On Q-Derived Polynomials. Appendix.

E.V. Flynn, Mathematical Institute, University of Oxford

The following is an appendix to the article *On Q-Derived Polynomials.* All equation and reference numbering are as in that article, and so the following only makes sense if read in conjunction with the article! The purpose of this appendix is to finish off finding $\mathcal{C}_1(\mathbb{Q})$, where $\mathcal{C}_1$ is as in (1.3), that is: $\mathcal{C}_1 : Y^2 = (X^2+15)(X^2+45)(X^2+135)$.

We first, as in §2, consider any curve $\mathcal{C}$ of the form (repeating (2.1)):

$$\mathcal{C} : Y^2 = F(X) = (X^2-k)(X^2-rk)(X^2-r^2k),\ r,k \in \mathbb{Q},\ k \neq 0, r \neq 0, \pm 1, \qquad (A.1)$$

with Jacobian J. We shall, as usual, assume that k, rk and $-rk$ are nonsquares.

The map $(X,Y) \mapsto (-X,Y)$ is an involution on $\mathcal{C}$, and the function X^2 is invariant under this map. There are then maps $\theta_1 : (X,Y) \mapsto (X^2,Y)$ and $\theta_2 : (X,Y) \mapsto (1/X^2, Y/X^3)$ from $\mathcal{C}$ to the elliptic curves (repeating (2.2)):

$$\begin{aligned} \mathcal{E}^a &: y^2 = (x-k)(x-rk)(x-r^2k), \\ \mathcal{E}^b &: \underline{y}^2 = (-k\underline{x}+1)(-rk\underline{x}+1)(-r^2k\underline{x}+1), \end{aligned} \qquad (A.2)$$

respectively, generalising (1.4). As in [11], these induce the isogeny $\phi_1 = \theta_1^* + \theta_2^* : A_1 \to J$, where $A_1 = \mathcal{E}^a \times \mathcal{E}^b$. There is an injective homomorphism (a special case of [8]):

$$\begin{aligned} \mu_1 : J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big) &\longrightarrow \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2 \\ &: \{(X_1,Y_1),(X_2,Y_2)\} \\ &\mapsto [(X_1^2-k)(X_2^2-k), (X_1^2-rk)(X_2^2-rk), (X_1^2-r^2k)(X_2^2-r^2k)]. \end{aligned} \qquad (A.3)$$

In the definition of μ_1, we take $X_i - \alpha_\ell$ to be 1 when $(X_i,Y_i) = \infty^+$ or ∞^-, and take $X_i - \alpha_\ell$ to be $\prod_{j\neq\ell}(\alpha_j - \alpha_\ell)$ when $X_i = \alpha_\ell$, and $\alpha_1,\ldots,\alpha_6$ are the roots of $F(X)$. Note that the product of the above triple is always 1 in $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ so that any one entry is redundant. The following lemma (a special case of [11]) is immediate.

Lemma A.1. *Let $J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big) = \{B_1,\ldots B_m\}$ and let $\mu_1(B_i) = [a_i,b_i,c_i]$ for each i, where μ_1 is as defined in (A.3). Let $(X,Y) \in \mathcal{C}(\mathbb{Q})$. Then $\{(X,Y),\infty^+\} = B_i$ in $J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$ for some $i \in \{1,\ldots,m\}$ and there exist $v_a, v_b, v_c \in \mathbb{Q}$ such that*

$$\begin{aligned} \mathcal{E}_{i,a} &: v_a^2 = a_i(X^2-rk)(X^2-r^2k) \\ \mathcal{E}_{i,b} &: v_b^2 = b_i(X^2-k)(X^2-r^2k) \\ \mathcal{E}_{i,c} &: v_c^2 = c_i(X^2-k)(X^2-rk) \end{aligned} \qquad (A.4)$$

□

Lemma A.2. *Let $\mathcal{C}_1$ be the curve $Y^2 = (X^2+15)(X^2+45)(X^2+135)$ with Jacobian J, and A_1, ϕ_1, μ_1 be as in Lemma A.1, and $D_1, \ldots, D_8$ be aas in Lemma 3.1. Then $J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$ is given by: $D_1 = \mathcal{O}, D_5 = \{(3,432), \infty^+\}$, whose images under μ_1 are given by: $\mu_1(D_1) = [1,1,1]$ and $\mu_1(D_5) = [6,6,1]$.*

Proof. Recall from the proof of Lemma 3.1 that $D_2, D_3, D_5, \{\infty^+, \infty^-\}$ were shown to generate $J(\mathbb{Q})/2J(\mathbb{Q})$ and D_2, D_3, D_5 were shown to generate $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$, where A and ϕ are as in Lemma 2.1. Now note that $\{\infty^+, \infty^+\}$, as well as D_1, D_2, D_3, D_4, all map to $[1,1,1]$ under μ_1. This implies that $\phi_1(A_1(\mathbb{Q})) \subset \phi_2(A_2(\mathbb{Q}))$ and that $J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big) = \{D_1, D_5\}$. □

We are now in a position to apply Lemma A.1 and determine all of $\mathcal{C}_1(\mathbb{Q})$.

Lemma A.3. *Let $\mathcal{C}_1 : Y^2 = (X^2+15)(X^2+45)(X^2+135)$.*
Then $\mathcal{C}_1(\mathbb{Q}) = \{\infty^+, \infty^-, (\pm 3, \pm 432)\}$.

Proof. We can apply Lemmas 2.1 and A.1 with $r = 3, k = -15, \alpha = \sqrt{-15}$, $K = \mathbb{Q}(\alpha)$ and $[d_1, e_1], \ldots [d_8, e_8]$ as in (3.1). As in the proof of Lemma 3.2, let $(X,Y) \in \mathcal{C}_1(\mathbb{Q})$ and let $x = 2X/(X^2 - rk) \in \mathbb{Q}$. Then $\{(X,Y), \infty^+\} = D_i$ in $J(\mathbb{Q})/\phi\big(A(\mathbb{Q})\big)$ for some $i \in \{1, \ldots 8\}$. In the second part of the proof of Lemma 3.2, it was shown that, if $i = 5, 6, 7, 8$, then (X,Y) is one of: $\infty^+, \infty^-, (\pm 3, \pm 432)$. In the first part of the same proof, the cases $i = 1,2,3,4$ were dismissed by showing that (X,Y) would then not be in the image of the map $(X, Y_1, Y_2, Y_3) \mapsto (X, Y_1 Y_2 Y_3/6)$ from $\mathcal{F}_1(\mathbb{Q})$ to $\mathcal{C}(\mathbb{Q})$. This was sufficient in that proof, since Lemma 3.2 was only required to find all members of $\mathcal{C}_1(\mathbb{Q})$ in the image of this map. To complete the proof of Lemma A.3 it is sufficient to show that the cases $i = 1,2,3,4$ do not give rise to any new members of $\mathcal{C}(\mathbb{Q})$.

First note that, if $i = 1,2,3,4$ then, by Lemma A.2, $\{(X,Y), \infty^+\} = D_1$ in $J(\mathbb{Q})/\phi_1\big(A_1(\mathbb{Q})\big)$ and specialising $\mathcal{E}_{i,a}$ of Lemma A.1 gives that X must satisfy: $v_a^2 = (X^2+45)(X^2+135)$ for some $v_a \in \mathbb{Q}$. This is an elliptic curve of rank 0 over $\mathbb{Q}$, with only ∞^+ and ∞^- as $\mathbb{Q}$-rational points. Hence the cases $i = 1,2,3,4$ give no further members of $\mathcal{C}_1(\mathbb{Q})$, as claimed. □

It is interesting to note, in the above proof, that covers from either ϕ or ϕ_1 separately are insufficient to find $\mathcal{C}_1(\mathbb{Q})$; we must use ϕ_1 for the cases $i = 1,2,3,4$ and ϕ for the cases $i = 5,6,7,8$.