European Journal of Mathematics (2023) 9:51
https://doi.org/10.1007/s40879-023-00643-y

RESEARCH ARTICLE

On 7-division fields of CM elliptic curves

Jessica Alessandrì[1] · Laura Paladino[2]

Received: 16 June 2022 / Revised: 26 October 2022 / Accepted: 8 March 2023

Abstract

Let $\mathcal{E}$ be a CM elliptic curve defined over a number field K, with Weiestrass form $y^3 = x^3 + bx$ or $y^2 = x^3 + c$. For every positive integer m, we denote by $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$ and by $K_m := K(\mathcal{E}[m])$ the m-th division field, i.e. the extension of K generated by the coordinates of the points in $\mathcal{E}[m]$. We classify all the fields K_7. In particular we give explicit generators for K_7/K and produce all the Galois groups $\mathrm{Gal}(K_7/K)$. We also show some applications to the Local–Global Divisibility Problem and to modular curves.

Keywords Elliptic curves · Complex multiplication · Torsion points

Mathematics Subject Classification 11G05 · 11F80

1 Introduction

Let K be a number field with algebraic closure $\overline{K}$ and let $\mathcal{E}$ be an elliptic curve defined over K. We keep the standard notation $\mathcal{E}[m]$ for the m-torsion subgroup of $\mathcal{E}$ and by K_m we denote the m-th division field $K(\mathcal{E}[m])$, i.e. the field obtained by adding to K the coordinates of the points in $\mathcal{E}[m]$. Since the beginning of the studies on elliptic curves, the m-th division fields have played a key rôle. The properties of K_m/K are related to Galois representations on the total Tate module, to Iwasawa theory, to modularity and to the proof of the Mordell–Weil theorem. The extension K_m/K is a Galois extension, in fact it is the splitting field of the m-th division polynomial, i.e. the polynomial

The authors are members of INdAM-GNSAGA.

✉ Laura Paladino
laura.paladino@unical.it

Jessica Alessandrì
jessica.alessandri@graduate.univaq.it

[1] Università degli Studi dell'Aquila, Via Vetoio, Coppito 1, 67100 Coppito, AQ, Italy

[2] Università della Calabria, Ponte Bucci, Cubo 30B, 87036 Rende, CS, Italy

Published online: 22 June 2023

whose roots are the abscissas of the m-torsion points of $\mathcal{E}$, and the polynomials whose roots are the ordinates corresponding to those abscissas. The extension K_m/K is monogeneous by Artin's primitive element theorem, however, in general it is not easy to find an explicit single generator. It is also well known that $\mathcal{E}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$. Therefore, if $\{P_1, P_2\}$ is a generating set for $\mathcal{E}[m]$, with $P_i = (x_i, y_i)$, for $i = 1, 2$, then $K_m = K(x_1, x_2, y_1, y_2)$ and $\{x_1, x_2, y_1, y_2\}$ is the generating set for $K(\mathcal{E}[m])$ that is usually adopted. We are interested in showing explicit generators for this extension, searching for generating sets as easy as possible to be used in applications. Indeed there are many potential applications, for instance in Galois representations (see for example [22]), local–global problems on elliptic curves (see Sect. 8.1), descent problems (see for example [1, 21] among others), points on modular curves and points on Shimura curves.

In the previous papers of this series [2, 3, 17], some of those applications have been shown, as well as some new generating sets involving a primitive m-th root of the unity ζ_m. In fact, by the properties of the Weil pairing e_m, the image $\zeta_m := e_m(P_1, P_2) \in K_m$ is a primitive m-th root of unity and $K(\zeta_m) \subseteq K_m$ (see for instance [24]). It turned out that ζ_m can be used as a generator for K_m/K and in particular, when m is odd, we have $K_m = K(x_1, \zeta_m, y_2)$ [3, Theorem 1.1]. When $m = p$ is a prime number, this generating set is minimal among the subsets of $\{x_1, x_2, \zeta_m, y_1, y_2\}$ (for further details see [3]). On the contrary, in the case when $m = p^n$, with $n \geqslant 2$, we can replace ζ_{p^n} with ζ_p, i.e. $K_{p^n} = K(x_1, \zeta_p, y_2)$, for every $n \geqslant 1$ (see [8, Theorem 1.1]).

Observe that when $K = \mathbb{Q}$, we have $\zeta_m \notin K$ and therefore $\mathbb{Q}(\mathcal{E}[m]) \neq \mathbb{Q}$, for every $m \geqslant 3$. In particular the extension $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is "as minimal as possible" when $\mathbb{Q}(\mathcal{E}[m]) = \mathbb{Q}(\zeta_m)$. Merel and Rebolledo proved that if such an equality holds when $m = p$ is a prime, then $p \leqslant 5$ (see [15, 20]). A classification of all elliptic curves such that $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ is given in [16] and a classification of all elliptic curves such that $\mathbb{Q}(\mathcal{E}[5]) = \mathbb{Q}(\zeta_5)$ is given in [12]. In this last paper González Jiménez and Lozano-Robledo also investigate the cases when $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is an abelian extension for all elliptic curves over number fields. Among other important results, in particular they prove that if $\mathcal{E}$ is a CM elliptic curve and $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is abelian, then $m \in \{2, 3, 4, 5, 6, 8\}$.

For $m = 3$ and $m = 4$, explicit descriptions of all possible fields K_3 and K_4 in terms of generators, degrees and Galois groups were given in [3] in 2016 (see also [2]). The generators of the fields K_8 were produced in 2017 in [27], in which the author also gives some information on the action of certain elements of $\mathrm{Gal}(K_8/K)$. In 2018 a complete description of the fields K_5 in terms of generators, degrees and Galois groups was produced in [17] for the families of CM elliptic curves $\mathcal{F}_1\colon y^2 = x^3 + bx$, with $b \in K$ and $\mathcal{F}_2\colon y^2 = x^3 + c$, with $c \in K$.

Here we give a classification of every possible field K_7, for the curves of the same families $\mathcal{F}_1$ and $\mathcal{F}_2$, showing in particular explicit generators for the extension K_7/K. We also show all possible Galois groups $\mathrm{Gal}(K_7/K)$ for the curves in $\mathcal{F}_1$ and $\mathcal{F}_2$.

The paper is structured as follows. In the first part of it we describe generators, possible degrees and possible Galois groups for the curves of the family $\mathcal{F}_1$. Then we give a similar description for the curves of the family $\mathcal{F}_2$. In the last part of the paper we show some applications of these results. In particular we produce an application to the Local–Global Divisibility Problem, which was stated in [9] by Dvornicich and Zannier in 2001 (see Sect. 8.1 for further details). In addition we deduce some properties concerning CM points on modular curves.

2 Generators of $K(\mathcal{E}[7])$ for elliptic curves $y^2 = x^3 + bx$

For every positive integer m, the m-th division polynomial of an elliptic curve $\mathcal{E}$ is the polynomial whose roots are the abscissas of the m-torsion points of $\mathcal{E}$. It is generally denoted by $\Psi_m(x)$. The polynomial Ψ_m has degree $\frac{m^2-1}{2}$ when m is odd and $\frac{m^2-4}{2}$ when m is even. Let $\mathcal{E}_1$ be an elliptic curve defined over K, with Weierstrass form $y^2 = x^3 + bx$. We will denote by ϕ_1 the complex multiplication of $\mathcal{E}_1$, i.e. $\phi_1((x, y)) = (-x, iy)$, for every point $P = (x, y) \in \mathcal{E}_1$. Since ϕ_1 is an automorphism of $\mathcal{E}_1$, we have that Ψ_m is a polynomial in x^2. When $m = 7$, the 7-th division polynomial of $\mathcal{E}_1$ is the polynomial

$$\begin{aligned} q_7(x) &:= 7x^{24} + 308bx^{22} - 2954b^2x^{20} - 19852b^3x^{18} - 35231b^4x^{16} \\ &\quad - 82264b^5x^{14} - 111916b^6x^{12} - 42168b^7x^{10} + 15673b^8x^8 \\ &\quad + 14756b^9x^6 + 1302b^{10}x^4 + 196b^{11}x^2 - b^{12}. \end{aligned}$$

We can set $t := x^2$ and consider the polynomial $q_7(t)$ of degree 12 to look for the abscissas of the 7-torsion points of $\mathcal{E}_1$. For every $\alpha \in K_7$, we denote by $\overline{\alpha}$ its complex conjugate. Let i be a root of $x^2 + 1 = 0$, let σ_1 be the automorphism of the extension $\mathbb{Q}(\zeta_7, i)/\mathbb{Q}$ mapping ζ_7 to ζ_7^5 and let

$$\begin{aligned} \omega_1 &:= (6i + 4)\zeta_7^5 + (6i - 2)\zeta_7^4 + (2i - 2)\zeta_7^3 + (2i + 4)\zeta_7^2 + 8i\zeta_7 + 4i - 3; \\ \omega_3 &:= \sigma_1(\omega_1) = (2i + 2)\zeta_7^5 + 6\zeta_7^4 + (-4i + 6)\zeta_7^3 + (-6i + 2)\zeta_7^2 - 4i\zeta_7 - 2i - 1; \\ \omega_5 &:= \sigma_1(\omega_3) = (4i - 6)\zeta_7^5 + (-2i - 4)\zeta_7^4 + (6i - 4)\zeta_7^3 - 6\zeta_7^2 + 4i\zeta_7 + 2i - 7; \\ \omega_{s+1} &:= \overline{\omega_s}, \quad \text{for } s \in \{1, 3, 5\}; \\ \theta_1 &:= \frac{1}{7}\big((-3520i - 1568)\zeta_7^5 + (-4800i + 2352)\zeta_7^4 + (-256i + 2352)\zeta_7^3 \\ &\qquad + (-1536i - 1568)\zeta_7^2 - 5056i\zeta_7 - 2528i + 3584\big); \\ \theta_3 &:= \sigma_1(\theta_1) = \frac{1}{7}\big((-256i - 2352)\zeta_7^5 + (1280i - 3920)\zeta_7^4 + (3264i - 3920)\zeta_7^3 \\ &\qquad + (4800i - 2352)\zeta_7^2 + 4544i\zeta_7 + 2272i + 1232\big); \\ \theta_5 &:= \sigma_1(\theta_3) = \frac{1}{7}\big((-3264i + 3920)\zeta_7^5 + (1536i + 1568)\zeta_7^4 + (-3520i + 1568)\zeta_7^3 \\ &\qquad + (1280i + 3920)\zeta_7^2 - 1984i\zeta_7 - 992i + 5152\big); \\ \theta_{s+1} &:= \overline{\theta_s}, \quad \text{for } s \in \{1, 3, 5\}. \end{aligned}$$

With the use of a software of computational algebra (we used AXIOM, that is also implemented in SAGE), one can verify that $q_7(t)$ factors over $K(i,\zeta_7)$ as follows:

$$q_7(t) := 7\prod_{j=1}^{6}\left(t-\left(\omega_j b+\frac{1}{2}b\sqrt{\theta_j}\right)\right)\left(t-\left(\omega_j b-\frac{1}{2}b\sqrt{\theta_j}\right)\right).$$

Thus the roots of $q_7(x)$, i.e. the abscissas of the 7-torsion points of $\mathcal{E}_1$, are

$$\begin{aligned} x_{2j-1} &= \sqrt{\omega_j b+\frac{1}{2}b\sqrt{\theta_j}}; & x_{2j} &= \sqrt{\omega_j b-\frac{1}{2}b\sqrt{\theta_j}};\\ -x_{2j-1} &= -\sqrt{\omega_j b+\frac{1}{2}b\sqrt{\theta_j}}; & -x_{2j} &= -\sqrt{\omega_j b-\frac{1}{2}b\sqrt{\theta_j}}; \end{aligned}$$

for $1\leqslant j\leqslant 6$. By using the equation $y^2=x^3+bx$, we can calculate the corresponding ordinates. For ease of notation, we will denote by iP the point $\phi_1(P)=(-x,iy)$, where $P=(x,y)\in\mathcal{E}_1$. It turns out that the 48 points of exact order 7 of $\mathcal{E}_1$ are the following:

$$\begin{aligned} \pm P_{2j-1} &:= (x_{2j-1},\pm y_{2j-1})\\ &= \left(\sqrt{\omega_j b+\frac{1}{2}b\sqrt{\theta_j}},\pm\sqrt{\left(\omega_j+\frac{1}{2}\sqrt{\theta_j}+1\right)b\sqrt{\omega_j b+\frac{1}{2}b\sqrt{\theta_j}}}\right);\\ \pm P_{2j} &:= (x_{2j},\pm y_{2j})\\ &= \left(\sqrt{\omega_j b-\frac{1}{2}b\sqrt{\theta_j}},\pm\sqrt{\left(\omega_j-\frac{1}{2}\sqrt{\theta_j}+1\right)b\sqrt{\omega_j b-\frac{1}{2}b\sqrt{\theta_j}}}\right);\\ \pm iP_{2j-1} &:= (-x_{2j-1},\pm iy_{2j-1}),\quad \pm iP_{2j} := (-x_{2j},\pm iy_{2j}); \end{aligned}$$

for $1\leqslant j\leqslant 6$.

Theorem 2.1 *Let θ_j and ω_j be as above, for $j=1,\ldots,6$, and let $\varepsilon\in\{+,-\}$ fixed. Then*

$$K_7=K(i,\zeta_7,y_j)=K\left(i,\zeta_7,\sqrt{\left(\omega_j+\varepsilon\frac{1}{2}\sqrt{\theta_j}+1\right)b\sqrt{\omega_j b+\varepsilon\frac{1}{2}b\sqrt{\theta_j}}}\right).$$

Proof If P is a nontrivial 7-torsion point, then iP is a 7-torsion point too. If iP is not a multiple of P, then a basis for $\mathcal{E}_1[7]$ is given by $\{P,iP\}$. Observe that $iP=nP$ if and only if $(i-n)P=O$. Since the ring of automorphisms of $\mathcal{E}_1$ is $\mathbb{Z}[i]$ and 7 is inert in $\mathbb{Z}[i]$, we see that iP is not a multiple of P, for every $P\in\mathcal{E}_1[7]$ of exact order 7, and we can choose $\{P_j,iP_j\}$ as a generating set of $\mathcal{E}_1[7]$, for any $j=1,\ldots,12$. We have $K_7=K(x_j,y_j,-x_j,iy_j)=K(x_j,y_j,i)$. On the other hand, by [3, Theorem 1.1], the field K_7 is equal to $K(x_j,\zeta_7,iy_j)$. Then in particular $K_7=K(x_j,i,\zeta_7,y_j)$. By calculating y_j^2 and y_j^4, one can verify that $\sqrt{\theta_j} \in K(i, \zeta_7, y_j^4)$. Thus $x_j \in K(i, \zeta_7, y_j)$ and we get the conclusion

$$K_7 = K(i, \zeta_7, y_j) = K\left(i, \zeta_7, \sqrt{\left(\omega_j + \varepsilon\,\frac{1}{2}\sqrt{\theta_j} + 1\right) b\sqrt{\omega_j b + \varepsilon\,\frac{1}{2} b\sqrt{\theta_j}}}\right),$$

for every $j = 1, \ldots, 6$ and $\varepsilon \in \{+, -\}$. □

3 Degrees $[K_7 : K]$ for the curves of $\mathcal{F}_1$

For ease of notation, from now on we will fix the generating set $\{P_1, iP_1\}$ for $\mathcal{E}_1[7]$. By Theorem 2.1 we have $K_7 = K\big(i, \zeta_7, \sqrt{\left(\omega_1 + \frac{1}{2}\sqrt{\theta_1} + 1\right) b\sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}}\big)$. As explained in the proof of Theorem 2.1, such a choice is without loss of generality and all the results that we are going to show about the degree $[K_7 : K]$ and the Galois group $\mathrm{Gal}(K_7/K)$ hold as well for every other generating set of the extension K_7/K listed in Theorem 2.1.

Theorem 3.1 *Let* $\mathcal{E}_1 : y^2 = x^3 + bx$, *with* $b \in K$. *Let*

$$y_1 = \sqrt{\left(\omega_1 + \frac{1}{2}\sqrt{\theta_1} + 1\right) b\sqrt{\omega_1 b + \frac{1}{2}\, b\sqrt{\theta_1}}}$$

and consider the conditions

A. $i \notin K$;

B1. $\zeta_7 + \zeta_7^{-1} \notin K(i)$;

B2. $\zeta_7 \notin K(i, \zeta_7 + \zeta_7^{-1})$;

C. $\sqrt{\theta_1} \notin K(i, \zeta_7)$;

D. $\sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}} \notin K(i, \zeta_7, \sqrt{\theta_1})$;

E. $y_1 \notin K\big(i, \zeta_7, \sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}\big)$.

The possible degrees of the extension K_7/K *are given in Table 1:*

Table 1 Degrees $[K(\mathcal{E}_1[7]) : K]$

d	Holding conditions	d	Holding conditions
96	**A**, **B1**, **B2**, **C**, **D**, **E**	8	**E** *and two of* **A**, **B2**, **C**, **D** *or* **A**, **B2** *and* **C**
48	**B1**, **E**, *and three of* **A**, **B2**, **C**, **D**	6	**B1** *and one of* **A**, **B2**, **C**, **E**
32	**A**, **B2**, **C**, **D**, **E**	4	*two of* **A**, **B2**, **C** *or* **E** *and one of* **A**, **B2**, **C**, **D**
24	**B1**, **E** *and two of* **A**, **B2**, **C**, **D** *or* **A**, **B1**, **B2** *and* **C**	3	**B1**
16	**E** *and three of* **A**, **B2**, **C**, **D**	2	*one of* **A**, **B2**, **C**, **E**
12	**B1**, **E** *and one of* **A**, **B2**, **C**, **D** *or* **B1** *and two of* **A**, **B2**, **C**	1	*no conditions hold*

Proof Consider the tower of extensions

$$\begin{aligned} &K \subseteq K(i) \subseteq K(i, \zeta_7 + \zeta_7^{-1}) \subseteq K(i, \zeta_7) \\ &\quad \subseteq K\big(i, \zeta_7, \sqrt{\theta_1}\big) \subseteq K\left(i, \zeta_7, \sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}\right) \subseteq K(i, \zeta_7, y_1). \end{aligned}$$

The degree $d := [K_7 : K]$ is the product of the degrees of the intermediate extensions appearing in the tower. Each extension gives a contribution to the degree less than or equal to 2, except for the extension $K(i) \subset K(i, \zeta_7 + \zeta_7^{-1})$ which gives a contribution dividing 3. With the use of the software of computational algebra AXIOM, we have verified that if K is linearly disjoint from $\mathbb{Q}(i, \zeta_7)$ over $\mathbb{Q}$, then θ_1 is not a square in $K(i, \zeta_7)$. A priori we can have all the possible combinations of the conditions **A**, **B1**, **B2**, **C**, **D** and **E**. However, some of the cases do not occur. The extensions $\mathbb{Q}(i)$ and $\mathbb{Q}(\zeta_7)$ are linearly disjoint over $\mathbb{Q}$, so condition **A** is independent of conditions **B1** and **B2** and the other way around. On the other hand, the extensions $\mathbb{Q}(i, \zeta_7, \sqrt{\theta_1})$, $\mathbb{Q}\big(i, \zeta_7, \sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}\big)$ and $\mathbb{Q}(i, \zeta_7, y_1)$ are not linearly disjoint over $\mathbb{Q}(i, \zeta_7)$. Then conditions **C**, **D** and **E** might be dependent on each other. Suppose that **E** does not hold. Then $y_1 \in K\big(i, \zeta_7, \sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}\big)$, i.e. $y_1 = \alpha + \beta\sqrt{\omega_1 b + \frac{1}{2} b\sqrt{\theta_1}}$, with $\alpha, \beta \in K(i, \zeta_7, \sqrt{\theta_1})$. By $y_1^2 = x_1^3 + bx_1$, we deduce

$$\begin{cases} 2\alpha\beta = b\omega_1 + b + \frac{b}{2}\sqrt{\theta_1} \\ \alpha^2 + \beta^2\Big(\omega_1 b + \frac{b}{2}\sqrt{\theta_1}\Big) = 0 \end{cases}$$

(recall that $b \neq 0$, otherwise the curve would be singular and we would not have an elliptic curve). Therefore

$$\begin{cases} \alpha = \dfrac{b\omega_1 + b + \frac{b}{2}\sqrt{\theta_1}}{2\beta} \\ \dfrac{b^2(\omega_1 + 1 + \frac{1}{2}\sqrt{\theta_1})^2 + 4\beta^4(\omega_1 b + \frac{b}{2}\sqrt{\theta_1})}{4\beta^2} = 0. \end{cases}$$

Hence $b^2\big(\omega_1 + 1 + \frac{1}{2}\sqrt{\theta_1}\big)^2 + 4\beta^4\big(\omega_1 b + \frac{b}{2}\sqrt{\theta_1}\big) = 0$, i.e. $\omega_1 b + \frac{b}{2}\sqrt{\theta_1} = -\frac{b^2(\omega_1 + 1 + \frac{1}{2}\sqrt{\theta_1})^2}{4\beta^4}$ is a square in $K(i, \zeta_7, \sqrt{\theta_1})$ and condition **D** does not hold too. Therefore we cannot have cases when condition **D** holds and condition **E** does not hold and in particular this implies that condition **E** may not hold only when $d \leqslant \frac{96}{4} = 24$. On the contrary, with a similar calculation, one can see that the assumption that condition **D** does not hold, in general gives no contradiction with the holding of condition **C**. There are no similar dependences for other possible combinations of the conditions, thus all the other cases may take place. One can get examples of extensions realizing the scenarios given by all the possible combinations by considering the curve in the family $\mathcal{F}_1$ with $b = 1$ and setting the base field K as the extension of $\mathbb{Q}$ whose generators are the ones of K_7/K appearing in the conditions which do not hold. The final computation that gives the degree and the corresponding conditions in Table 1 is straightforward. □

Notice that $[K_7 : K] \leqslant 96 < 2016 = |\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})|$ and the Galois representation

$$\rho_{\mathcal{E}_1,7} \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$$

is not surjective, in accordance with $\mathcal{E}_1$ having complex multiplication.

4 Galois groups Gal(K_7/K) for the curves of $\mathcal{F}_1$

Let $\mathcal{E}_1$ be a curve of the family $\mathcal{F}_1$, let $G := \mathrm{Gal}(K_7/K)$ and let $d := |G|$. Let Q_{16} be the generalized quaternion group of order 16.

Theorem 4.1 *Let K be a field with $\mathrm{char}(K) \neq 2, 3$ and let $\mathcal{E}_1$ be an elliptic curve with Weierstrass form $y^2 = x^3 + bx$, where $b \in K$. Then $\mathrm{Gal}(K_7/K)$ is isomorphic to a subgroup of $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$. In particular, if $[K_7 : K] = 96$, then $\mathrm{Gal}(K_7/K) \simeq Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$.*

Proof Assume that all the conditions in Theorem 3.1 hold. Then $[K_7 : K] = 96$. The image of $\mathrm{Gal}(\overline{K}/K)$ via the Galois representation $\rho_{\mathcal{E}_1,7}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ isomorphic to $G = \mathrm{Gal}(K_7/K)$. We denote by G both $\mathrm{Gal}(K_7/K)$ and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. As a consequence of the properties of the Weil pairing, the action of $\mathrm{Gal}(K_7/K)$ on ζ_7 is via determinant, i.e. $\sigma(\zeta_7) = \zeta_7^{\det(\sigma)}$, where σ denotes both an element of G and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. Consider the tower of extensions in Fig. 1.

We denote by H both $\mathrm{Gal}(K_7/K(\zeta_7))$ and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. We have that the Galois group $\mathrm{Gal}(K(\zeta_7)/K) \simeq G/H$ is isomorphic to $\mathbb{Z}/6\mathbb{Z}$. If σ fixes ζ_7, then $\det(\sigma) = 1$ and $\sigma \in \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. Therefore H is isomorphic to a subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ of order 16. It is well known that $|\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})| = 336 = 16 \cdot 21$. Therefore the image of H in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is a 2-Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. By Sylow's Theorems, the 2-Sylow subgroups are all conjugate and in particular they

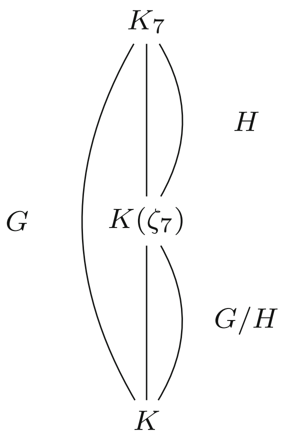

Fig. 1 Tower

are all isomorphic. So it suffices to determine the structure of a 2-Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$ to get H up to isomorphism. The structure of such a group is known; however, according to our knowledge, there is no explicit reference in the literature. So, for the reader's convenience, we are going to describe it. We know that one of the automorphisms of G is the complex multiplication ϕ_1. We consider again $\{P_1, iP_1\}$ as a generating set of $\mathcal{E}_1[7]$. We have

$$P_1 \xmapsto{\phi_1} iP_1 \xmapsto{\phi_1} -P_1 \xmapsto{\phi_1} -iP_1 \xmapsto{\phi_1} P_1.$$

Then the representation of ϕ_1 in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is

$$\phi_1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and $\det(\phi_1) = 1$. Therefore $\phi_1 \in H$. Observe that $\phi_1^2 = -\mathrm{Id}$.

Consider the matrix

$$\tau_1 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

Since $\det(\tau_1) = 1$, we have that $\tau_1 \in \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. In addition τ_1 has order 8 and in particular $\tau_1^4 = -\mathrm{Id}$. One can easily verify that $\phi_1\tau_1 = \tau_1^{-1}\phi_1$. Therefore the group generated by ϕ_1 and τ_1 has the following presentation:

$$\langle \phi_1, \tau_1 \mid \phi_1^2 = \tau_1^4 = -\mathrm{Id},\ \phi_1\tau_1 = \tau_1^{-1}\phi_1 \rangle$$

and it is then isomorphic to the generalized quaternion group Q_{16}, i.e. the dicyclic group Dic_4. This is a group of order 16, hence it is a 2-Sylow subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. Thus H is isomorphic to Q_{16} too. We have

$$H = \langle \phi_1, \varphi_1 \mid \phi_1^2 = \varphi_1^4 = -\mathrm{Id},\ \phi_1\varphi_1 = \varphi_1^{-1}\phi_1 \rangle,$$

where φ_1 is a conjugate of τ_1. To deduce G, we have to look more closely at the automorphism generating $G/H \simeq \mathbb{Z}/6\mathbb{Z}$. In fact $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) \simeq \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \rtimes (\mathbb{Z}/7\mathbb{Z})^* \simeq \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \rtimes \mathbb{Z}/6\mathbb{Z}$. Thus $G \simeq H \rtimes \mathbb{Z}/6\mathbb{Z} \simeq Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$. We are going to show that this semidirect product is not a direct product. The group $\mathrm{Gal}(K(\zeta_7)/K) \simeq G/H$ is generated by an automorphism ψ_1 corresponding to the automorphism σ_1 of $\mathbb{Q}(\zeta_7, i)/\mathbb{Q}$ mapping ζ_7 to ζ_7^5. Since $\sigma_1(\omega_1) = \omega_3$ and $\sigma_1(\theta_1) = \theta_3$, then we have that ψ_1 acts on the basis $\{P_1, iP_1\}$ by mapping P_1 to one of the points $\pm P_s$, $\pm iP_s$, for some $s \in \{5, 6\}$. Observe that if x_1 is sent to x_s (respectively $-x_s$), for some $s \in \{5, 6\}$, then $-x_1$ is sent to $-x_s$ (resp. x_s). Therefore if ψ_1 maps the point P_1 to P_s (resp. $-P_s$) then ψ_1 maps the point iP_1 to one of the points $\pm iP_s$. Similarly if ψ_1 maps the point P_1 to iP_s (resp. $-iP_s$), then ψ_1 maps the point iP_1 to one of the points $\pm P_s$. Let

$\psi_1(P_1) = \alpha P_1 + \beta i P_1$. Then $\psi_1(iP_1) = \pm(-\beta P_1 + \alpha i P_1)$, i.e.

$$\psi_1 = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix} \quad \text{or} \quad \psi_1 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}.$$

Since $iP_1 = \phi_1(P_1)$, we have that if ψ_1 and ϕ_1 commute, then $\psi_1(iP_1) = \phi_1(\psi_1(P_1))$ $= \alpha i P_1 - \beta P_1$. In this case the representation of ψ_1 in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is the following:

$$\psi_1 = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha \end{pmatrix}.$$

Observe that every power of ψ_1 is a matrix of the same type

$$\psi_1^n = \begin{pmatrix} \alpha_n & -\beta_n \\ \beta_n & \alpha_n \end{pmatrix},$$

for some $\alpha_n, \beta_n \in \mathbb{Z}/7\mathbb{Z}$. In particular

$$\psi_1^3 = \begin{pmatrix} \alpha^3 - 3\alpha\beta^2 & \beta^3 - 3\alpha^2\beta \\ -\beta^3 + 3\alpha^2\beta & \alpha^3 - 3\alpha\beta^2 \end{pmatrix} = \begin{pmatrix} \alpha_3 & -\beta_3 \\ \beta_3 & \alpha_3 \end{pmatrix},$$

for some $\alpha_3, \beta_3 \in \mathbb{Z}/7\mathbb{Z}$. Since $G/H \simeq \mathbb{Z}/6\mathbb{Z}$ and $G = H \rtimes G/H$, we have that $\psi_1^6 = \mathrm{Id}$. Hence

$$(\psi_1^3)^2 = \begin{pmatrix} \alpha_3^2 - \beta_3^2 & -2\alpha_3\beta_3 \\ 2\alpha_3\beta_3 & \alpha_3^2 - \beta_3^2 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 7.$$

Thus $\alpha_3\beta_3 \equiv 0 \pmod 7$, implying $\alpha_3 = 0$ or $\beta_3 = 0$. Therefore $\alpha^3 - 3\alpha\beta^2 \equiv 0 \pmod 7$ or $\beta^3 - 3\alpha^2\beta \equiv 0 \pmod 7$, i.e. $\alpha = 0$ or $\beta = 0$ or $\alpha^2 \equiv 3\beta^2 \pmod 7$ or $\beta^2 \equiv 3\alpha^2 \pmod 7$. The last two congruences have no nontrivial solutions in $\mathbb{Z}/7\mathbb{Z}$. Thus $\alpha = 0$ or $\beta = 0$. Assume $\alpha = 0$, then

$$\psi_1 = \begin{pmatrix} 0 & -\beta \\ \beta & 0 \end{pmatrix} = \beta\phi_1.$$

Since $\psi_1^6 = \mathrm{Id}$ and $\phi_1^2 = -\mathrm{Id}$, we have $-\beta^6 \equiv 1 \pmod 7$ and we get a contradiction with Fermat's Little Theorem. If $\beta = 0$, then we see that the automorphism Ψ_1 is represented by a scalar matrix $\alpha \cdot \mathrm{Id}$. Since Ψ_1 acts on ζ_7 via determinant and we are assuming that Ψ_1 is the automorphism of order 6 induced by the automorphism σ_1 mapping ζ_7 to ζ_7^5, we have that $\det(\Psi_1) \equiv 5 \pmod 7$, i.e. $\alpha^2 \equiv 5 \pmod 7$. This congruence has no solutions in $\mathbb{Z}/7\mathbb{Z}$. Therefore

$$\psi_1 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}$$

and ψ_1 and ϕ_1 do not commute. Hence G is not isomorphic to $Q_{16} \times \mathbb{Z}/6\mathbb{Z}$. If $[K_7 : K] < 96$, then G is isomorphic to a proper subgroup of $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$. □

We are going to describe the Galois group $G = \mathrm{Gal}(K_7/K)$ (up to isomorphism), for all possible $d := [K_7 : K] \leqslant 96$. We firstly make a few general remarks. In the last part of the proof of Theorem 4.1 we have shown that

$$\psi_1 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}.$$

Hence

$$\psi_1^2 = \begin{pmatrix} \alpha^2 + \beta^2 & 0 \\ 0 & \alpha^2 + \beta^2 \end{pmatrix} = -\det(\psi_1)\,\mathrm{Id}$$

and then ψ_1^2 and ψ_1^4 commute with every other automorphism of G. Observe that instead $\psi_1^3 = -\det(\psi_1)\psi_1$ does not commute with ϕ_1.

We recall that every subgroup of a generalized quaternion group is cyclic or it is a (generalized) quaternion group itself. The only proper non abelian subgroup of Q_{16} is Q_8. The other proper nontrivial subgroups of Q_{16} are the groups $\mathbb{Z}/m\mathbb{Z}$, with $m \in \{2, 4, 8\}$.

By [25, Chapter II, Theorem 2.3], the extension $K_7/K(i)$ is abelian. Therefore, when condition **A** does not hold, we have that G is an abelian group. Observe that if conditions **C**, **D** and **E** hold, then $\mathrm{Gal}(K_7/K(i, \zeta_7))$ is an abelian group of order 8, which is a subgroup of Q_{16}, i.e. $\mathrm{Gal}(K_7/K(i, \zeta_7)) \simeq \mathbb{Z}/8\mathbb{Z}$. In this case we have $\mathrm{Gal}(K_7/K(i, \zeta_7)) = \langle \varphi_1 \rangle$. In addition $\mathrm{Gal}(K_7/K(i)) = \langle \varphi_1, \psi_1 \rangle \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. In particular ψ_1 commutes with φ_1. Moreover we deduce that the existence of any power of φ_1 in G is related to the holding of at least some of the conditions **C**, **D** and **E**. We also deduce that if **A** does not hold, then $\phi_1 \notin G$. On the other hand if **A** holds and at least one of **C**, **D** and **E** holds, then G has a subgroup of order 4, which is isomorphic to a subgroup of Q_{16} that is not generated by any power of φ_1. Hence in this case ϕ_1 is an automorphism of G. We also observe that ϕ_1 does not commute with every power φ_1^n of φ_1, with $n \not\equiv 0 \pmod 4$; in fact $\phi_1 \varphi_1^n = \varphi_1^{-n} \phi_1$, for every $n \not\equiv 0 \pmod 4$. Thus if Q_8 is a subgroup of G under certain conditions, then we have that $\phi_1 \in H$. Furthermore note that $\phi_1^2 = \varphi_1^4 = -\mathrm{Id}$ is an automorphism of $\mathrm{Gal}(K_7/K(i))$.

Galois groups Gal $(K(\mathcal{E}_1[7])/K)$

$d = 96$. If the degree d of the extension K_7/K is 96, then all the conditions in Table 1 hold. We have already proved in Theorem 4.1 that $G \simeq Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$.

$d = 48$. If the degree d of the extension K_7/K is 48, then condition **B1** holds, because of $3 \mid d$. If **E** does not hold, then as stated in the proof of Theorem 3.1 we have that **D** does not hold and we would have an extension of degree $d < 48$. Therefore condition **E** holds.

- If **A** does not hold, then G is abelian, as mentioned above. We have $G = \langle \varphi_1, \psi_1 \rangle \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

- If **A** holds, we have that ϕ_1 is an automorphism of order 4 of G (recall that condition **E** holds too) and G is not abelian (recall that we have already observed that ϕ_1 does not commute with any map in Q_{16} except its powers).
  If **B2** holds, then ψ_1 has order 6 and $G \simeq Q_8 \rtimes \mathbb{Z}/6\mathbb{Z}$.
  If **B2** does not hold, then $G/H \simeq \mathbb{Z}/3\mathbb{Z}$ is generated by ψ_1^2, which is represented by a scalar matrix, as we have observed above. Thus $G \simeq Q_{16} \times \mathbb{Z}/3\mathbb{Z}$.

$d = 32$. If the degree d of the extension K_7/K is 32, then all the conditions hold but **B1**. Thus we have that $G/H \simeq \mathbb{Z}/2\mathbb{Z}$ is generated by the automorphism ψ_1^3 mapping ζ_7 to ζ_7^{-1} and $G \simeq Q_{16} \rtimes \mathbb{Z}/2\mathbb{Z}$.

$d = 24$. Condition **B1** must hold in all cases when $d = 24$, because of $3 \mid d$.

- If **B2** holds, then $G/H \simeq \mathbb{Z}/6\mathbb{Z}$.
  If **A** does not hold, then G is abelian and we have $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
  Assume that **A** holds. Since **B2** holds, we have that either **C** or **E** also holds and $\phi_1 \in G$. Therefore $H = \langle \phi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ and $G = \langle \phi_1, \psi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z} \simeq D_8 \times \mathbb{Z}/3\mathbb{Z}$ (recall that ϕ_1 does not commute with ψ_1).
- If **B2** does not hold, then $G/H \simeq \mathbb{Z}/3\mathbb{Z}$.
  If **A** does not hold, then G is abelian and we have $G \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
  Assume that **A** holds. Since we are assuming that **B2** does not hold, then **E** holds. We have that $\phi_1 \in G$. Therefore H is a subgroup of Q_{16} of order 8, which is not abelian (recall that ϕ_1 does not commute with any map in Q_{16} except its powers). The group G/H is generated by ψ_1^2 or ψ_1^4. Since these two maps commute with every homomorphism in G, we have $G \simeq Q_8 \times \mathbb{Z}/3\mathbb{Z}$.

$d = 16$. If the degree d of the extension K_7/K is 16, as stated in Table 1, then condition **B1** does not hold and **E** holds. Only one of the other conditions does not hold.

- If **B2** does not hold, then G/H is trivial. Therefore $G \simeq Q_{16}$.
- If **B2** holds, then $G/H = \langle \psi_1^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and $|H| = 8$.
  If **A** does not hold, then we have an abelian extension and $G \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  Assume that **A** holds. Since **E** holds, we have that $\phi_1 \in G$ and H is not abelian. Therefore $G \simeq Q_8 \rtimes \mathbb{Z}/2\mathbb{Z}$ (recall that ψ_1^3 does not commute with ϕ_1).

$d = 12$. If the degree d of the extension K_7/K is 12, then Q_8 cannot be a subgroup of G. Condition **B1** holds because of $3 \mid d$. We have the following cases.

- If **B2** holds, then $G/H \simeq \mathbb{Z}/6\mathbb{Z}$ and $H \simeq \mathbb{Z}/2\mathbb{Z}$. Thus G is abelian and $G \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.
- If **B2** does not hold, then G/H has order 3 and it is generated by ψ_1^2 or ψ_1^4. In this case H has order 4. Since every abelian subgroup of Q_{16} is cyclic and ψ_1^2 and ψ_1^4 commute with every other automorphism of G, we have $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

$d = 8$. If the degree d of the extension K_7/K is 8, then **B1** does not hold.

- If **A** does not hold, then we have an abelian extension.
  If **B2** holds, then G/H has order 2, H has order 4 and $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
  If **B2** does not hold, then $G = H \simeq \mathbb{Z}/8\mathbb{Z}$.
- Assume that **A** holds.
  If **B2** does not hold, then $G = H$ has order 8. In this case **E** holds, hence ϕ_1 is an automorphism of G and $G \simeq Q_8$.
  Assume that **B2** holds. We have that one of **C** and **E** holds too. Hence $G/H = \langle \psi_1^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and $H = \langle \phi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. The complex multiplication ϕ_1 is an automorphism of G which does not commute with ψ_1^3. Then $G \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$.

$d = 6$. If the degree d of the extension K_7/K is 6, then condition **B1** must hold in all cases, as listed in Table 1, and G/H has order divisible by 3. In every case we have an abelian group of order 6, i.e. $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
$d = 4$. If the degree d of the extension K_7/K is 4, then **B1** does not hold.

- If **B2** does not hold, then G/H is trivial and $G = H$ is isomorphic to a subgroup of Q_{16} of order 4. Thus $G \simeq \mathbb{Z}/4\mathbb{Z}$.
- If **B2** holds, then $G/H \simeq \mathbb{Z}/2\mathbb{Z}$ and G is isomorphic to the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d \leqslant 3$. If the degree d of the extension K_7/K is 3, 2 or 1, the Galois group is respectively $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ or $\{\mathrm{Id}\}$.

5 Generators of the 7-th division field for elliptic curves $y^2 = x^3 + c$

Let $\mathcal{E}_2$ be an elliptic curve with Weierstrass form $y^2 = x^3 + c$, with $c \in K$. Then the m-th division polynomial $\Psi_m(x)$ of $\mathcal{E}_2$ is a polynomial in x^3, because of the automorphism of $\mathcal{E}_2$ given by the complex multiplication ϕ_2, which maps (x, y) to $(\zeta_3 x, y)$. If $m = p$ is an odd prime, then $\Psi_p(x)$ has degree $\frac{p^2-1}{2}$. Observe that $3 \mid p^2 - 1$. Set $t := x^3$, then $\Psi_p(t)$ is a polynomial of degree $\frac{p^2-1}{6}$ in the variable t. For $1 \leqslant j \leqslant \frac{p^2-1}{6}$, let δ_j be the roots of $\Psi_p(t)$. Therefore the $p^2 - 1$ abscissas of the p-torsion points of $\mathcal{E}_2$ of exact order p are $\left\{\sqrt[3]{\delta_j c}, \zeta_3 \sqrt[3]{\delta_j c}, \zeta_3^2 \sqrt[3]{\delta_j c} \mid 1 \leqslant j \leqslant \frac{p^2-1}{6}\right\}$. We also have that the ordinates of the points with abscissas in $\left\{\sqrt[3]{\delta_j}, \zeta_3 \sqrt[3]{\delta_j}, \zeta_3^2 \sqrt[3]{\delta_j}\right\}$ are $\pm\sqrt{(\delta_j + 1)c}$. The point $\phi_2\left(\left(\sqrt[3]{\delta_j c}, \sqrt{\delta_j + c}\right)\right) = \left(\zeta_3 \sqrt[3]{\delta_j c}, \sqrt{\delta_j + c}\right)$ is still a p-torsion point of $\mathcal{E}_2$, for every δ_j. If $P_j = \left(\sqrt[3]{\delta_j c}, \sqrt{\delta_j + c}\right)$ and $\phi_2(P_j)$ are linearly independent, then $\{P_j, \phi_2(P_j)\}$ is a generating set for $\mathcal{E}_2[p]$. In this case, we have both

$$K(\mathcal{E}_2[p]) = K\left(\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j + 1)c}\right), \quad K(\mathcal{E}_2[p]) = K\left(\sqrt[3]{\delta_j c}, \zeta_p, \sqrt{(\delta_j + 1)c}\right)$$

(this last equality following by [3, Theorem 1.1]). We now make these generating sets explicit for $p = 7$, by producing the coordinates of the points in $\mathcal{E}_2[7]$.

We denote by $r_7(x)$ the 7-th division polynomial of a curve $\mathcal{E}_2 \in \mathcal{F}_2$. We have

$$\begin{aligned} r_7(x) := 7x^{24} &+ 3944c\,x^{21} - 42896c^2x^{18} - 829696c^3x^{15} - 928256c^4x^{12} \\ &- 1555456c^5x^9 - 2809856c^6x^6 - 802816c^7x^3 + 65536c^8. \end{aligned}$$

Let σ_2 be the automorphism of $\mathbb{Q}(\zeta_3, \zeta_7)/\mathbb{Q}$ mapping ζ_7 to ζ_7^5, let φ be the automorphism of $\mathbb{Q}(\zeta_3, \zeta_7)/\mathbb{Q}$ mapping ζ_3 to ζ_3^2 and let

$$\begin{aligned}
\delta_1 \ &:= -\big((-132\zeta_3 - 120)\zeta_7^5 + (-168\zeta_3 - 12)\zeta_7^4 + (-24\zeta_3 + 60)\zeta_7^3 \\
&\qquad +(-60\zeta_3 - 84)\zeta_7^2 + (-192\zeta_3 - 96)\zeta_7 - 96\zeta_3 + 52\big); \\
\delta_2 \ &:= \sigma_2(\delta_1) = -\big((-24\zeta_3 - 84)\zeta_7^5 + (36\zeta_3 - 108)\zeta_7^4 + (108\zeta_3 - 72)\zeta_7^3 \\
&\qquad +(168\zeta_3 + 12)\zeta_7^2 + (144\zeta_3 + 72)\zeta_7 + 72\zeta_3 + 64\big); \\
\delta_3 \ &:= \sigma_2(\delta_2) = -\big((108\zeta_3 + 180)\zeta_7^5 + (-60\zeta_3 + 24)\zeta_7^4 + (132\zeta_3 + 120)\zeta_7^3 \\
&\qquad +(-36\zeta_3 + 108)\zeta_7^2 + (72\zeta_3 + 36)\zeta_7 + 36\zeta_3 + 172\big); \\
\delta_4 \ &:= \sigma_2(\delta_3) = -\big((132\zeta_3 + 12)\zeta_7^5 + (168\zeta_3 + 156)\zeta_7^4 + (24\zeta_3 + 84)\zeta_7^3 \\
&\qquad +(60\zeta_3 - 24)\zeta_7^2 + (192\zeta_3 + 96)\zeta_7 + 96\zeta_3 + 148\big); \\
\delta_5 \ &:= \sigma_2(\delta_4) = -\big((24\zeta_3 - 60)\zeta_7^5 + (-36\zeta_3 - 144)\zeta_7^4 + (-108\zeta_3 - 180)\zeta_7^3 \\
&\qquad +(-168\zeta_3 - 156)\zeta_7^2 + (-144\zeta_3 - 72)\zeta_7 - 72\zeta_3 - 8\big); \\
\delta_6 \ &:= \sigma(\delta_5) = -\big((-108\zeta_3 + 72)\zeta_7^5 + (60\zeta_3 + 84)\zeta_7^4 + (-132\zeta_3 - 12)\zeta_7^3 \\
&\qquad +(36\zeta_3 + 144)\zeta_7^2 + (-72\zeta_3 - 36)\zeta_7 - 36\zeta_3 + 136\big); \\
\delta_7 \ &:= \frac{12\zeta_3 + 8}{7}; \\
\delta_8 \ &:= \varphi(\delta_8) = -\frac{12\zeta_3 + 4}{7}.
\end{aligned}$$

The polynomial $r_7(x)$ factors over $K(\zeta_3, \zeta_7)$ as follows:

$$r_7(x) = 7\prod_{j=1}^{8}(x^3 + \delta_j c).$$

Then, as mentioned above, the 48 torsion points of $\mathcal{E}_2$ with exact order 7 are

$$\begin{aligned}
\pm P_j = (x_j, \pm y_j) &= \left(\sqrt[3]{\delta_j c}, \pm\sqrt{(\delta_j + 1)c}\right); \\
\pm\phi(P_j) = (\zeta_3 x_j, \pm y_j) &= \left(\zeta_3\sqrt[3]{\delta_j c}\,, \pm\sqrt{(\delta_j + 1)c}\right); \\
\pm\phi^2(P_j) = (\zeta_3^2 x_j, \pm y_j) &= \left(\zeta_3^2\sqrt[3]{\delta_j c}\,, \pm\sqrt{(\delta_j + 1)c}\right);
\end{aligned}$$

for $1 \leqslant j \leqslant 8$.

Theorem 5.1 *Let δ_j be as above, with $1 \leqslant j \leqslant 6$. Then*

$$K_7 = K\left(\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j + 1)c}\right) = K\left(\sqrt[3]{\delta_j c}, \zeta_7, \sqrt{(\delta_j + 1)c}\right).$$

Proof We have already observed at the beginning of this section that if $\phi_2(P)$ is a 7-torsion point that is not a multiple of P, then a basis for $\mathcal{E}_2[7]$ is given by $\{P, \phi_2(P)\}$ and $K_7 = K(x(P), \zeta_3, y(P))$. However, in some cases the point $\phi_2(P)$ is a multiple of P. This happens for the points P_j and $\phi_2(P_j)$, when $j = 7, 8$ (in fact if $\zeta_7 \notin K$, then $\zeta_7 \notin K(x(P_j), \zeta_3, y(P_j))$, for $j = 7, 8$, contradicting the well-known property of the Weil pairing recalled above). By the use of a software of computational algebra (we used AXIOM again), one can verify that $x(2P_1) = x(P_3)$ (i.e. $2P_1 = P_3$ or $2P_1 = -P_3$) and $x(4P_1) = x(P_5)$ (i.e. $4P_1 = P_5$ or $4P_1 = -P_5$). Suppose that $\phi_2(P_1) = nP_1$. Since $\phi_2^2(P_1) = -P_1 - \phi_2(P_1)$, we have $(n^2 + n + 1)P_1 = O$. Thus n is a root of $n^2 + n + 1$ modulo 7, hence $n \equiv 2, 4 \pmod 7$. But, as noticed above, we have $x(2P_1) \neq x(\phi_2(P_1))$ and $x(4P_1) \neq x(\phi_2(P_1))$. Thus $\phi_2(P_1)$ and P_1 are linearly independent. Similar arguments apply for P_3 and P_5. In addition one can verify that $x(2P_2) = x(P_4)$ and $x(4P_2) = x(P_6)$ and repeat the arguments for those points too. Therefore P_j and $\phi_2(P_j)$ are linearly independent for $j = 1, \ldots, 6$ and $\{P_j, \phi_2(P_j)\}$ is a basis of $\mathcal{E}_2[7]$, for every $j = 1, \ldots, 6$. Then $K_7 = K\left(\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j + 1)c}\right)$. As stated above, by [3, Theorem 1.1] we also have $K_7 = K\left(\sqrt[3]{\delta_j c}, \zeta_7, \sqrt{(\delta_j + 1)c}\right)$. □

6 Degrees $[K_7 : K]$ for the curves of $\mathcal{F}_2$

By the results achieved in Theorem 5.1, we are going to describe the possible degrees $[K_7 : K]$ for the elliptic curves of the family $\mathcal{F}_2$. From now on we will fix the generating set $\{P_1, \phi_2(P_1)\}$ for $\mathcal{E}_2[7]$. Thus $K_7 = K\left(\sqrt[3]{\delta_1 c}, \zeta_3, \sqrt{(\delta_1 + 1)c}\right) = K\left(\sqrt[3]{\delta_1 c}, \zeta_7, \sqrt{(\delta_1 + 1)c}\right)$. Clearly all the results that we are going to show about the degree $[K_7 : K]$ and the Galois group $\mathrm{Gal}(K_7/K)$ hold as well for every other generating set $\left\{\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j + 1)c}\right\}$ or $\left\{\sqrt[3]{\delta_j c}, \zeta_7, \sqrt{(\delta_j + 1)c}\right\}$ of the extension K_7/K, with $2 \leqslant j \leqslant 6$.

Theorem 6.1 *Let $\mathcal{E}_2\colon y^2 = x^3 + c$, with $c \in K$. Let δ_1 be as above. Consider the conditions*

A. $\zeta_3 \notin K$;
B1. $\zeta_7 + \zeta_7^{-1} \notin K(\zeta_3)$; **C**. $\sqrt[3]{\delta_1 c} \notin K(\zeta_3, \zeta_7)$;
B2. $\zeta_7 \notin K(\zeta_3, \zeta_7 + \zeta_7^{-1})$; **D**. $\sqrt{(\delta_1 + 1)c} \notin K(\zeta_3, \zeta_7)$.

The possible degrees of the extension K_7/K are given in Table 2:

Table 2 Degrees $[K(\mathcal{E}_2[7]):K]$

d	Holding conditions	d	Holding conditions
72	**A**, **B1**, **B2**, **C**, **D**	8	**A**, **B2**, **D**
36	**B1**, **C** *and two of* **A**, **B2**, **D**	6	*one of* **B1**, **C** *and one of* **A**, **B2**, **D**
24	*one of* **B1**, **C** and **A**, **B2**, **D**	4	*two of* **A**, **B2**, **D**
18	**B1**, **C** *and one of* **A**, **B2**, **D**	3	*one of* **B1**, **C**
12	*one of* **B1**, **C** *and two of* **A**, **B2**, **D**	2	*one of* **A**, **B2**, **D**
9	**B1**, **C**	1	*no conditions hold*

Proof Consider the tower of extensions in Fig. 1.

$$\begin{aligned} K \subseteq K(\zeta_3) \subseteq K(\zeta_3, \zeta_7 + \zeta_7^{-1}) \subseteq K(\zeta_3, \zeta_7) \\ \subseteq K\big(\zeta_3, \zeta_7, \sqrt[3]{\delta_1 c}\big) \subseteq K\big(\zeta_3, \zeta_7, \sqrt[3]{\delta_1 c}, \sqrt{(\delta_1+1)c}\big). \end{aligned}$$

We have that each of the degrees $[K(\zeta_3, \zeta_7 + \zeta_7^{-1}) : K(\zeta_3)]$ and $[K(\zeta_3, \zeta_7, \sqrt[3]{\delta_1 c}) : K(\zeta_3, \zeta_7)]$ divides 3. In addition each of the degrees $[K(\zeta_3) : K]$, $[K(\zeta_3, \zeta_7) : K(\zeta_3, \zeta_7 + \zeta_7^{-1})]$ and $[K_7 : K(\zeta_3, \zeta_7, \sqrt[3]{\delta_1 c})]$ divides 2. Since the fields $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_7)$ are linearly disjoint over $\mathbb{Q}$, then condition **A** is independent of conditions **B1** and **B2** and the other way around. In addition, with the software AXIOM we have verified that when $K \cap \mathbb{Q}(\zeta_3, \zeta_7) = \mathbb{Q}$ neither $\delta_1 + 1$ is a square in $K(\zeta_3, \zeta_7)$, nor δ_1 is a cube in $K(\zeta_3, \zeta_7)$. Then the fields $K(\sqrt[3]{\delta_1 c})$ and $K(\sqrt{(\delta_1+1)c})$ are linearly disjoint over $\mathbb{Q}(\zeta_3, \zeta_7)$. Hence all the conditions are independent on each other, except **B1** and **B2**. Then we can have all the possible combinations of the conditions. The conclusions follow immediately from $[K_7 : K]$ being the product of the degrees of the intermediate extensions appearing in the tower. One can produce examples of extensions realizing the scenarios given by all the possible combinations by considering the curve in the family $\mathcal{F}_2$ with $c = 1$ and setting the base field K as the extension of $\mathbb{Q}$ whose generators are the ones of K_7/K appearing in the conditions which do not hold. □

Notice that $[K_7 : K] \leqslant 72 < 2016 = |\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})|$ and the Galois representation

$$\rho_{\mathcal{E}_2,7} \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$$

is not surjective, in accordance with $\mathcal{E}_2$ having complex multiplication.

7 Galois groups Gal(K_7/K) for the curves of $\mathcal{F}_2$

Let $\mathcal{E}_2$ be a curve of the family $\mathcal{F}_2$. We are going to show all possible Galois groups $\mathrm{Gal}(K(\mathcal{E}_2[7])/K)$, with respect to the degrees $d = [K_7 : K] \leqslant 72$.

Theorem 7.1 *Let K be a field with* $\mathrm{char}(K) \neq 2, 3$ *and let $\mathcal{E}_2$ be an elliptic curve with Weierstrass form $y^2 = x^3 + c$, where $c \in K$. Then* $\mathrm{Gal}(K_7/K)$ *is isomorphic to a subgroup of $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$. In particular, if* $[K_7 : K] = 72$, *then* $\mathrm{Gal}(K_7/K) \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$.

Proof Suppose that all the conditions in Theorem 6.1 hold, so that $[K_7 : K] = 72$. The image of $\mathrm{Gal}(\overline{K}/K)$ via the Galois representation $\rho_{\mathcal{E}_2,7}$ is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ isomorphic to $G = \mathrm{Gal}(K_7/K)$. As for the family $\mathfrak{F}_1$, we denote by G both $\mathrm{Gal}(K_7/K)$ and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. Consider the tower of extensions in Fig. 1. We denote by H both $\mathrm{Gal}(K_7/K(\zeta_7))$ and its image in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. The Galois group $\mathrm{Gal}(K(\zeta_7)/K)$ is then isomorphic to the quotient G/H. The group H has order 12, because of $\mathrm{Gal}(K(\zeta_7)/K) \simeq \mathbb{Z}/6\mathbb{Z}$. Since the action of $\sigma \in \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ on ζ_7 is given by $\sigma(\zeta_7) := \zeta_7^{\det(\sigma)}$, then $\det(\sigma) = 1$, for every $\sigma \in H$. Thus H is indeed a subgroup of $\mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z})$. We are going to describe H up to isomorphism. For every positive integer n, we denote by D_{2n} the dihedral group of order $2n$. Since we are assuming that all the conditions in Theorem 6.1 hold, then the complex multiplication ϕ_2 and $-\mathrm{Id}$ are automorphisms of H. The complex multiplication ϕ_2 has order 3 and acts on the basis $\{P_1, \phi_2(P_1)\}$ as

$$P_1 \xmapsto{\phi_2} \phi_2(P_1), \quad \phi_2(P_1) \xmapsto{\phi_2} \phi_2^2(P_1).$$

Since $\phi_2^2(P_1) = -P_1 - \phi_2(P_1)$, we can represent ϕ_2 in $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ as

$$\phi_2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Then the inverse of ϕ_2 is represented by the matrix

$$\phi_2^{-1} = \phi_2^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

The automorphism $-\mathrm{Id}$, swapping the ordinates $P \xmapsto{-\mathrm{Id}} -P$ for every $P \in \mathcal{E}_2[7]$, corresponds to the automorphism of K_7/K that maps $\sqrt{(\delta_j + 1)c}$ to $-\sqrt{(\delta_j + 1)c}$, for all $1 \leqslant j \leqslant 8$. Clearly ϕ_2 and $-\mathrm{Id}$ commute, so H has a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$. We are going to show that H is not abelian. Suppose that H is abelian. Then it is isomorphic to either $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$. Let $\sigma \in H$. Since σ commutes with ϕ_2, one gets that

$$\sigma = \begin{pmatrix} \alpha & -\beta \\ \beta & \alpha - \beta \end{pmatrix},$$

for some $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$. We have already observed that $-\mathrm{Id} \in H$. If $H \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, then there exists $\sigma \in H$ such that $\sigma^4 = \mathrm{Id}$ and $\sigma^2 = -\mathrm{Id}$, i.e.

$$\sigma^2 = \begin{pmatrix} \alpha^2 - \beta^2 & \beta^2 - 2\alpha\beta \\ 2\alpha\beta - \beta^2 & \alpha^2 - 2\alpha\beta \end{pmatrix} \equiv \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \pmod 7.$$

The congruence $\beta^2 - 2\alpha\beta \equiv 0 \pmod 7$ implies $\beta = 0$ or $\beta = 2\alpha$. If $\beta = 0$, then $\alpha^2 \equiv -1 \pmod 7$, which has no solutions. If $\beta = 2\alpha$, then $-3\alpha^2 \equiv -1 \pmod 7$, which has no solutions as well. On the other hand, if $H \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$, then there exists $\sigma \in H$ such that $\sigma^2 = \mathrm{Id}$ and $\sigma \neq \pm\mathrm{Id}$. By

$$\sigma^2 = \begin{pmatrix} \alpha^2 - \beta^2 & \beta^2 - 2\alpha\beta \\ 2\alpha\beta - \beta^2 & \alpha^2 - 2\alpha\beta \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 7,$$

we get again $\beta = 0$ or $\beta = 2\alpha$. If $\beta = 0$, then $\sigma = \pm\mathrm{Id}$ and we have a contradiction. Suppose $\beta = 2\alpha$. From $\det(\sigma) \equiv 1 \pmod 7$ we get $\alpha^2 \equiv -2 \pmod 7$, which has no solutions. Therefore H is not abelian, as claimed. In addition H is a group of order 12, with a subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z}$. We have that either $H \simeq \mathrm{D}_{12}$ or $H \simeq \mathrm{Dic}_3$, where Dic_3 is the dicyclic group of order 12 (which is isomorphic to $\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$). Suppose that $H \simeq \mathrm{D}_{12}$. We also have $H \simeq \mathrm{D}_6 \times \mathbb{Z}/2\mathbb{Z}$, thus H is generated by $-\mathrm{Id}$, ϕ_2 and another automorphism τ of order 2 such that $\phi_2\tau = \tau\phi_2^{-1}$ (i.e. $\langle\phi_2, \tau\rangle \simeq \mathrm{D}_6$ and $H = \langle -\mathrm{Id}\rangle \times \langle\phi_2, \tau\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathrm{D}_6 \simeq \mathrm{D}_{12}$). The relation $\phi_2\tau = \tau\phi_2^{-1}$ implies that τ is represented by a matrix of the form

$$\tau = \begin{pmatrix} \alpha & \beta \\ \alpha + \beta & -\alpha \end{pmatrix},$$

for some $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$. Since τ has order 2, we have

$$\tau^2 = \begin{pmatrix} \alpha^2 + \beta^2 + \alpha\beta & 0 \\ 0 & \alpha^2 + \beta^2 + \alpha\beta \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 7,$$

i.e. $\alpha^2 + \beta^2 + \alpha\beta \equiv 1 \pmod 7$. On the other hand, since $\det(\tau) \equiv 1 \pmod 7$, we have that $\alpha^2 + \beta^2 + \alpha\beta \equiv -1 \pmod 7$ and we find a contradiction. Therefore the group H is isomorphic to $\mathrm{Dic}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ and it is generated by the complex multiplication ψ_2, which has order 3, and an automorphism τ_2 of order 4, such that

$$H = \left\langle \phi_2, \tau_2 \mid \phi_2^3 = \tau_2^4 = 1,\ \phi_2\tau_2 = \tau_2\phi_2^{-1} \right\rangle.$$

In addition $\tau_2^2 = -\mathrm{Id}$. Since $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z}) \simeq \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \rtimes \mathbb{F}_7^* \simeq \mathrm{SL}_2(\mathbb{Z}/7\mathbb{Z}) \rtimes \mathbb{Z}/6\mathbb{Z}$, we have that $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$. For completeness we are going to show that this last semidirect product is not a direct product (as in the case of the family $\mathcal{F}_1$). The group G/H is generated by an automorphism ψ_2 of order 6 corresponding to the automorphism σ_2 of $\mathrm{Gal}(\mathbb{Q}(\zeta_7)/\mathbb{Q})$ mapping ζ_7 to ζ_7^5. As stated above, we have

$$\delta_1 \xmapsto{\sigma_2} \delta_2 \xmapsto{\sigma_2} \delta_3 \xmapsto{\sigma_2} \delta_4 \xmapsto{\sigma_2} \delta_5 \xmapsto{\sigma_2} \delta_6 \xmapsto{\sigma_2} \delta_1.$$

Then $\Psi_2(P_1)$ is one of the points $\pm\Psi_2^n(P_2)$, with $n \in \{0, 1, 2\}$ (where $\phi_2^0 = \mathrm{Id}$). Since $\Psi_2(x_1) = \zeta_3 x_1$, we have that $\Psi_2(\phi_2(P_1))$ is one of the points $\pm\Psi_2^{n+1}(P_2) = \pm\Psi_2(\Psi_2(P_1))$. Suppose that $\Psi_2(P_1) = \alpha P_1 + \beta\Psi_2(P_1)$, for some $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$, thus we see that $\Psi_2(\phi_2(P_1)) = \pm(\beta P_1 + (\beta - \alpha)\Psi_2(P_1))$. Thus

$$\Psi_2 = \begin{pmatrix} \alpha & -\beta \\ \beta & -\beta + \alpha \end{pmatrix} \quad \text{or} \quad \Psi_2 = \begin{pmatrix} \alpha & \beta \\ \beta & \beta - \alpha \end{pmatrix}.$$

Only in the first case Ψ_2 and ϕ_2 commute. By [25, Chapter II, Theorem 2.3], the extension $K_7/K(\zeta_3)$ is abelian. If all the conditions in Theorem 6.1 hold, then the complex multiplication ϕ_2 and Ψ_2 are automorphisms of $\mathrm{Gal}(K_7/K(\zeta_3))$. Therefore they must commute and we get

$$\Psi_2 = \begin{pmatrix} \alpha & -\beta \\ \beta & -\beta+\alpha \end{pmatrix}.$$

Observe that Ψ_2^2 maps P_1 to $\phi_2^j(P_3)$, for some $j \in \{0, 1, 2\}$ and $\phi_2(P_1)$ to $\phi_2^{j+1}(P_3)$. As noted in the proof of Theorem 5.1, we have $x(P_3) = x(2P_1)$, i.e. $P_3 = 2P_1$ or $P_3 = -2P_1$. We also have $x(\phi_2(P_3)) = x(2\phi_2(P_1)) = \phi_2(x(2P_1))$. Hence the automorphism Ψ_2^2 is equal to $\phi_2^j\omega$ for some j, where ω is represented by one of the following matrices:

$$\omega = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{or} \quad \omega = \begin{pmatrix} -2 & 0 \\ 0 & -2 \end{pmatrix}.$$

The second case is not possible, since Ψ_2^2 would not have order 3. Thus we have $\Psi_2^2 = \phi_2^j\omega$, with

$$\omega = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Since $\Psi_2^2 \in G/H$ and $\phi_2^j \in H$, we may assume without loss of generality that $\Psi_2^2 = \omega$, by eventually changing the representative of the class Ψ_2^2 in G/H. Observe that then Ψ_2^2 commutes with every other automorphism of G. Furthermore, we have

$$\Psi_2^2 = \begin{pmatrix} \alpha^2-\beta^2 & \beta^2-2\alpha\beta \\ 2\alpha\beta-\beta^2 & \alpha^2-2\alpha\beta \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \pmod 7,$$

Thus $\beta(\beta-2\alpha) = 0$, implying $\beta = 0$ or $\beta = 2\alpha$. If $\beta = 0$, then $\det(\psi_2) = \alpha^2 \equiv 5 \pmod 7$ (recall that $\psi_2(\zeta_7) = \zeta_7^5 = \zeta_7^{\det(\psi_2)}$), which has no solutions. So $\beta = 2\alpha$ and $-3\alpha^2 \equiv 2 \pmod 7$, i.e. $\alpha \equiv 2 \pmod 7$ or $\alpha \equiv -2 \pmod 7$. Thus we get

$$\psi_2 = \begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix} \quad \text{or} \quad \psi_2 = \begin{pmatrix} -2 & -3 \\ 3 & 2 \end{pmatrix} = -\begin{pmatrix} 2 & 3 \\ -3 & -2 \end{pmatrix}.$$

Again, by eventually change the representative of the class of ψ_2 in G/H, we may assume without loss of generality that

$$\psi_2 = \begin{pmatrix} -2 & -3 \\ 3 & 2 \end{pmatrix}.$$

We consider an automorphism $\rho \in H$ induced by the automorphism of $\mathrm{Gal}(K_7/K)$ mapping ζ_3 to ζ_3^2. Thus ρ maps P_1 to $\phi_2^j(P_4)$, for some $j \in \{0, 1, 2\}$ and we have that there exists a power ϕ_2^s of ϕ_2, with $s \in \{0, 1, 2\}$ such that $j + s \equiv 0 \pmod 3$. We call $\widetilde{\rho}$ the product $\phi_2^s \rho$ and we have that it maps P_1 to P_4. Since ψ_2^3 also maps P_1 to P_4 and

$$\psi_2^3 = \begin{pmatrix} 3 & 1 \\ -1 & 4 \end{pmatrix},$$

then we have

$$\widetilde{\rho} = \begin{pmatrix} 3 & \alpha \\ -1 & \beta \end{pmatrix},$$

for some $\alpha, \beta \in \mathbb{Z}/7\mathbb{Z}$. Thus

$$\widetilde{\rho}\psi_2 - \psi_2\widetilde{\rho} = \begin{pmatrix} 3\alpha - 3 & 3\beta + 4\alpha - 2 \\ 3\beta - 5 & -3\alpha + 3 \end{pmatrix},$$

and therefore $\widetilde{\rho}$ and ψ_2 commute if and only if $\alpha \equiv 1 \pmod 7$ and $\beta \equiv -3 \pmod 7$. But then in this case $\det(\widetilde{\rho}) = -1$ and we would have a contradiction with $\rho \in H$. Therefore $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$ with $G \neq \mathrm{Dic}_3 \times \mathbb{Z}/6\mathbb{Z}$. For every $d = [K_7 : K] < 72$, we have that G is isomorphic to a proper subgroup of $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$. □

Observe that the situation for the Galois groups of the family $\mathcal{F}_2$ is similar to that of the Galois groups of the family $\mathcal{F}_1$; in fact for the curves in $\mathcal{F}_1$ have that $G \simeq \mathrm{Dic}_4 \rtimes \mathbb{Z}/6\mathbb{Z}$, since the dicyclic group Dic_4 of order 16 is nothing but the quaternion group Q_{16}.

We are going to describe the possible Galois groups $G = \mathrm{Gal}(K(\mathcal{E}_2[7])/K)$ when $d \leqslant 72$. In the proof of Theorem 7.1, we showed that $\psi_2^3 = 2\psi_2$ does not commute with $\widetilde{\rho}$. In addition we deduce that τ_2 does not commute with ψ_2 (otherwise we would get $G \simeq \mathrm{Dic}_3 \times \mathbb{Z}/6\mathbb{Z}$) and neither does it commute with ψ_2^3. Recall that, by the mentioned [25, Chapter II, Theorem 2.3], we have that G is abelian whenever **A** does not hold. Recall also that every nontrivial proper subgroup of $\mathrm{Dic}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z}$, with $m \in \{2, 3, 4, 6\}$. In particular, if **D** does not hold, then H is abelian. Furthermore, if **D** does not hold and $\phi_2 \in H$, then we have that every other automorphism of H commutes with ϕ_2 and it is then represented by a matrix of the form

$$\begin{pmatrix} \alpha & -\beta \\ \beta & \alpha - \beta \end{pmatrix},$$

for some α and β in $\mathbb{Z}/7\mathbb{Z}$. Every matrix of this type commutes with ψ_2 too. Therefore, if **D** does not hold, then G is abelian as well.

Galois groups Gal $(K(\mathcal{E}_2[7])/K)$

$d = 72$. If the degree d of the extension K_7/K is 72, then all the conditions hold. We have proved in Theorem 7.1 that in this case $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$.

$d = 36$. If the degree d of the extension K_7/K is 36, then condition **B1** and condition **C** hold.

- If one of **A** and **D** does not hold, then we have an abelian group. Since both condition **B1** and condition **B2** hold, then $G/H \simeq \mathbb{Z}/6\mathbb{Z}$ and thus $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z})^2 \times (\mathbb{Z}/3\mathbb{Z})^2$.
- If **B2** does not hold, then $G/H \simeq \mathbb{Z}/3\mathbb{Z}$ and $G = \langle \phi_2, \tau_2, \psi_2^2 \rangle$. Since ψ_2^2 is represented by a diagonal matrix and commutes with every other automorphism, we have $G \simeq \mathrm{Dic}_3 \times \mathbb{Z}/3\mathbb{Z}$.

$d = 24$. Only one of condition **B1** and condition **C** holds and all the other conditions hold.

- If **C** does not hold, then $G = \langle \tau_2, \psi_2 \rangle \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/6\mathbb{Z} \simeq \mathrm{D}_8 \times \mathbb{Z}/3\mathbb{Z}$.
- If **B1** does not hold, then $G/H \simeq \mathbb{Z}/2\mathbb{Z} = \langle \psi_2^3 \rangle$. Thus $G \simeq \mathrm{Dic}_3 \rtimes \mathbb{Z}/2\mathbb{Z}$.

$d = 18$. Conditions **B1** and **C** hold and the automorphism ϕ_2 has order 3. Since only one of the other conditions holds, we have that at least one of **A** or **D** does not hold and G is abelian.

- If either **A** or **D** holds, then $G \simeq (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$.
- If both **A** and **D** do not hold, then **B2** holds. We have $G/H = \langle \psi_2 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$ and $H \simeq \langle \phi_2 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$. Since ϕ_2 and ψ_2 commute, we have that $G \simeq (\mathbb{Z}/3\mathbb{Z})^2 \times \mathbb{Z}/2\mathbb{Z}$ as well.

$d = 12$. Only one of conditions **B1** and **C** holds and two of the other conditions hold.

- If both **B1** and **B2** do not hold, then the extension G/H is trivial and $G = H \simeq \mathrm{Dic}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.
- If **B1** does not hold and **B2** holds, then $H \simeq \mathbb{Z}/2\mathbb{Z}$ and $G/H \simeq \mathbb{Z}/6\mathbb{Z}$. One of **A** and **D** does not hold, so the extension K_7/K is abelian with Galois group $G \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.
- If **B1** holds and **B2** does not hold, then G/H is generated by ψ_2^2 and $H = \langle \tau_2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. Since ψ_2^2 commutes with τ_2, we get that the Galois group G is isomorphic to $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- If both **B1** and **B2** hold, then $G/H \simeq \mathbb{Z}/6\mathbb{Z}$ and $H \simeq \mathbb{Z}/2\mathbb{Z}$. We have that one of **A** and **D** does not hold, hence K_7/K is an abelian extension with Galois group $G \simeq \mathbb{Z}/3\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

$d = 9$. The only holding conditions are **B1** and **C**. Then $H = \langle \phi_2 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ and $G/H \simeq \mathbb{Z}/3\mathbb{Z}$. We have $G \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

$d = 8$. If the degree d of the extension K_7/K is 8, then all the conditions hold but **B1** and **C**. Thus $H = \langle \tau_2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ and $G/H = \langle \psi_2^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. We have observed that τ_2 and ψ_2^3 do not commute, hence $G \simeq \mathbb{Z}/4\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \simeq \mathrm{D}_8$.

$d = 6$. If the degree d of the extension K_7/K is 6, then either **B1** or **C** holds and one of the other condition holds. In all cases the group G is isomorphic to $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d = 4$. If the degree d of the extension K_7/K is 4, then both **B1** and **C** do not hold.

- If **B2** does not hold, then G/H is trivial and $G = H = \langle \tau_2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$.
- If **B2** holds, then $G/H \simeq \mathbb{Z}/2\mathbb{Z}$ and G is isomorphic to the Klein group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d \leqslant 3$. If the degree d of the extension K_7/K is 3 or 2 or 1, obviously the Galois group is isomorphic to, respectively, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ or $\{\mathrm{Id}\}$.

8 Some applications

As mentioned in Sect. 1, we are going to describe some applications of the results produced in the previous sections.

8.1 A minimal bound for the local–global divisibility by 7

The first application concerns the following Local–Global question that was stated in [9] by Dvornicich and Zannier as a generalization of a particular case of the famous Hasse principle on quadratic forms (for further details one can see [6, 10, 11, 18, 19] among others; Dvornicich and the corresponding author also produced a survey [7] about this topic).

Problem 8.1 (Dvornicich, Zannier, 2001) Let K be a number field, M_K the set of the places v of K and K_v the completion of K at v. Let $\mathcal{G}$ be a commutative algebraic group defined over K. Fix a positive integer m and assume that there exists a K-rational point P in $\mathcal{G}$, such that $P = mD_v$, for some $D_v \in \mathcal{G}(K_v)$, for all but finitely many $v \in M_K$. Does there exist $D \in \mathcal{G}(K)$ such that $P = mD$?

We have stated the question in its original form, for all commutative algebraic groups, but from here on we will confine the discussion to elliptic curves $\mathcal{E}$ over K. It is a common method in local–global questions to translate the problem into a cohomological question. Dvornicich and Zannier stated the following definition of a subgroup of $H^1(G, \mathcal{E}[m])$ which encodes the hypotheses of the problem and whose triviality assures the validity of the local–global divisibility by m in $\mathcal{E}$ over K [9, Proposition 2.1]:

$$H^1_{\mathrm{loc}}(G, \mathcal{E}[m]) := \bigcap_{v \in \Sigma} \left(\ker H^1(G, \mathcal{E}[m]) \xrightarrow{\mathrm{res}_v} H^1(G_v, \mathcal{E}[m]) \right),$$

where Σ is the set of places of K unramified in $K(\mathcal{E}[m])$ and res_v is the usual restriction map.

The group $H^1_{\mathrm{loc}}(G, \mathcal{E}[m])$ is called *first local cohomology group* and gives an obstruction to the validity of this Hasse principle for divisibility of points by m in $\mathcal{E}$ over a finite extensions of K linearly disjoint from $K(\mathcal{E}[m])$ [10, Theorem 3]. Since every $v \in \Sigma$ is unramified in $K(\mathcal{E}[m])$, then G_v is a cyclic subgroup of G, for all $v \in \Sigma$. By the Chebotarev Density Theorem, the local Galois group G_v varies over *all* cyclic subgroups of G as v varies in $\varSigma$. Observe that indeed it suffices to take

$$H^1_{\text{loc}}(G, \mathcal{E}[m]) = \bigcap_{v \in S} \Big(\ker H^1(G, \mathcal{E}[m]) \xrightarrow{\text{res}_v} H^1(G_v, \mathcal{E}[m])\Big), \tag{1}$$

with S a subset of $\varSigma$ such that G_v varies over all cyclic subgroups of G as v varies in S. Observe that in particular we can choose a finite set S (on the contrary $\varSigma$ is not finite). In [9] the authors showed that the local–global divisibility by a prime number p holds in $\mathcal{E}$ over K (this was also proved in [26, Theorem 1] and a very similar statement was proved in [5, Lemma 6.1 and its corollary] and [4, Theorem 8.1]). In particular, the local–global divisibility by 7 holds in $\mathcal{E}$ over K. Thus, if we are able to find such a set S and prove that the local divisibility by 7 holds for $P \in \mathcal{E}(K)$, for all $v \in S$, then we get that P is globally divisible by 7, i.e. that P has a K-rational 7-divisor. So it suffices to have the local divisibility by 7 for a finite number of suitable places to get the global divisibility by 7. In [8], Dvornicich and the corresponding author produced an explicit effective version of the hypotheses of Problem 8.1 in all elliptic curves over number fields, by producing an explicit finite set S, for every positive integer m and every elliptic curve $\mathcal{E}$. Such an effective version is given by an upper bound $B(m, \mathcal{E})$ (depending on m and $\mathcal{E}$) to the places of K unramified in K_m, such that the validity of the local divisibility for all places less than $B(m, \mathcal{E})$ assures the global divisibility (in the cases when the Hasse principle for divisibility of points holds in $\mathcal{E}$ over K). With such a bound it is not necessary to take into account the distinctness of the Galois groups G_v in testing the local divisibility, since it is already assured by the density of places v that are considered. However, for this reason the cardinality of the set S produced in [8] is not as minimal as possible. It is indeed a very hard problem to obtain a similar result with an explicit set S of minimal cardinality (i.e. with the assumption that the local Galois groups G_v, corresponding to the places in S, are pairwise distinct), for all positive integers m. It is also a difficult problem just to find the minimal possible cardinality for S for every m. In view of the results achieved for the Galois groups $\text{Gal}(K_7/K)$ for the elliptic curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$, we give an answer to this last question when $m = 7$ for the curves of these families (in [17] an answer was given when $m = 5$ for the curves of the same families). For these curves we produce an upper bound to the cardinality of S which is surprisingly small and it is as minimal as possible when the degree $[K_7 : K]$ is maximum (i.e. $[K_7 : K] = 96$ for the curves in $\mathcal{F}_1$ and $[K_7 : K] = 72$ for the curves in $\mathcal{F}_2$). With the description of the Galois groups given in Sects. 4 and 7 and with the description of the cyclic subgroups of G given in the proofs of the following Theorems 8.2 and 8.3, one can easily deduce the minimal cardinality for S, for every $\mathcal{E}_1 \in \mathcal{F}_1$ and $\mathcal{E}_2 \in \mathcal{F}_2$.

Theorem 8.2 *Let $\mathcal{E}_1$ be an elliptic curve defined over a number field K, with Weierstrass equation $y^2 = x^2 + bx$, for some $b \in K$. There exist sets $S \subseteq M_K$ of cardinality $s \leqslant 18$ such that if $P = 7D_v$, with $D_v \in \mathcal{E}_1(K_v)$, for all $v \in S$, then $P = 7D$, for some $D \in \mathcal{E}_1(K)$. In particular, if $[K_7 : K] = 96$, then $s = 18$.*

Proof Let s be the number of distinct cyclic subgroups of G. As stated above, the set S can be chosen as a subset of M_K with cardinality s, such that G_v varies over all cyclic subgroups of G, as v varies in S, and G_v and G_w are pairwise distinct cyclic subgroups of G, for all $v, w \in S$, with $v \neq w$. It suffices to show that $s \leqslant 18$, i.e. that G has at most 18 cyclic subgroups. We have proved in Sect. 4, that for every $\mathcal{E}_1 \in \mathcal{F}_1$, the Galois group G is isomorphic to a subgroup of $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$. We keep the notation used in Sect. 4 for the generators of Q_{16} and $\mathbb{Z}/6\mathbb{Z}$, i.e. $Q_{16} = \langle \phi_1, \varphi_1 \,|\, \phi_1^2 = \varphi_1^4 = -\mathrm{Id}, \phi_1\varphi_1 = \varphi_1^{-1}\phi_1 \rangle$ and $\mathbb{Z}/6\mathbb{Z} = \langle \psi_1 \rangle$. The group Q_{16} has seven nontrivial cyclic subgroups: $\langle \varphi_1 \rangle \simeq \mathbb{Z}/8\mathbb{Z}$, $\langle -\mathrm{Id} \rangle = \langle \phi_1^2 \rangle = \langle \varphi_1^4 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and the five cyclic subgroups of order 4 generated respectively by $\phi_1, \varphi_1^2, \phi_1\varphi_1, \phi_1\varphi_1^2$ and $\phi_1\varphi_1^3$. We also have the nontrivial cyclic subgroups of $\mathbb{Z}/6\mathbb{Z}$, i.e $\langle \psi_1^3 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \psi_1^2 \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ and $\langle \psi_1 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$ itself. All of these groups are cyclic subgroups of G. In addition we have the group $\langle \varphi_1, \psi_1^2 \rangle \simeq \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/24\mathbb{Z}$, five copies of $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ given by the direct products of the five subgroups of order 4 of Q_{16} with $\langle \psi_1^2 \rangle$, the subgroup $\langle -\mathrm{Id}, \psi_1^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and the trivial group $\langle \mathrm{Id} \rangle$. Therefore $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$ contains 18 cyclic subgroups and every subgroup G of $Q_{16} \rtimes \mathbb{Z}/6\mathbb{Z}$ has at most 18 cyclic subgroups. Thus $s \leqslant 18$. In particular, if $[K_7 : K] = 96$, then G has exactly 18 cyclic subgroups and in this case $s = 18$ is sharp (in fact, if $s < 18$, then the hypotheses of Problem 8.1 are not satisfied). □

Theorem 8.3 *Let $\mathcal{E}_2$ be an elliptic curve defined over a number field K, with Weierstrass equation $y^2 = x^2 + c$, for some $c \in K$. There exist sets $S \subseteq M_K$ of cardinality $s \leqslant 15$ such that if $P = 7D_v$, with $D_v \in \mathcal{E}(K_v)$, for all $v \in S$, then $P = 7D$, for some $D \in \mathcal{E}(K)$. In particular, if $[K_7 : K] = 72$, then $s = 15$.*

Proof Let s be the number of distinct cyclic subgroups of G. By the discussion concerning the minimal possible cardinality of the set S in Eq. (1), we can choose S containing exactly s places v, such that G_v varies over all cyclic subgroups of G as v varies in S and G_v and G_w are pairwise distinct cyclic subgroups of G, for all $v, w \in S$, with $v \neq w$. We just have to show that G has at most 15 cyclic subgroups. As proved in Sect. 7, for every $\mathcal{E}_2 \in \mathcal{F}_2$, the Galois group G is isomorphic to a subgroup of $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$. In the notation of Sect. 7, a presentation of the group $\mathrm{Dic}_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$ is $\langle \phi_2, \tau_2 \,|\, \phi_2^3 = \tau_2^4 = \mathrm{Id}, \tau_2\phi_2 = \phi_2^{-1}\tau_2 \rangle$. We have six nontrivial cyclic subgroups of Dic_3: $\langle -\mathrm{Id} \rangle$, $\langle \phi_2 \rangle$, $\langle \tau_2 \rangle$, $\langle \tau_2\phi_2 \rangle = \langle \tau_2^3\phi_2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, $\langle \tau_2\phi_2^2 \rangle = \langle \tau_2^3\phi_2^2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, $\langle -\phi_2 \rangle = \langle -\phi_2^2 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$. We have three nontrivial cyclic subgroups of $\langle \psi_2 \rangle \simeq \mathbb{Z}/6\mathbb{Z}$, i.e. $\langle \psi_2 \rangle$, $\langle \psi_2^2 \rangle$, $\langle \psi_2^3 \rangle$. In addition, we have two other cyclic subgroups of $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$ that are isomorphic to $\mathbb{Z}/3 \times \mathbb{Z}/2\mathbb{Z}$, i.e. $\langle \phi_2, \psi_2^3 \rangle$, $\langle -\mathrm{Id}, \psi_2^2 \rangle$ and three subgroups isomorphic to $\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, i.e. $\langle \tau_2, \psi_2^2 \rangle$, $\langle \tau_2\phi_2, \psi_2^2 \rangle$, $\langle \tau_2\phi_2^2, \psi_2^2 \rangle$. Finally we have the trivial subgroup $\langle \mathrm{Id} \rangle$. Thus $\mathrm{Dic}_3 \rtimes \mathbb{Z}/6\mathbb{Z}$ has 15 cyclic subgroups and $s \leqslant 15$. In particular, if $[K_7 : K] = 72$, then G has exactly 15 cyclic subgroups and in this case the bound $s = 15$ is sharp. □

8.2 Remarks on modular curves

We are going to deduce some information about CM points on modular curves by the results produced about the fields K_7.

8.2.1 On CM points of modular curves

Let $\mathcal{H}$ be the complex upper half plane $\{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ via the Möbius trasformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}.$$

By Γ we denote a congruence group, i.e. a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ containing the *principal congruence group of level m*

$$\Gamma(m) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, A \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{m} \right\},$$

for some positive integer m. When m is minimal, the congruence group is said to be *of level m*. Important congruence groups of level m are

$$\Gamma_0(m) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{m} \right\},$$

and

$$\Gamma_1(m) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{m} \right\}.$$

The quotient $\mathcal{H}/\Gamma$ of $\mathcal{H}$ by the action of Γ, with the analytic structure induced by $\mathcal{H}$, is a Riemann surface, that is denoted by Y_Γ. The modular curve X_Γ, associated to Γ, is the compactification of Y_Γ by the addition of a finite number of cusps, i.e. the rational points corresponding to the orbits of $\mathbb{P}^1(\mathbb{Q})$ under Γ. The modular curves associated to the groups $\Gamma(m)$, $\Gamma_0(m)$ and $\Gamma_1(m)$ are denoted respectively by $X(m)$, $X_0(m)$ and $X_1(m)$. They are moduli spaces of families of elliptic curves with an extra structure of level m as follows (for further details see for example [13, 14, 23]):

(i) non-cuspidal points in $X_0(m)$ correspond to pairs $(\mathcal{E}, C_m)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and C_m is a cyclic subgroup of $\mathcal{E}[m]$ of order m;

(ii) non-cuspidal points in $X_1(m)$ correspond to pairs $(\mathcal{E}, P)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and P is a point of order m;

(iii) non-cuspidal points in $X(m)$ correspond to triples $(\mathcal{E}, P, Q)$, where $\mathcal{E}$ is an elliptic curve (defined over $\mathbb{C}$) and P, Q are points of order m generating $\mathcal{E}[m]$.

A *CM point* on a modular curve is a point which corresponds to an elliptic curve with complex multiplication. For every modular curve X, we denote by $X(K)_{\mathrm{CM}}$ the set of its K-rational CM points.

From what we have shown in the previous sections we can deduce the following facts (see in particular Theorem 5.1).

Proposition 8.4 *Let K be a number field. Let δ_j and P_j be as in Sect. 5, for $1 \leqslant j \leqslant 8$, and let $\mathcal{E}_{2,j,\gamma} : y^2 = x^3 + c_{j,\gamma}$, with $c_{j,\gamma} := \delta_j^2(\delta_j + 1)^3\gamma^6$, for some $\gamma \in \mathbb{Q}$. If $\mathbb{Q}(\zeta_3, \zeta_7) \subseteq K$, then*

(i) *The pairs* $(\mathcal{E}_{2,j,\gamma}, P_j)$, $(\mathcal{E}_{2,j,\gamma}, \langle P_j\rangle)$, *with* $1 \leqslant j \leqslant 8$, *define* K*-rational CM points on* $X_1(7)$ *and respectively on* $X_0(7)$.

(ii) *The triples* $(\mathcal{E}_{2,j,\gamma}, P_j, \phi_2(P_j))$, *with* $1 \leqslant j \leqslant 8$, *define* K*-rational CM points on* $X(7)$.

(iii) *In particular* $X_0(7)(K)_{\mathrm{CM}} \neq \emptyset$, $X_1(7)(K)_{\mathrm{CM}} \neq \emptyset$ *and* $X(7)(K)_{\mathrm{CM}} \neq \emptyset$.

Proof If $1 \leqslant j \leqslant 6$, then $c_{j,\gamma}, \sqrt[3]{\delta_j c_{j,\gamma}}, \sqrt{\delta_j c_{j,\gamma}} \in \mathbb{Q}(\zeta_3, \zeta_7)$. Since $\mathbb{Q}(\zeta_3, \zeta_7) \subseteq K$, then the pairs $(\mathcal{E}_{2,j,\gamma}, P_j)$ and $(\mathcal{E}_{2,j,\gamma}, \langle P_j\rangle)$, for $1 \leqslant j \leqslant 6$, define K-rational CM points of $X_1(7)$ and respectively of $X_0(7)$. Furthermore, the triples $(\mathcal{E}_{2,j,\gamma}, P_j, \phi_2(P_j))$ define K-rational CM points on $X(7)$.

If $j \in \{7, 8\}$, then $c_{j,\gamma} \in \mathbb{Q}(\zeta_3)$. We also have that $\sqrt[3]{\delta_j c_{j,\gamma}} = \delta_j(\delta_j+1)\gamma^2 \in \mathbb{Q}(\zeta_3)$ and $\sqrt{\delta_j c_{j,\gamma}} = \delta_j(\delta_j + 1)^2\gamma^3 \in \mathbb{Q}(\zeta_3)$. Owing to $\mathbb{Q}(\zeta_3, \zeta_7) \subseteq K$, then the pairs $(\mathcal{E}_{2,j,\gamma}, P_j)$ and $(\mathcal{E}_{2,j,\gamma}, \langle P_j\rangle)$ define K-rational CM points of $X_1(7)$ and respectively of $X_0(7)$. Furthermore, the triples $(\mathcal{E}_{2,j,\gamma}, P_j, \phi_2(P_j))$ define K-rational CM points on $X(7)$. □

Moreover, from the results proved in Sects. 2 and 5, we can immediately deduce the following propositions.

Proposition 8.5 *Let* K *be an extension of* $\mathbb{Q}(i, \zeta_7)$. *Let* $\mathcal{E}_1 \in \mathcal{F}_1$ *and let* $P \in \mathcal{E}_1[7]$ *such that* $\{P, iP\}$ *is a generating set of* $\mathcal{E}_1[7]$. *Then*

(i) *the pair* $(\mathcal{E}_1, \langle P\rangle)$ *defines a non-cuspidal* K*-rational CM point of* $X_0(7)$ *if and only if* $y(P) \in K$;

(ii) *the pair* $(\mathcal{E}_1, P)$ *defines a non-cuspidal* K*-rational CM point of* $X_1(7)$ *if and only if* $y(P) \in K$;

(iii) *the triple* $(\mathcal{E}_1, P, iP)$ *defines a non-cuspidal* K*-rational CM point of* $X(7)$ *if and only if* $y(P) \in K$.

Proposition 8.6 *Let* K *be an extension of* $\mathbb{Q}(\zeta_3, \zeta_7)$. *Let* $\mathcal{E}_2 \in \mathcal{F}_2$ *and let* $P \in \mathcal{E}_2[7]$ *be such that* $\{P, \phi_2(P)\}$ *is a generating set of* $\mathcal{E}_2[7]$. *Then*

(i) *the pair* $(\mathcal{E}_2, \langle P\rangle)$ *defines a non-cuspidal* K*-rational CM point of* $X_0(7)$ *if and only if* $y(P) \in K$;

(ii) *the pair* $(\mathcal{E}_2, P)$ *defines a non-cuspidal* K*-rational CM point of* $X_1(7)$ *if and only if* $y(P) \in K$;

(iii) *the triple* $(\mathcal{E}_2, P, \phi_2(P))$ *defines a non-cuspidal* K*-rational CM point of* $X(7)$, *if and only if* $y(P) \in K$.

Acknowledgements We thank the anonymous referees for their valuable comments and suggestions that allow us to improve our paper.

Funding Open access funding provided by Universitá della Calabria within the CRUI-CARE Agreement.

References

1. Bandini, A.: Three-descent and the Birch and Swinnerton–Dyer conjecture. Rocky Mountain J. Math. **34**(1), 13–27 (2004)
2. Bandini, A., Paladino, L.: Number fields generated by the 3-torsion points of an elliptic curve. Monatsh. Math. **168**(2), 157–181 (2012)
3. Bandini, A., Paladino, L.: Fields generated by torsion points of elliptic curves. J. Number Theory **169**, 103–133 (2016)
4. Cassels, J.W.S.: Arithmetic on curves of genus 1. III. The Tate–Šafarevič and Selmer groups. Proc. Lond. Math. Soc. **12**, 259–296 (1962)
5. Cassels, J.W.S.: Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung. J. Reine Angew. Math. **211**, 95–112 (1962)
6. Creutz, B.: On the local-global principle for divisibility in the cohomology of elliptic curve. Math. Res. Lett. **23**(2), 377–387 (2016)
7. Dvornicich, R., Paladino, L.: Local-global questions for divisibility in commutative algebraic groups. Eur. J. Math. **8**(suppl. 2), S599–S628 (2022)
8. Dvornicich, R., Paladino, L.: On the division fields of an elliptic curve and an effective bound to the hypotheses of the local-global divisibility. Int. J. Number Theory **18**(7), 1567–1590 (2022)
9. Dvornicich, R., Zannier, U.: Local-global divisibility of rational points in some commutative algebraic groups. Bull. Soc. Math. France **129**(3), 317–338 (2001)
10. Dvornicich, R., Zannier, U.: On local-global principle for the divisibility of a rational point by a positive integer. Bull. London Math. Soc. **39**(1), 27–34 (2007)
11. Gillibert, F., Ranieri, G.: On the local-global divisibility over abelian varieties. Ann. Inst. Fourier (Grenoble) **68**(2), 847–873 (2018)
12. González-Jiménez, E., Lozano-Robledo, Á.: Elliptic curves with abelian division fields. Math. Z. **283**(3–4), 835–859 (2016)
13. Katz, N.M., Mazur, B.: Arithmetic Moduli of Elliptic Curves. Annals of Mathematics Studies, vol. 108. Princeton Univrsity Press, Princeton (1985)
14. Knapp, A.W.: Elliptic Curves. Mathematical Notes, vol. 40. Princeton University Press, Princeton (1992)
15. Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. **124**(1–3), 437–449 (1996)
16. Paladino, L.: Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9. J. Théor. Nombres Bordeaux **22**(1), 138–160 (2010)
17. Paladino, L.: On 5-torsion of CM elliptic curves. Riv. Mat. Univ. Parma (N.S.) **9**(2), 329–350 (2018)
18. Paladino, L.: Divisibility questions in commutative algebraic groups. J. Number Theory **205**, 210–245 (2019)
19. Paladino, L., Ranieri, G., Viada, E.: On minimal set for counterexamples to the local-global principle. J. Algebra **415**, 290–304 (2014)
20. Rebolledo Hochart, M.: Field generated by the 13-torsion points of elliptic curves. Acta Arith. **109**(3), 219–230 (2003)
21. Schaefer, E.F., Stoll, M.: How to do a p-descent on an elliptic curve. Trans. Amer. Math. Soc. **356**(3), 1209–1231 (2004)
22. Sharma, D.: Locally indecomposable Galois representations with full residual images. Int. J. Number Theory **13**(5), 1191–1211 (2015)
23. Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions. Princeton University Press, Princeton (1994)
24. Silverman, J.H.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, vol. 106, 2nd edn. Springer, Dordrecht (2009)
25. Silverman, J.H.: Advanced Topic in Elliptic Curves. Graduate Texts in Mathematics, vol. 151. Springer, New York (1994)
26. Wong, S.: Power residues on abelian varieties. Manuscripta Math. **102**(1), 129–138 (2000)
27. Yelton, J.: A note on 8-division fields of elliptic curves. Eur. J. Math. **3**(3), 603–613 (2017)