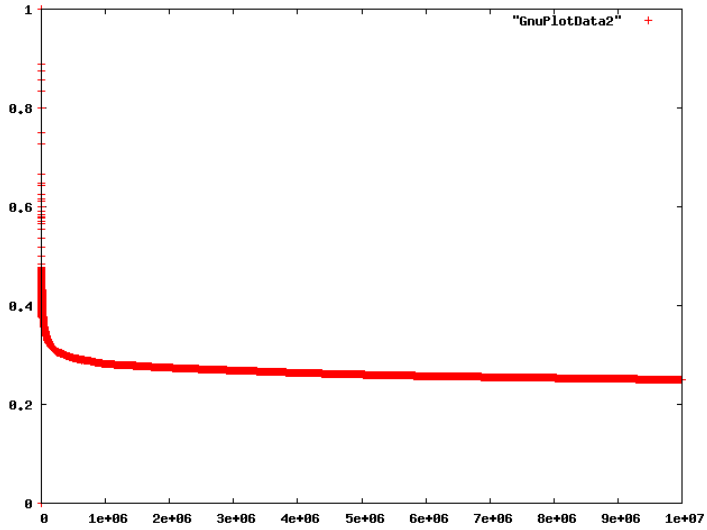


FIGURE 1. Plot of $\pi(T)$

3.2. **A Family of Elliptic Curves With the Same Mod 4 Representation.** Let E/K be an elliptic curve. We would like to describe a family of elliptic curves

$$\{E_i/K \mid K(E[4]) = K(E_i[4])\}.$$

One sees from Figure 3, that $K(E[4]) = M\,K(\sqrt[4]{\Delta_{L/K}}, \sqrt{-1})$, so that $K(E[4])/K$ is completely determined by M/K. If $M \subseteq K(E_i[4])$ then $K(E_i[4]) = K(E[4])$.

Fix an elliptic curve $E_0 : y^2 = x^3 + \dfrac{3j_0}{1728 - j_0}x + \dfrac{2j_0}{1728 - j_0}$ defined over K, with $\mathrm{Gal}(K(E_0[4])/K) \cong \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and let M/K be the unique S_4 extension contained in $K(E_0[4])$. The invariant of E_0 is j_0 and therefore by Theorem 3.1, the principal quartic $p(u) := u^4 + \dfrac{32}{j_0}u + \dfrac{4}{j_0}$ generates M/K.

A K-rational point, Q, on $\Gamma_{p(u)}$ corresponds to a principal quartic

$$p_Q(u) := u^4 + A(Q)u + B(Q) \in K[u].$$

Set $j(Q) = \dfrac{2^{14}B(Q)^3}{A(Q)^4}$ and let

$$E_Q : y^2 = x^3 + \frac{3j(Q)}{1728 - j(Q)}x + \frac{2j(Q)}{1728 - j(Q)}$$

The elliptic curve, E_Q, is well defined, since the discriminant of $p_Q(u) \neq 0$ implies that $j(Q) \neq 1728$. The splitting field of $u^4 + \dfrac{32}{j(Q)}u + \dfrac{4}{j(Q}$ is contained in $K(E_Q[4])$. But as in the proof of Corollary 3.1, this splitting field is the same as that of $p_Q(u)$ and therefore equals M.

This establishes the following theorem:

Theorem 3.3. *Let $E_0 : y^2 = x^3 + \dfrac{3j_0}{1728 - j_0}x + \dfrac{2j_0}{1728 - j_0}$ be an elliptic curve with $j_0 \in K$ and with $Gal(K(E_0[4])/K) \cong GL_2(\mathbb{Z}/4\mathbb{Z})$. Let $p(u) = u^4 + \dfrac{32}{j_0}u + \dfrac{4}{j_0}$ have roots $\{u_1, u_2, u_3, u_4\}$ and set*

$$\Gamma_{p(u)} = \left\{ (a:b:c:d) \in \mathbb{P}^3 \;\middle|\; \begin{array}{l} \displaystyle\sum_{i=1}^{4}(a + bu_i + cu_i^2 + du_i^3) = 0 \\ \displaystyle\sum_{i=1}^{4}(a + bu_i + cu_i^2 + du_i^3)^2 = 0 \end{array} \right\}$$

Define the K-rational function

$$\begin{array}{lcl} j : \Gamma_{p(u)}(K) & \longrightarrow & \mathbb{P}_1 \\ Q = (a:b:c:d) & \mapsto & j(Q) = \dfrac{-12^4 \left[\displaystyle\sum_{i=1}^{4}\left(a + b\,u_i + c\,u_i^2 + d\,u_i^3\right)^4\right]^3}{\left[\displaystyle\sum_{i=1}^{4}\left(a + b\,u_i + c\,u_i^2 + d\,u_i^3\right)^3\right]^4} \end{array}$$

Then the elliptic curve

$$E_Q : y^2 = x^3 + \frac{3j(Q)}{1728 - j(Q)}x + \frac{2j(Q)}{1728 - j(Q)}$$

is well defined and $E_Q[4] \cong E_0[4]$ as $Gal(\overline{K}/K)$ modules.

References

1. C. Adelmann, *The Decomposition of Primes in Torsion Point Fields*, Springer-Verlag, 2001.
2. T. Crespo, *Explicit Construction of $\tilde{A}_n$ Type Fields*, J. Algebra **127** (1989), 452-461.
3. H. G. Grundman & T. L. Smith, *Automatic Realizability of Galois groups of order 16*, Expo. Math. **13** (1995), 289-319.
4. Christopher Holden, *Mod 4 Galois Representations and Elliptic Curves.* Proceedings of the American Mathematical Society, 136:31-39, 2008.
5. T.Y. Lam, *Introduction to Quadratic Forms over Fields*, Graduate Studies in Mathematics, Volume **67** American Mathematical Society, 2005.
6. Arne Ledet, *Brauer Type Embedding Problems*, Fields Institute Monographs, American Mathematical Society.

7. Kevin Mugo, *A Generating Polynomial for the Octahedral Extension in the 4-torsion Point Field of an Elliptic Curve*
Preprint, HAL ID: hal-01378831, `https://hal.archives-ouvertes.fr/hal-01378831`