Riv. Mat. Univ. Parma, Vol. **9** (2018), 329-350

Laura Paladino

On 5-torsion of CM elliptic curves

Abstract. Let $\mathcal{E}$ be an elliptic curve defined over a number field K. Let m be a positive integer. We denote by $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$ and by $K_m := K(\mathcal{E}[m])$ the field obtained by adding to K the coordinates of the points of $\mathcal{E}[m]$. We describe the fields K_5, when $\mathcal{E}$ is a CM elliptic curve defined over K, with Weiestrass form either $y^2 = x^3 + bx$ or $y^2 = x^3 + c$. In particular we classify the fields K_5 in terms of generators, degrees and Galois groups. Furthermore we show some applications of those results to the Local-Global Divisibility Problem and to modular curves.

Keywords. Elliptic curves, complex multiplication, torsion points.

Mathematics Subject Classification (2010): 11G05, 11F80, 11G18.

Contents

Received: August 4, 2018; accepted in revised form: December 17, 2018.

1 - Introduction

Let $\mathcal{E}$ be an elliptic curve defined over a number field K. We denote by $\overline{K}$ the algebraic closure of K. Let m be a positive integer. We denote by $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$ and by $K_m := K(\mathcal{E}[m])$ the field generated by the m-torsion points of $\mathcal{E}$, i.e. the field obtained by adding to K the coordinates of the points of $\mathcal{E}[m]$. It is well-known that K_m/K is a Galois extension, whose Galois group we denote by G. For every point $P \in \mathcal{E}$, we indicate by $x(P)$, $y(P)$ its coordinates. Furthermore, for every positive integer n, we indicate the n-th multiple of P by nP. It is well-known that $\mathcal{E}[m] \simeq (\mathbb{Z}/m\mathbb{Z})^2$. Let $\{P_1, P_2\}$ be a $\mathbb{Z}$-basis for $\mathcal{E}[m]$; thus $K_m = K(x(P_1), x(P_2), y(P_1), y(P_2))$. To ease notation, we put $x_i := x(P_i)$ and $y_i := y(P_i)$ $(i = 1, 2)$. Knowing explicit generators for K_m could have a lot of interesting applications, for instance about Galois representations, local-global problems on elliptic curves (see [**15**] and [**16**]), descent problems (see for example [**20**] and the particular cases [**2**] and [**3**]), points on modular curves (see [**4**], [**5**]) and points on Shimura curves. The Shimura curves are moduli spaces of abelian surfaces $\mathcal{A}$ with some extra structures, where $\mathcal{A}$ is simple or $\mathcal{A} = \mathcal{E} \times \mathcal{E}$, for some CM elliptic curve $\mathcal{E}$ (see Remark 8.1). So the elliptic curves with complex multiplication are particularly interesting since their squares (with some extra structures) correspond to points on certain Shimura curves. In the literature there are not many papers about fields generated by m-torsion points of elliptic curves (see also [**1**] and [**14**]). A recent and very interesting paper about number fields $\mathbb{Q}(\mathcal{E}[m])$ is [**11**]. The discussion there is restricted to the case when $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is an abelian extension, even for CM elliptic curves. Among other results, in particular the authors prove that if $\mathcal{E}$ is an elliptic curve with complex multiplication and $\mathbb{Q}(\mathcal{E}[m])/\mathbb{Q}$ is abelian, then $m \in \{2, 3, 4\}$. In this paper we will describe all possible extensions (even not abelian) $K(\mathcal{E}[5])/K$, for every K, when $\mathcal{E}$ is a CM elliptic curve with Weierstrass form $y^2 = x^3 + bx$ or $y^2 = x^3 + c$, for some $b, c \in K$. We will classify them in terms of generators, degree and Galois groups.

By Artin's primitive element theorem, we know that the extension K_m/K is monogeneous and one can find a single generator for K_m/K by combining the above coordinates. Anyway, in general it is not easy to find this single generator.

So, during the last few years we have searched for systems of generators easier to be found and to be used in applications. For every m, by the properties of the Weil pairing e_m, we have that the image $\zeta_m := e_m(P_1, P_2) \in K_m$ is a primitive m-th root of unity and that $K(\zeta_m) \subseteq K_m$ (see for instance [**23**]). When m is odd, a generating set for K_m is showed in the following statement (see [**5**]).

Theorem 1.1. *In the above notations, we have*

$$K_m = (x_1, \zeta_m, y_2), \tag{1}$$

for all odd integers m.

Of course, in general it is easier to work with the generating set as in (1). Furthermore, that generating set is often minimal among the subsets of $\{x_1, x_2, \zeta_m, y_1, y_2\}$ (for further details see [**5**]). For $m = 3$ and $m = 4$ there are explicit descriptions of all possible fields K_3 and K_4, in terms of generators, degrees and Galois groups (see in particular [**5**] and also [**4**]). Here we give a similar classification of every possible field K_5, for all elliptic curves with complex multiplication, belonging to the families:

$$\mathcal{F}_1 : y^2 = x^3 + bx, \quad \text{with } b \in K \qquad \text{and} \qquad \mathcal{F}_2 : y^2 = x^3 + c, \quad \text{with } c \in K.$$

In the last part of the paper, we show some applications to the Local-Global Divisibility Problem and to CM points of modular curves.

2 - Generators of $K(\mathcal{E}[5])$ for elliptic curves $y^2 = x^3 + bx$

If $\mathcal{E}$ is an elliptic curve defined over K, with Weierstrass form $y^2 = x^3+bx+c$, then the abscissas of the points of order 5 of $\mathcal{E}$ are the roots of the polynomial

$$\begin{aligned} p_5(x) := &-5x^{12} - 62bx^{10} - 380cx^9 + 105b^2x^8 - 240bcx^7 + (240c^2 + 300b^3)x^6 \\ &+ 696b^2cx^5 + (1920bc^2 + 125b^4)x^4 + (1600c^3 + 80b^3c)x^3 \\ &+ (240b^2c^2 + 50b^5)x^2 + (640bc^3 + 100b^4c)x + 256c^4 + 32b^3c^2 - b^6. \end{aligned}$$

If $\mathcal{E}_1 : y^2 = x^3 + bx$ is an elliptic curve of the family $\mathcal{F}_1$, then the abscissas of the points of order 5 of $\mathcal{E}$ are the roots of the polynomial

$$q_5(x) := -5x^{12} - 62bx^{10} + 105b^2x^8 + 300b^3x^6 + 125b^4x^4 + 50b^5x^2 - b^6.$$

Over $K(\zeta_5)$ we have

$$\begin{aligned} q_5(x) = &-5 \cdot \left(x^4 + (-8\zeta_5^3 - 8\zeta_5^2 + 2)bx^2 + (-8\zeta_5^3 - 8\zeta_5^2 + 5)\, b\right) \\ &\cdot \left(x^4 + \frac{2}{5}bx^2 + \frac{1}{5}b^2\right) \cdot \left(x^4 + (8\zeta_5^3 + 8\zeta_5^2 + 10)bx^2 + (8\zeta_5^3 + 8\zeta_5^2 + 13)\, b\right) \end{aligned}$$

and over $K(i,\zeta_5)$ we have

$$\begin{aligned}q_5(x) = -5 &\cdot \big(x^2 + ((-4i+4)\zeta_5^3 + 4\zeta_5^2 - 4i\zeta_5 - 2i + 5)\, b\big)\\ &\cdot \big(x^2 + (-4\zeta_5^3 + (-4i-4)\zeta_5^2 - 4i\zeta_5 - 2i + 1)\, b\big)\\ &\cdot \big(x^2 + ((4i+4)\zeta_5^3 + 4\zeta_5^2 + 4i\zeta_5 + 2i + 5)\, b\big)\\ &\cdot \big(x^2 + (-4\zeta_5^3 + (4i-4)\zeta_5^2 + 4i\zeta_5 + 2i + 1)\, b\big)\\ &\cdot \left(x^2 + \frac{1-2i}{5}\, b\right) \cdot \left(x^2 + \frac{1+2i}{5}\, b\right),\end{aligned}$$

where as usual we denote by i a root of $x^2+1=0$.

Let

$$\begin{aligned}\theta_1 &:= -((-4i+4)\zeta_5^3 + 4\zeta_5^2 - 4i\zeta_5 - 2i + 5);\\ \theta_2 &:= -(-4\zeta_5^3 + (-4i-4)\zeta_5^2 - 4i\zeta_5 - 2i + 1);\\ \theta_3 &:= -((4i+4)\zeta_5^3 + 4\zeta_5^2 + 4i\zeta_5 + 2i + 5);\\ \theta_4 &:= -(-4\zeta_5^3 + (4i-4)\zeta_5^2 + 4i\zeta_5 + 2i + 1);\\ \omega_1 &:= -\frac{1-2i}{5}\, b;\\ \omega_2 &:= -\frac{1+2i}{5}\, b.\end{aligned}$$

By the factorization of $q_5(x)$ showed above, one can verify that the 24 points of exact order 5 of $\mathcal{E}_1$ are the following:

$$\begin{aligned}
&\pm P_1 := (x_1, \pm y_1) = \left(\sqrt{\theta_1 b}, \pm\sqrt{(\theta_1+1)b\sqrt{\theta_1 b}}\right) && \pm\, iP_1 := (-x_1, \pm iy_1);\\
&\pm P_2 := (x_2, \pm y_2) = \left(\sqrt{\theta_2 b}, \pm\sqrt{(\theta_2+1)b\sqrt{\theta_2 b}}\right) && \pm\, iP_2 := (-x_2, \pm iy_2);\\
&\pm P_3 := (x_3, \pm y_3) = \left(\sqrt{\theta_3 b}, \pm\sqrt{(\theta_3+1)b\sqrt{\theta_3 b}}\right) && \pm\, iP_3 := (-x_3, \pm iy_3);\\
&\pm P_4 := (x_4, \pm y_4) = \left(\sqrt{\theta_4 b}, \pm\sqrt{(\theta_4+1)b\sqrt{\theta_4 b}}\right) && \pm\, iP_4 := (-x_4, \pm iy_4);\\
&\pm P_5 := (x_5, \pm y_5) = \left(\sqrt{\omega_1 b}, \pm\sqrt{(\omega_1+1)b\sqrt{\omega_1 b}}\right) && \pm\, iP_5 := (-x_5, \pm iy_5);\\
&\pm P_6 := (x_6, \pm y_6) = \left(\sqrt{\omega_2 b}, \pm\sqrt{(\omega_2+1)b\sqrt{\omega_2 b}}\right) && \pm\, iP_6 := (-x_6, \pm iy_6).
\end{aligned}$$

We will denote by ϕ_1 the complex multiplication of $\mathcal{E}_1$, i.e. $\phi_1(x,y) = (-x, iy)$, for every point $P=(x,y)\in\mathcal{E}_1$. Moreover, to ease notation, we will denote by iP the point $\phi_1(P) = (-x, iy)$.

Remark 2.1. In many cases if P is a nontrivial m-torsion point, then $\phi_1(P)$ is a m-torsion point that is not a multiple of P. Then a basis for $\mathcal{E}[m]$ is given by $\{P, \phi_1(P)\}$. Anyway, in a few special cases the point $\phi_1(P)$ is a multiple of P. For instance $\phi_1(P_j) = 2P_j$, for $j \in \{5, 6\}$; then $\{P_j, \phi_1(P_j)\}$ is not a basis of $\mathcal{E}_1[5]$, for $j \in \{5, 6\}$. We would not have this problem by choosing a root of $q_5(x)$ different from x_5 and x_6 (as we will see in the proof of the next theorem).

Theorem 2.1. *For $1 \leqslant j \leqslant 4$, let θ_j be as above. Then*

$$K_5 = K\left(i, \zeta_5, \sqrt{(\theta_j + 1)b\sqrt{\theta_j b}}\right).$$

Proof. For every point $P \in \mathcal{E}_1[5]$, let $\langle P \rangle$ denote the subgroup of $\mathcal{E}_1[5]$ generated by P. Since $5P = 0$, then $\langle P \rangle = \{P, 2P, -2P, -P, O\}$. Thus it suffices to show that $x(2P_j) \neq x(iP_j)$, for some $1 \leqslant j \leqslant 4$, to have that $\{P_j, \phi_1(P_j)\}$ is a generating set for $\mathcal{E}_1[5]$. With a bit of computation, one can verify that $x(2P_1) = x_3$ and $x(2P_2) = x_4$. Therefore, for every $1 \leqslant j \leqslant 4$, the point $\phi_1(P_j)$ is not a multiple of P_j and $\{P_j, \phi_1(P_j)\}$ is a basis of $\mathcal{E}_1[5]$. Furthermore observe that $\sqrt{\theta_j b} \in K\left(i, \zeta_5, \sqrt{(\theta_j + 1)b\sqrt{\theta_j b}}\right)$. Then the conclusion follows by Remark 2.1 and Theorem 1.1. □

Remark 2.2. We give another proof that $x(2P_j) \neq x(iP_j)$ implies $K_5 = K\left(i, \zeta_5, \sqrt{(\theta_j + 1)b\sqrt{\theta_j b}}\right)$ (for every $1 \leqslant j \leqslant 4$). Note that $\phi_1(P) = nP$, for some positive integer $1 \leqslant n \leqslant 4$, if and only if $(\phi_1 - n)P = 0$. Since $P \in \mathcal{E}_1[5]$ and the ring of automorphisms of $\mathcal{E}_1$ is $\mathbb{Z}[i]$, we should have that $i - n$ divides 5 in $\mathbb{Z}[i]$. The only possibilities for n are ±2, because $(2 + i)(2 - i) = 5$.

3 - Degrees $[K_5 : K]$ for the curves of $\mathcal{F}_1$

To ease the notation, from now on we will fix the generating set $\{P_1, \phi_1(P_1)\}$ for $\mathcal{E}_1[5]$. Thus $K_5 = K(i, \zeta_5, \sqrt{(\theta_1 + 1)b\sqrt{\theta_1 b}})$. Clearly, such a choice is without loss of generalization and all the results that we are going to show about the degree $[K_5 : K]$ and the Galois group $\mathrm{Gal}(K_5/K)$, hold as well for every other generating set $\{i, \zeta_5, \sqrt{(\theta_j + 1)b\sqrt{\theta_j b}}\}$ of the extension K_5/K, with $2 \leqslant j \leqslant 4$.

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

A. $i \notin K$;	**C.** $\sqrt{\theta_1 b} \notin K(i, \zeta_5)$;
B1. $\zeta_5 + \zeta_5^{-1} \notin K$;	**D.** $\sqrt{(\theta_1+1)b\sqrt{\theta_1 b}} \notin K(i, \zeta_5, \sqrt{\theta_1 b})$.
B2. $\zeta_5 \notin K(\zeta_5 + \zeta_5^{-1})$;	

The possible degrees of the extension K_5/K are the following

Table 1.

d	holding conditions	d	holding conditions
32	**A**, **B1**, **B2**, **C**, **D**	4	2 *among* **A**, **B1**, **B2**, **C**, **D**
16	4 *among* **A**, **B1**, **B2**, **C**, **D**	2	1 *among* **A**, **B1**, **B2**, **C**, **D**
8	3 *among* **A**, **B1**, **B2**, **C**, **D**	1	*no holding conditions*

Proof. Consider the tower of extensions

$$K \subseteq K(i) \subseteq K(i, \zeta_5 + \zeta_5^{-1}) \subseteq K(i, \zeta_5)$$
$$\subseteq K(i, \zeta_5, \sqrt{\theta_1 b}) \subseteq K(i, \zeta_5, \sqrt{(\theta_1+1)b\sqrt{\theta_1 b}}).$$

The degree of K_5/K is the product of the degrees of the intermediate extensions appearing in the tower. Clearly each of those extensions gives a contribution to the degree less than or equal to 2. The final computation is straightforward. □

Observe that $[K_5 : K] \leqslant 32$ is in accordance with the fact that $\mathcal{E}_1$ has complex multiplication and then the Galois representation

$$\rho_{\mathcal{E}_1,5} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

is not surjective.

4 - Galois groups $\mathrm{Gal}(K_5/K)$ for the curves of $\mathcal{F}_1$

Let $\mathcal{E}_1$ be a curve of the family $\mathcal{F}_1$, let $G := \mathrm{Gal}(K(\mathcal{E}_1[5])/K)$ and let $d := |G|$. By the observations made in the previous sections about the generators of K_5 and about the degree $[K_5 : K]$, we have that G is generated by the following 3 automorphisms.

i) The automorphism ϕ_1 of order 4 given by complex multiplication. We have $\phi_1(P_j) = iP_j$, for all $1 \leqslant j \leqslant 6$. Observe that $\phi_1^2 = -\mathrm{Id}$.

ii) The automorphism ψ_1 of order 4 mapping ζ_5 to ζ_5^2. Note that

$$P_1 \overset{\psi_1}{\longmapsto} P_2 \overset{\psi_1}{\longmapsto} P_3 \overset{\psi_1}{\longmapsto} P_4 \overset{\psi_1}{\longmapsto} P_1,$$

as well as

$$iP_1 \overset{\psi_1}{\longmapsto} iP_2 \overset{\psi_1}{\longmapsto} iP_3 \overset{\psi_1}{\longmapsto} iP_4 \overset{\psi_1}{\longmapsto} iP_1.$$

The other 5-torsion points of $\mathcal{E}_1$ are fixed by ψ_1.

iii) The automorphism ρ_1 of order 2 sending i to $-i$. Observe that

$$\begin{aligned} x_1 = \sqrt{\theta_1 b} &= \sqrt{-((-4i+4)\zeta_5^3 + 4\zeta_5^2 - 4i\zeta_5 - 2i + 5)b} \\ &= i\sqrt{((-4i+4)\zeta_5^3 + 4\zeta_5^2 - 4i\zeta_5 - 2i + 5)b}, \end{aligned}$$

consequently

$$\begin{aligned} \rho_1(x_1) &= -i\sqrt{((4i+4)\zeta_5^3 + 4\zeta_5^2 + 4i\zeta_5 + 2i + 5)b} \\ &= -\sqrt{-((4i+4)\zeta_5^3 + 4\zeta_5^2 + 4i\zeta_5 + 2i + 5)b} \\ &= -\sqrt{\theta_3 b} \ = -x_3 \end{aligned}$$

and then

$$\rho_1(y_1) = \sqrt{-(\theta_3 + 1)\sqrt{\theta_3 b}} = i\sqrt{(\theta_3 + 1)\sqrt{\theta_3 b}} = iy_3.$$

Thus ρ_1 swaps P_1 and iP_3. Moreover one can verify that ρ_1 swaps P_2 and iP_4, P_5 and P_6. We have

$$\begin{array}{ll} P_1 \xleftrightarrow{\rho_1} iP_3 & \qquad iP_1 \xleftrightarrow{\rho_1} P_3; \\ P_2 \xleftrightarrow{\rho_1} iP_4 & \qquad iP_2 \xleftrightarrow{\rho_1} P_4; \\ P_5 \xleftrightarrow{\rho_1} P_6 & \qquad iP_6 \xleftrightarrow{\rho_1} -iP_5. \end{array}$$

Observe that one can also calculate the images of the 3 generators ζ_5, i and y_1 of the extension K_5/K via the homomorphisms ϕ_1, ψ_1 and ρ_1 (instead of working with the points) to describe $\mathrm{Gal}(K_5/K)$. By [**24**, Chapter II, Theorem 2.3], the extension $K_5/K(i)$ is abelian, thus $\langle \phi_1, \psi_1 \rangle \simeq \mathbb{Z}/4 \times \mathbb{Z}/4$ when all the conditions in the statement of Theorem 2.1 hold. Moreover, with a quick computation, one verifies that ψ_1 and ρ_1 commute. On the contrary ϕ_1 and ρ_1 do not commute in general, in fact

$$\rho_1\phi_1((x_1, y_1)) = \rho_1((-x_1, iy_1)) = (x_3, y_3) = P_3;$$

and

$$\phi_1\rho_1((x_1, y_1)) = \phi_1((-x_3, iy_3)) = (x_3, -y_3) = -P_3.$$

Instead we have $\rho_1\phi_1((P_1)) = \phi_1^{-1}\rho_1((P_1))$ and $\rho_1\phi_1((iP_1)) = \phi_1^{-1}\rho_1((iP_1))$. Being $\{P_1, iP_1\}$ a generating set for K_5, we can conclude $\rho_1\phi_1 = \phi_1^{-1}\rho_1$. Thus, when all the conditions hold, we have $\langle\phi_1, \rho_1\rangle \simeq D_8$, where, for every positive integer n, we denote the dihedral group of order $2n$ by D_{2n}. We are going to describe the Galois groups $G = \mathrm{Gal}(K_5/K)$, with respect to the degrees $[K_5 : K]$.

$d = 32$ If the degree d of the extension K_5/K is 32, then all the conditions hold. We have $G = \langle\phi_1, \psi_1, \rho_1 | \phi_1^4 = \psi_1^4 = \rho_1^2 = \mathrm{Id}, \phi_1\psi_1 = \psi_1\phi_1, \rho_1\psi_1 = \psi_1\rho_1, \phi_1\rho_1 = \phi_1^{-1}\rho_1\rangle \simeq D_8 \times \mathbb{Z}/4\mathbb{Z}$.

$d = 16$ If the degree d of the extension K_5/K is 16, then only one condition does not hold.

If **A** does not hold, then ρ_1 fixes K_5 and we have an abelian group $G = \langle\phi_1, \psi_1\rangle \simeq \mathbb{Z}/4 \times \mathbb{Z}/4$.

If one among **B1** and **B2** does not hold, then $G \simeq D_8 \times \mathbb{Z}/2\mathbb{Z}$.

If one among **C** and **D** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

$d = 8$ If the degree d of the extension K_5/K is 8, then two conditions do not hold.

If **B1** and **B2** do not hold, then $G = \langle\phi_1, \rho_1\rangle \simeq D_8$. This is the only case in which the Galois group G has order 8 and it is not abelian.

If **A** does not hold and one among **B1** and **B2** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If **A** does not hold and one among **C** and **D** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ again.

If one among **B1** and **B2** does not hold and one among **C** and **D** does not hold then $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

$d = 4$ If the degree d of the extension K_5/K is 4, then three conditions do not hold. If both **B1** and **B2** hold or if both **C** and **D** hold, then $G \simeq \mathbb{Z}/4\mathbb{Z}$. Otherwise $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$d \leqslant 2$ If the degree d of the extension K_5/K is either 2 or 1, clearly the Galois group is respectively $\mathbb{Z}/2\mathbb{Z}$ or $\{\mathrm{Id}\}$.

5 - Generators of $K(\mathcal{E}[5])$ for elliptic curves $y^2 = x^3 + c$

Let $\mathcal{E}_2 : y^2 = x^3 + c$ be an elliptic curve of the family $\mathcal{F}_2$.

Remark 5.1. Let ϕ_2 denote the complex multiplication of $\mathcal{E}_2$, i.e. $\phi_2(x,y) = (\zeta_3 x, y)$. In many cases, if P is a nontrivial m-torsion point, then $\phi_2(P)$ is an m-torsion point that is not a multiple of P. Then a basis for $\mathcal{E}[m]$ is given by $\{P, \phi_2(P)\}$ and $K_m = K(x(P), y(P), \zeta_3)$. For elliptic curves with complex multiplication ϕ_2, a generating set $\{x(P), y(P), \zeta_3\}$ is often easier to adopt than the one in (1). Anyway, in a few special cases, the point $\phi_2(P)$ is a multiple of P. For example, the abscissas of the 3-torsion points of $\mathcal{E}_2$ are

$$x_1 = 0; \quad x_2 = \sqrt[3]{-4c}; \quad x_3 = \zeta_3 x_2; \quad x_4 = \zeta_3^2 x_2.$$

Let P_1 be a point of abscissas x_1. Clearly $\phi_2(P_1) = P_1$ and then $\{P_1, \phi_2(P_1)\}$ is not a basis of $\mathcal{E}_2[3]$. On the other hand, $\{P_h, \phi_2(P_h)\}$ is a basis of $\mathcal{E}_2[3]$, for $2 \leqslant h \leqslant 4$. So in general we have to be careful in our choice of P, when we use such a basis $\{P, \phi_2(P)\}$. Anyway, the point $\phi_2(P)$ is not a multiple of P, for every P of exact order 5, as we will see in the proof of Theorem 5.1.

The abscissas of the points of order 5 of $\mathcal{E}_2$ are the roots of the polynomial

$$r_5(x) := -5x^{12} - 380cx^9 + 240c^2x^6 + 1600c^3x^3 + 256c^4.$$

Over $K(\zeta_5)$ we have

$$r_5(x) = -5 \cdot \left(x^6 + (-36\zeta_5^3 - 36\zeta_5^2 + 20)cx^3 + \frac{-288\zeta_5^3 - 288\zeta_5^2 + 176}{5}c^2\right)$$
$$\cdot \left(x^6 + (36\zeta_5^3 + 36\zeta_5^2 + 56)cx^3 + \frac{288\zeta_5^3 - 288\zeta_5^2 + 464}{5}c^2\right)$$

and over $K(\zeta_3, \zeta_5)$ we have

$$r_5(x) =$$
$$-5 \cdot \left(x^3 + \frac{(-132\zeta_3 + 24)\zeta_5^3 + (36\zeta_3 + 108)\zeta_5^2 + (-96\zeta_3 - 48)\zeta_5 - 48\zeta_3 + 116}{5}c\right)$$
$$\cdot \left(x^3 + \frac{(-36\zeta_3 - 108)\zeta_5^3 + (-132\zeta_3 - 156)\zeta_5^2 + (-168\zeta_3 - 84)\zeta_5 - 84\zeta_3 + 8}{5}c\right)$$
$$\cdot \left(x^3 + \frac{(132\zeta_3 + 156)\zeta_5^3 + (-36\zeta_3 + 72)\zeta_5^2 + (96\zeta_3 + 48)\zeta_5 + 48\zeta_3 + 164}{5}c\right)$$
$$\cdot \left(x^3 + \frac{(36\zeta_3 - 72)\zeta_5^3 + (132\zeta_3 - 24)\zeta_5^2 + (168\zeta_3 + 84)\zeta_5 + 84\zeta_3 + 92}{5}c\right).$$

Let

$$
\begin{aligned}
\delta_1 &:= -\frac{(-132\zeta_3+24)\zeta_5^3+(36\zeta_3+108)\zeta_5^2+(-96\zeta_3-48)\zeta_5-48\zeta_3+116}{5};\\
\delta_2 &:= -\frac{(-36\zeta_3-108)\zeta_5^3+(-132\zeta_3-156)\zeta_5^2+(-168\zeta_3-84)\zeta_5-84\zeta_3+8}{5};\\
\delta_3 &:= -\frac{(132\zeta_3+156)\zeta_5^3+(-36\zeta_3+72)\zeta_5^2+(96\zeta_3+48)\zeta_5+48\zeta_3+164}{5};\\
\delta_4 &:= -\frac{(36\zeta_3-72)\zeta_5^3+(132\zeta_3-24)\zeta_5^2+(168\zeta_3+84)\zeta_5+84\zeta_3+92}{5}.
\end{aligned}
$$

Then the 24 torsion points of $\mathcal{E}_2$ with exact order 5 are:

$$
\begin{aligned}
\pm P_1 &= (x_1, \pm y_1) &&= \left(\sqrt[3]{\delta_1 c}, \pm\sqrt{(\delta_1+1)c}\right);\\
\pm\phi_2(P_1) &= (\zeta_3 x_1, \pm y_1) &&= \left(\zeta_3\sqrt[3]{\delta_1 c}\,, \pm\sqrt{(\delta_1+1)c}\right);\\
\pm\phi_2^2(P_1) &= (\zeta_3^2 x_1, \pm y_1) &&= \left(\zeta_3^2\sqrt[3]{\delta_1 c}\,, \pm\sqrt{(\delta_1+1)c}\right);\\[1ex]
\pm P_2 &= (x_2, \pm y_2) &&= \left(\sqrt[3]{\delta_2 c}, \pm\sqrt{(\delta_2+1)c}\right);\\
\pm\phi_2(P_2) &= (\zeta_3 x_2, \pm y_2) &&= \left(\zeta_3\sqrt[3]{\delta_2 c}\,, \pm\sqrt{(\delta_2+1)c}\right);\\
\pm\phi_2^2(P_2) &= (\zeta_3^2 x_2, \pm y_2) &&= \left(\zeta_3^2\sqrt[3]{\delta_2 c}\,, \pm\sqrt{(\delta_2+1)c}\right);\\[1ex]
\pm P_3 &= (x_3, \pm y_3) &&= \left(\sqrt[3]{\delta_3 c}, \pm\sqrt{(\delta_3+1)c}\right);\\
\pm\phi_2(P_3) &= (\zeta_3 x_3, \pm y_3) &&= \left(\zeta_3\sqrt[3]{\delta_3 c}\,, \pm\sqrt{(\delta_3+1)c}\right);\\
\pm\phi_2^2(P_3) &= (\zeta_3^2 x_3, \pm y_3) &&= \left(\zeta_3^2\sqrt[3]{\delta_3 c}\,, \pm\sqrt{(\delta_3+1)c}\right);\\[1ex]
\pm P_4 &= (x_4, \pm y_4) &&= \left(\sqrt[3]{\delta_4 c}, \pm\sqrt{(\delta_4+1)c}\right);\\
\pm\phi_2(P_4) &= (\zeta_3 x_4, \pm y_4) &&= \left(\zeta_3\sqrt[3]{\delta_4 c}\,, \pm\sqrt{(\delta_4+1)c}\right);\\
\pm\phi_2^2(P_4) &= (\zeta_3^2 x_4, \pm y_4) &&= \left(\zeta_3^2\sqrt[3]{\delta_4 c}\,, \pm\sqrt{(\delta_4+1)c}\right).
\end{aligned}
$$

Theorem 5.1. *Let δ_j be as above, with $1 \leqslant j \leqslant 4$. We have*

$$K_5 = K(\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j+1)c}) = K(\sqrt[3]{\delta_j c}, \zeta_5, \sqrt{(\delta_j+1)c}).$$

Proof. Let $P_j = (\sqrt[3]{\delta_j c}, \sqrt{(\delta_j+1)c})$. We have $\phi_2(P_j) = nP_j$, for some positive integer n, if and only if $(\phi_2 - n)P_j = 0$. Since $P \in \mathcal{E}_2[5]$ and 5 is inert in

$\mathbb{Z}[\zeta_3]$ (the ring of automorphisms of $\mathcal{E}_2$), then $\phi_2(P_j) \neq nP_j$, for every positive integer n. Therefore $\{P_j, \phi_2(P_j)\}$ is a basis of $\mathcal{E}_2[5]$. By Remark 5.1 and by Theorem 1.1 we have $K_5 = K(\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j+1)c}) = K(\sqrt[3]{\delta_j c}, \zeta_5, \sqrt{(\delta_j+1)c})$. □

6 - Degrees $[K_5 : K\,]$ for the curves of $\mathcal{F}_2$

By the results achieved in Theorem 5.1, we are going to describe the possible degrees $[K_5 : K]$, for the elliptic curves of the family $\mathcal{F}_2$. To ease the notation, from now on we will fix the generating set $\{P_1, \phi_1(P_1)\}$ for $\mathcal{E}_2[5]$. Thus $K_5 = K(\sqrt[3]{\delta_1 c}, \zeta_3, \sqrt{(\delta_1+1)c}) = K(\sqrt[3]{\delta_1 c}, \zeta_5, \sqrt{(\delta_1+1)c})$. Clearly all the results that we are going to show about the degree $[K_5 : K]$ and the Galois group $\mathrm{Gal}(K_5/K)$ hold as well for every other generating set $\{\sqrt[3]{\delta_j c}, \zeta_3, \sqrt{(\delta_j+1)c}\}$ or $\{\sqrt[3]{\delta_j c}, \zeta_5, \sqrt{(\delta_j+1)c}\}$ of the extension K_5/K, with $2 \leqslant j \leqslant 4$.

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

A. $\zeta_3 \notin K$;

B1. $\zeta_5 + \zeta_5^{-1} \notin K(\zeta_3)$; **C**. $\sqrt[3]{\delta_1 c} \notin K(\zeta_3, \zeta_5)$;

B2. $\zeta_5 \notin K(\zeta_3, \zeta_5 + \zeta_5^{-1})$; **D**. $\sqrt{(\delta_1+1)c} \notin K(\zeta_3, \zeta_5)$.

The possible degrees of the extension K_5/K are the following

Table 2.

d	holding conditions	d	holding conditions
48	**A**, **B1**, **B2**, **C**, **D**	6	**C** *and* 1 *among* **A**, **B1**, **B2**, **D**
24	**C** *and* 3 *among* **A**, **B1**, **B2**, **D**	4	2 *among* **A**, **B1**, **B2**, **D**
16	**A**, **B1**, **B2**, **D**	3	**C**
12	**C** *and* 2 *among* **A**, **B1**, **B2**, **D**	2	1 *among* **A**, **B1**, **B2**, **D**
8	3 *among* **A**, **B1**, **B2**, **D**	1	*no holding conditions*

Proof. Consider the tower of extensions

$$\begin{aligned} K &\subseteq K(\zeta_3) \subseteq K(\zeta_3, \zeta_5 + \zeta_5^{-1}) \subseteq K(\zeta_3, \zeta_5) \\ &\subseteq K(\zeta_3, \zeta_5, \sqrt[3]{\delta_1 c}) \subseteq K(\zeta_3, \zeta_5, \sqrt[3]{\delta_1 c}, \sqrt{(\delta_1+1)c}). \end{aligned}$$

The degree of K_5/K is the product of the degrees of the intermediate extensions appearing in the tower. Each of those extension gives a contribution to the degree that is less than or equal to 2, except the extension $K(\zeta_3, \zeta_5, \sqrt[3]{(\delta_1)c})/$

$K(\zeta_3, \zeta_5)$ that gives a contribution equal to 1 or 3. The final computation is straightforward. □

Observe that $[K_5 : K] \leqslant 48$ is in accordance with the fact that $\mathcal{E}_2$ has complex multiplication and then the Galois representation

$$\rho_{\mathcal{E}_2,5} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$$

is not surjective.

7 - Galois groups $\mathrm{Gal}(K_5/K)$ for the curves of $\mathcal{F}_2$

We have the following four generating automorphisms of the Galois group $G = \mathrm{Gal}(K(\mathcal{E}_2[5])/K)$.

i) The automorphism ϕ_2 of the complex multiplication permuting the abscissas as follows

$$\sqrt[3]{\delta_j c} \mapsto \zeta_3 \sqrt[3]{\delta_j c} \mapsto \zeta_3^2 \sqrt[3]{\delta_j c} \mapsto \sqrt[3]{\delta_j c},$$

for every $1 \leqslant j \leqslant 4$, and fixing all the ordinates. Clearly ϕ_2 has order 3.

ii) The automorphism φ_1 of order 4 mapping ζ_5 to ζ_5^2, that consequentely maps

$$\delta_1 \mapsto \delta_2 \mapsto \delta_3 \mapsto \delta_4 \mapsto \delta_1,$$

i.e.

$$P_1 \xmapsto{\varphi_1} P_2 \xmapsto{\varphi_1} P_3 \xmapsto{\varphi_1} P_4 \xmapsto{\varphi_1} P_1;$$
$$\phi_2(P_1) \xmapsto{\varphi_1} \phi_2(P_2) \xmapsto{\varphi_1} \phi_2(P_3) \xmapsto{\varphi_1} \phi_2(P_4) \xmapsto{\varphi_1} \phi_2(P_1);$$
$$\phi_2^2(P_1) \xmapsto{\varphi_1} \phi_2^2(P_2) \xmapsto{\varphi_1} \phi_2^2(P_3) \xmapsto{\varphi_1} \phi_2^2(P_4) \xmapsto{\varphi_1} \phi_2^2(P_1).$$

iii) The automorphism -Id of order 2, mapping $\sqrt{(\delta_j+1)c}$ to $-\sqrt{(\delta_j+1)c}$, for all $1 \leqslant j \leqslant 4$, such that

$$P \xmapsto{-\mathrm{Id}} -P,$$

for all $P \in \mathcal{E}[5]$.

iv) The automorphism φ_2 of order 2 sending ζ_3 to ζ_3^2, and then swapping δ_1 and δ_3 and also δ_2 and δ_4. We have

$$P_1 \xleftrightarrow{\varphi_2} P_3 \qquad\qquad P_2 \xleftrightarrow{\varphi_2} P_4;$$

$$\phi_2(P_1) \xleftrightarrow{\varphi_2} \phi_2^2(P_3) \qquad\qquad \phi_2(P_2) \xleftrightarrow{\varphi_2} \phi_2^2(P_4);$$

$$\phi_2^2(P_1) \xleftrightarrow{\varphi_2} \phi_2(P_3) \qquad\qquad \phi_2^2(P_2) \xleftrightarrow{\varphi_2} \phi_2(P_4).$$

One easily verifies that all these authomorphisms commute, except ϕ_2 and φ_2. Indeed we have $\varphi_2\phi_2 = \phi_2^{-1}\varphi_2$.

Observe that $\psi_2 := \phi_2 \circ \varphi_1$ is a homomorphism of order 12 and that $G = \langle\psi_2, \varphi_2, -\mathrm{Id}\rangle$. The automorphism ψ_2 and φ_2 do not commute, since ϕ_2 do not commute with φ_2, instead one can verify that $\varphi_2 \circ \psi_2 = \psi_2^{-1} \circ \varphi_2$. Thus the group $\langle\psi_2, \varphi_2\rangle$ has a presentation $\langle\psi_2, \varphi_2 | \psi_2^{12} = \varphi_2^2 = \mathrm{Id}, \varphi_2\psi_2 = \psi_2^{-1}\varphi_2\rangle$ and it is isomorphic to D_{24}.

If all the conditions as in Table 2 hold, then we have the Galois group $G = \langle\psi_2, \varphi_2\rangle \times \langle-\mathrm{Id}\rangle \simeq D_{24} \times \mathbb{Z}/2\mathbb{Z}$ of order 48. By [**24**, Chapter II, Theorem 2.3], the extension $K_5/K(\zeta_3)$ is abelian. Thus, if condition **A** does not hold, then we have an abelian group. In all cases the group G is isomorphic to a subgroup of $D_{24} \times \mathbb{Z}/2\mathbb{Z}$ as follows. Let $d := [K_5 : K]$.

$d = 48$ If the degree d of the extension K_5/K is 48, then all the conditions hold. We have $G \simeq D_{24} \times \mathbb{Z}/2\mathbb{Z}$ as above.

$d = 24$ If the degree d of the extension K_5/K is 24, then condition **C** must hold (and one of the other conditions must not hold).

If **A** does not hold, then we have an abelian group. In this case $G = \langle\psi_2, -\mathrm{Id}\rangle \simeq \mathbb{Z}/12\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If **D** does not hold, then $G = \langle\psi_2, \varphi_2\rangle \simeq D_{24}$.

If one among the conditions **B1** and **B2** does not hold, then $G = \langle\psi_2, \varphi_2, -\mathrm{Id}\rangle$, where ψ_2^6 now fixes K_5 and $\langle\psi_2, \varphi_2\rangle$ is isomorphic to D_{12}. We have $G \simeq D_{12} \times \mathbb{Z}/2\mathbb{Z}$.

$d = 16$ If the degree d of the extension K_5/K is 16, then all the conditions hold but **C**. Thus ϕ_2 fixes K_5. We have an abelian extension and an abelian Galois group $G = \langle\varphi_1, \varphi_2, -\mathrm{Id}\rangle \simeq \mathbb{Z}/4\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

$d = 12$ If the degree d of the extension K_5/K is 12, then condition **C** must hold.

If **A** does not hold and one among **B1** and **B2** does not hold, then we have the abelian group $G = \langle\psi_2, -\mathrm{Id}\rangle \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If **D** does not hold and only one condition among **B1** and **B2** holds, then $G = \langle\psi_2, \varphi_2\rangle \simeq D_{12}$ (in this case ψ_2^6 fixes K_5).

If both **B1** and **B2** hold, then $G \simeq D_6 \times \mathbb{Z}/2\mathbb{Z} \simeq S_3 \times \mathbb{Z}/2\mathbb{Z}$, where S_3 is the symmetric group of order 6.

$d = 8$ If the degree d of the extension K_5/K is 8, then **C** does not hold and we have again an abelian extension.

If **D** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If **A** does not hold, then $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

If one among **B1** and **B2** does not holds, then $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.

$d = 6$ If the degree d of the extension K_5/K is 6, then **C** holds.

If **A** holds as well, then $G \simeq D_6 \simeq S_3$.

If **A** does not hold, then $G \simeq \mathbb{Z}/6\mathbb{Z}$.

$d = 4$ If the degree d of the extension K_5/K is 4, then **C** does not hold. If both **B1** and **B2** hold, then $G \simeq \mathbb{Z}/4\mathbb{Z}$, otherwise 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_5/K is 3 or 2 or 1, obviously the Galois group is respectively $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ or $\{\mathrm{Id}\}$.

8 - Some applications

We are going to show some applications of the results achieved in the previous sections. In particular we will show an application to the local-global divisibility problem, and some immediate applications to modular curves.

8.1 - *A minimal bound for the local-global divisibility by* 5

We recall the statement of the Local-Global Divisibility Problem and some key facts about the cohomology group that gives the obstruction to its validity in order to maintain the paper more self-contained. For further details one can see [**9**], [**8**] and [**17**].

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 $P = mD$?*

The classical question is considered for all commutative algebraic groups, but in our situation, we can confine the discussion only to elliptic curves $\mathcal{E}$ over K. Let $P \in \mathcal{E}[m]$ and let $D \in \mathcal{E}(\overline{K})$ be a m-divisor of P, i.e. $P = mD$. For every $\sigma \in G = \mathrm{Gal}(K_m/K)$, we have

$$m\sigma(D) = \sigma(mD) = \sigma(P) = P.$$

Thus $\sigma(D)$ and D differ by a point in $\mathcal{E}[m]$ and we can define a cocycle $\{Z_\sigma\}_{\sigma\in G}$ of G with values in $\mathcal{E}[m]$ by

$$Z_\sigma := \sigma(D) - D. \tag{2}$$

Such a cocycle vanishes in $H^1(G,\mathcal{E}[m])$, if and only if there exists a K-rational m-divisor of P (see for example [**9**] or [**8**]). In particular, the hypotheses about the validity of the local-divisibility in Problem 8.1 imply that the cocyle $\{Z_\sigma\}_{\sigma\in G}$ vanishes in $H^1(\mathrm{Gal}((K_m)_v/K_v),\mathcal{E}[m])$, for all but finitely many $v\in M_K$. Let G_v denote the group $\mathrm{Gal}((K_m)_v/K_v)$ and let Σ be the subset of M_K containing all the $v\in M_K$, that are unramified in K_m. Dvornicich and Zannier stated the following definition of a subgroup of $H^1(G,\mathcal{E}[m])$ which encodes the hypotheses of the problem in this cohomological context and essentially gives the obstruction to the validity of this Hasse principle (see [**9**] and [**10**] for further details)

$$H^1_{\mathrm{loc}}(G,\mathcal{E}[m]) := \bigcap_{v\in\Sigma}(\ker H^1(G,\mathcal{E}[m]) \xrightarrow{res_v} H^1(G_v,\mathcal{E}[m])), \tag{3}$$

where res_v is the usual restriction map.

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 Tchebotarev Density Theorem, the local Galois group G_v varies over *all* cyclic subgroups of G as v varies in Σ. Since the cocycle defined by (2) vanishes in $H^1(G_v,\mathcal{E}[m])$, if and only if there exists a K_v-rational m-divisor of P, then we have the following equivalent definition of the group $H^1_{\mathrm{loc}}(G,\mathcal{E}[m])$.

Definition 8.1. A cocycle $\{Z_\sigma\}_{\sigma\in G}\in H^1(G,\mathcal{E}[m])$ satisfies the *local conditions* if, for every $\sigma\in G$, there exists $A_\sigma\in\mathcal{E}[m]$ such that $Z_\sigma=(\sigma-1)A_\sigma$. The subgroup of $H^1(G,\mathcal{E}[m])$ formed by all the cocycles satisfying the local conditions is the *first local cohomology group* $H^1_{\mathrm{loc}}(G,\mathcal{E}[m])$.

The triviality of $H^1_{\mathrm{loc}}(G,\mathcal{E}[m])$ assures the validity of the local-global divisibility by m in $\mathcal{E}$ over K.

Theorem 8.1 (Dvornicich, Zannier, 2001). *If $H^1_{loc}(G,\mathcal{E}[m])=0$, then the local-global divisibility by m holds in $\mathcal{E}$ over K.*

In [**9**] the authors showed that the local-global divisibility by 5 holds in $\mathcal{E}$ over K (see also [**25**]). Anyway in that paper, as well as in all the other papers (of various authors) about the topic, there is no information about the minimal number of places v for which the validity of the local divisibility by a prime p in $\mathcal{E}$ over K_v is sufficient to have the global divisibility by p in $\mathcal{E}$ over K. For the first time, here we show such a lower bound for the number of places v when $p = 5$, in the case of the curves belonging to the families $\mathcal{F}_1$ and $\mathcal{F}_2$.

By Theorem 8.1, the triviality of the first cohomology group $H^1_{\text{loc}}(G, \mathcal{E}[m])$ is a sufficient condition to have an affirmative answer to Problem 8.1. We have already recalled that by the Tchebotarev Density Theorem, the group G_v varies over all the cyclic subgroups of G, as v varies among all the places of K, that are unramified in K_m. Observe that in fact we have

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

where S is a subset of Σ such that G_v varies over all cyclic subgroups of G as v varies in S. In particular we can choose a minimal set S if G_v varies over all cyclic subgroups of G as v varies in S and, moreover, G_v and G_w are pairwise distinct cyclic subgroups of G, for all $v, w \in S$, with $v \neq w$. If we are able to find such a minimal set S and to prove that the local-global divisibility by 5 holds in $\mathcal{E}(K_v)$, for all $v \in S$, then we get $H^1_{\text{loc}}(G, \mathcal{E}[m]) = 0$ (and consequently the validity of the Hasse principle for divisibility by 5 in $\mathcal{E}$ over K). Observe that in particular S is finite (on the contrary Σ is not finite). So it suffices to have the local divisibility by 5 for a finite number of suitable places to get the global divisibility by 5.

In view of the results achieved for the Galois groups $\text{Gal}(K_5/K)$ for elliptic curves of the families $\mathcal{F}_1$ and $\mathcal{F}_2$, we can prove that S could be chosen as a subset of Σ with a cardinality surprisingly small.

Theorem 8.2. *Let m be a positive integer. Let $\mathcal{E}$ 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 $s \leqslant 7$ such that if $P = 5D_v$, with $D_v \in \mathcal{E}(K_v)$, for all $v \in S$, then $P = 5D$, for some $D \in \mathcal{E}(K)$. In particular, if $[K_5 : K] = 32$, then $s = 7$.*

Proof. Let s be the number of distinct cyclic subgroups of G. As stated above, we can choose S 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 $v \neq w$. We have to show that $s \leqslant 7$, i.e. that G has at most 7 cyclic subgroups. We have proved in Section 4, that for every $\mathcal{E} \in \mathcal{F}_1$, the Galois group G is isomorphic to a subgroup of $D_8 \times \mathbb{Z}/4\mathbb{Z}$. The group D_8 has 5 cyclic subgroups, namely $\langle \phi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$, $\langle \phi_1^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \rho \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \phi_1 \rho \rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle \phi_1^2 \rho \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. In addition we have the cyclic subgroups $\langle \psi_1 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$ and $\langle \psi_1^2 \rangle \simeq \mathbb{Z}/2\mathbb{Z}$. Thus G has at most 7 cyclic subgroups. In particular, if $[K_5 : K] = 32$, then G has exactly 7 cyclic subgroups and then $s = 7$. □

Theorem 8.3. *Let m be a positive integer. Let $\mathcal{E}$ 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 $s \leqslant 13$ such that if $P = 5D_v$, with $D_v \in \mathcal{E}(K_v)$, for all $v \in S$, then $P = 5D$, for some $D \in \mathcal{E}(K)$. In particular, if $[K_5 : K] = 48$, then $s = 13$.*

Proof. Let s be the number of distinct cyclic subgroups of G. As in the proof of Theorem 8.2 we can choose S as a subset 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 $v \neq w$. We have to show that $s \leqslant 13$, i.e. that G has at most 13 cyclic subgroups. We have proved in Section 7, that for every $\mathcal{E} \in \mathcal{F}_2$, the Galois group G is isomorphic to a subgroup of $D_{24} \times \mathbb{Z}/2\mathbb{Z}$. The group D_{24} has 11 cyclic subgroups, namely $\langle\psi_1\rangle \simeq \mathbb{Z}/12\mathbb{Z}$, $\langle\psi_1^2\rangle \simeq \mathbb{Z}/6\mathbb{Z}$, $\langle\psi_1^3\rangle \simeq \mathbb{Z}/4\mathbb{Z}$, $\langle\psi_1^4\rangle \simeq \mathbb{Z}/3\mathbb{Z}$, $\langle\psi_1^6\rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle\varphi_2\rangle \simeq \mathbb{Z}/2\mathbb{Z}$, $\langle\psi_1\varphi_2\rangle \simeq \mathbb{Z}/12\mathbb{Z}$, $\langle\psi_1^2\varphi_2\rangle \simeq \mathbb{Z}/6\mathbb{Z}$, $\langle\psi_1^3\varphi_2\rangle \simeq \mathbb{Z}/4\mathbb{Z}$, $\langle\psi_1^4\varphi_2\rangle \simeq \mathbb{Z}/3\mathbb{Z}$, $\langle\psi_1^6\varphi_2\rangle \simeq \mathbb{Z}/2\mathbb{Z}$. In addition, we have the cyclic subgroups $\langle -\mathrm{Id}\rangle \simeq \mathbb{Z}/2\mathbb{Z}$ and $\langle\psi_1^4\rangle \times \langle -\mathrm{Id}\rangle \simeq \mathbb{Z}/6\mathbb{Z}$. Thus G has at most 13 cyclic subgroups. In particular, if $[K_5 : K] = 48$, then G has exactly 13 cyclic subgroups and then $s = 13$. □

Observe that the definition of $H^1_{\mathrm{loc}}(G, \mathcal{E}[m])$ is very similar to the one of the Tate-Shafarevich group $Ш(K, \mathcal{E}[m])$. Indeed by [**19**, Lemma 1.2], the group $Ш(K, \mathcal{E}[m])$ is isomorphic to the following subgroup of $H^1_{\mathrm{loc}}(G, \mathcal{E}[m])$

$$\bigcap_{v \in M_k} (\ker H^1(G, \mathcal{E}[m]) \xrightarrow{res_v} H^1(G_v, \mathcal{E}[m])). \tag{4}$$

In particular the triviality of $H^1_{\mathrm{loc}}(G, \mathcal{E}[m])$ implies the triviality of $Ш(K, \mathcal{E}[m])$. Thus we have the following corollaries of Theorem 8.2 and respectively Theorem 8.3.

Corollary 8.1. *Let m be a positive integer. Let $\mathcal{E}$ 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 $s \leqslant 7$ such that if $P = 5D_v$, with $D_v \in \mathcal{E}(K_v)$, for all $v \in S$, then $Ш(K, \mathcal{E}[5]) = 0$. In particular, if $[K_5 : K] = 32$, then $s = 7$.*

Corollary 8.2. *Let m be a positive integer. Let $\mathcal{E}$ 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 $s \leqslant 13$ such that if $P = 5D_v$, with $D_v \in \mathcal{E}(K_v)$, for all $v \in S$, then $Ш(K, \mathcal{E}[5]) = 0$. In particular, if $[K_5 : K] = 48$, then $s = 13$.*

8.2 - *Remarks on modular curves*

We recall some basic definitions about modular curves; for further details one can see for instance **[12]** and **[22]**. As usual, we denote by $\mathcal{H} = \{z \in \mathbb{C} : Im\, z > 0\}$ the complex upper half plane. It is well-known that the group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$ via the Möbius trasformations

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

Let N denote a positive integer. A *congruence group* is a subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ containing

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

for some N. When N is minimal, the congruence group is said to be *of level* N. Along with $\Gamma(N)$, the most important congruence groups of level N are

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

and

$$\Gamma_1(N) = \left\{ A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\} \; .$$

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 set of rational points corresponding to the orbits of $\mathbb{P}^1(\mathbb{Q})$ under Γ, i.e. the *cusps.*

The modular curves associated to the groups $\Gamma(N)$, $\Gamma_0(N)$ and $\Gamma_1(N)$ are denoted respectively by $X(N)$, $X_0(N)$ and $X_1(N)$. They are spaces of moduli of families of elliptic curves with an extra structure of level N as follows (for further details see for example **[12]**, **[13]** and **[22]**).

Theorem 8.4. *Let N be a positive integer. Then*

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

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

iii) *non cuspidal points in $X(N)$ 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 N generating $\mathcal{E}[N]$.*

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

We can deduce the following facts from what showed in the previous sections (see in particular Theorem 2.1 and Theorem 5.1).

Proposition 8.1. *Let K be a number field.*

i) *If $\mathbb{Q}(i) \subseteq K$, then $X_0(5)(K)_{CM} \neq \emptyset$ and $X_1(5)(K)_{CM} \neq \emptyset$.*

ii) *If $\mathbb{Q}(i, \zeta_5) \subseteq K$ or $\mathbb{Q}(\zeta_3, \zeta_5) \subseteq K$, then $X(5)(K)_{CM} \neq \emptyset$.*

Proof.

i) Let ω_l be as in Section 2, for some $1 \leqslant l \leqslant 2$. Let $\hat{b} = \omega_l(\omega_l + 1)^2\beta^4$, for some $\beta \in \mathbb{Q}(i)$, and let $\mathcal{E}_1 : y^2 = x^3 + \hat{b}x$. Observe that $\hat{b} \in \mathbb{Q}(i)$. Moreover $\sqrt{\omega_l \hat{b}} = \omega_l(\omega_l + 1)\beta^2 \in \mathbb{Q}(i)$ and $\sqrt{(\omega_l + 1)\hat{b}\sqrt{\omega_l \hat{b}}} = \omega_l(\omega_l + 1)^2\beta^3 \in \mathbb{Q}(i)$. If $\mathbb{Q}(i) \subseteq K$, then the couple $(\mathcal{E}_1, \langle P_{l+4} \rangle)$ defines a K-rational CM point of $X_0(5)$ and the couple $(\mathcal{E}_1, P_{l+4})$ defines a K-rational CM point of $X_1(5)$.

ii) Let θ_j be as in Section 2, for some $1 \leqslant j \leqslant 4$. Let $\tilde{b} = \theta_j(\theta_j + 1)^2\beta^4$, with $\beta \in \mathbb{Q}(i, \zeta_5)$, and let $\mathcal{E}_1 : y^2 = x^3 + \tilde{b}x$. We have $\tilde{b} \in \mathbb{Q}(i, \zeta_5)$. Furthermore $\sqrt{\theta_j \tilde{b}} = \theta_j(\theta_j + 1)\beta^2 \in \mathbb{Q}(i, \zeta_5)$ and $\sqrt{(\theta_j + 1)\tilde{b}\sqrt{\theta_j \tilde{b}}} = \theta_j(\theta_j + 1)^2\beta^3 \in \mathbb{Q}(i, \zeta_5)$. If $\mathbb{Q}(i, \zeta_5) \subseteq K$, then the triple $(\mathcal{E}_1, P_j, \phi_1(P_j))$ defines a K-rational CM point of $X(5)$.

Let δ_j be as in Section 5, for some $1 \leqslant j \leqslant 4$. Let $\tilde{c} = \delta_j^2(\delta_j + 1)^3\gamma^6$, for some $\gamma \in \mathbb{Q}(\zeta_3, \zeta_5)$, and let $\mathcal{E}_2 : y^2 = x^3 + \tilde{c}$. Observe that $\tilde{c} \in \mathbb{Q}(\zeta_3, \zeta_5)$. Moreover $\sqrt[3]{\delta_j \tilde{c}} = \delta_j(\delta_j + 1)\gamma^2 \in \mathbb{Q}(\zeta_3, \zeta_5)$ and $\sqrt{(\delta_j + 1)\tilde{c}} = \delta_j(\delta_j + 1)^2\gamma^3 \in \mathbb{Q}(\zeta_3, \zeta_5)$. If $\mathbb{Q}(\zeta_3, \zeta_5) \subseteq K$, then the triple $(\mathcal{E}_2, P_j, \phi_2(P_j))$ defines a K-rational CM point of $X(5)$.

□

We can deduce some other remarks about the K-rational CM points of $X_0(5)$, $X_1(5)$ and $X(5)$, when K contains $\mathbb{Q}(i, \zeta_5)$ or $\mathbb{Q}(\zeta_5)$ or $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$. We state them in the following three propositions. All the proofs easily follow from the results proved in Section 2 and in Section 5, and we leave them to the reader. As above ϕ_i denotes the complex multiplication of $\mathcal{E}_i$, for $i \in \{1, 2\}$.

Proposition 8.2. *Let K be an extension of $\mathbb{Q}(i,\zeta_5)$. Let $\mathcal{E}_1 \in \mathcal{F}_1$ and let $P \in \mathcal{E}_1[5]$ such that $\{P,\phi_1(P)\}$ is a generating set of $\mathcal{E}_1[5]$. Then*

i) *the couple $(\mathcal{E}_1, \langle P\rangle)$ defines a non-cuspidal K-rational CM point of $X_0(5)$, if and only if $y(P) \in K$;*

ii) *the couple $(\mathcal{E}_1, P)$ defines a non-cuspidal K-rational CM point of $X_1(5)$, if and only if $y(P) \in K$;*

iii) *the triple $(\mathcal{E}_1, P, \phi_1(P))$ defines a non-cuspidal K-rational CM point of $X(5)$, if and only if $y(P) \in K$.*

Proposition 8.3. *Let K be an extension of $\mathbb{Q}(\zeta_5)$ or an extension of $\mathbb{Q}(i)$. Let $\mathcal{E}_1 \in \mathcal{F}_1$ and let $P \in \mathcal{E}_1[5]$ such that $\{P,\phi_1(P)\}$ is a basis of $\mathcal{E}_1[5]$. Then*

> *the pair $(\mathcal{E}_1, \langle P\rangle)$ defines a non-cuspidal K-rational CM point of $X_0(5)$, if and only if $(\mathcal{E}_1, P)$ defines a non-cuspidal K-rational CM point of $X_1(5)$, if and only if $(\mathcal{E}_1, P, \phi_1(P))$ defines a non-cuspidal K-rational CM point of $X(5)$.*

Proposition 8.4. *Let K be an extension of $\mathbb{Q}(\zeta_3)$ or an extension of $\mathbb{Q}(\zeta_5)$. Let $\mathcal{E}_2 \in \mathcal{F}_2$ and let $P \in \mathcal{E}_2[5]$ such that $\{P,\phi_1(P)\}$ is a basis of $\mathcal{E}_2[5]$. Then*

> *the pair $(\mathcal{E}_2, \langle P\rangle)$ defines a non-cuspidal K-rational CM point of $X_0(5)$, if and only if $(\mathcal{E}_2, P)$ defines a non-cuspidal K-rational CM point of $X_1(5)$, if and only if $(\mathcal{E}_2, P, \phi_2(P))$ defines a K-rational CM point of $X(5)$.*

Remark 8.1. Similar reasonings produce points on some Shimura curves. The Shimura curve $\mathcal{X}(1)$ is a moduli space of abelian surfaces $\mathcal{A}$ with quaternionic multiplication, such that $\mathcal{A}$ is simple with $\mathrm{End}(\mathcal{A})\otimes\mathbb{Q} = M_2(\mathbb{Q})$ (as usual $M_2(\mathbb{Q})$ denotes the set of 2×2 matrices with entries in $\mathbb{Q}$) or $\mathcal{A} = \mathcal{E}\times\mathcal{E}$, where $\mathcal{E}$ is a CM elliptic curve. The modular curves $\mathcal{X}_0(N)$ and $\mathcal{X}_1(N)$ are moduli spaces of abelian surfaces $\mathcal{A}$ as above, but with some extra structures of level N (roughly speaking, certain particular subgroups of the N-torsion $\mathcal{A}[N]$, isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$, in the case of $\mathcal{X}_0(N)$ and points of order N in the case of $\mathcal{X}_1(N)$, see [**6**] and [**22**] for further details). We will call a CM point of a Shimura curve, a point corresponding to a square of an elliptic curve with complex multiplication. For $j \in \{0,1\}$, let $\mathcal{X}_j(5)(K)_{CM}$ denote the set of the K-rational CM points of $\mathcal{X}_j(5)$. By the results achieved in Section 2 and in Section 5, one can exhibit all the CM points of the curves $\mathcal{X}_0(5)$ and $\mathcal{X}_1(5)$ corresponding to squares of elliptic curves $\mathcal{E}_1 \in \mathcal{F}_1$ and squares of elliptic curves $\mathcal{E}_2 \in \mathcal{F}_2$. In particular we have an infinite number of fields K such that $\mathcal{X}_0(5)(K) \neq \emptyset$ and

$\mathcal{X}_1(5)(K) \neq \emptyset$. For instance we have the following corollary of Proposition 8.1. We recall that for some Shimura curves and certain fields F it is known that the set of F-rational points is on the contrary empty (see for example [**7**], [**18**] and [**21**]).

Corollary 8.3. *Let K be a number field.*

i) *If $\mathbb{Q}(i) \subseteq K$, then $\mathcal{X}_0(5)(K)_{CM} \neq \emptyset$ and $\mathcal{X}_1(5)(K)_{CM} \neq \emptyset$.*

ii) *If $\mathbb{Q}(\zeta_3, \zeta_5) \subseteq K$, then $\mathcal{X}_0(5)(K)_{CM} \neq \emptyset$ and $\mathcal{X}_1(5)(K)_{CM} \neq \emptyset$.*

Acknowledgments. I would like to thank Andrea Bandini for useful discussions and for some precious remarks about a preliminary version of this paper. I produced part of this work when I was a guest at the Max Planck Institute for Mathematics in Bonn. I am grateful to all people there for their kind hospitality and for the excellent work conditions. I am also grateful to the anonymous reviewer for his constructive comments and suggestions.

References

[**1**] C. Adelmann, *The decomposition of primes in torsion point fields*, Lecture Notes in Math., **1761**, Springer-Verlag, Berlin, 2001.

[**2**] A. Bandini, *Three-descent and the Birch and Swinnerton-Dyer conjecture*, Rocky Mountain J. Math. **34** (2004), 13–27.

[**3**] A. Bandini, 3-*Selmer groups for curves $y^2 = x^3 + a$*, Czechoslovak Math. J. **58** (2008), 429–445.

[**4**] A. Bandini and L. Paladino, *Number fields generated by the* 3*-torsion poins of an elliptic curve*, Monatsh. Math. **168** (2012), 157–181.

[**5**] A. Bandini and L. Paladino, *Fields generated by torsion poins of elliptic curves*, J. Number Theory **169** (2016), 103–133.

[**6**] P. L. Clark, *Rational points on Atkin-Lehner quotients of Shimura curves*, Ph.D. Thesis, Harvard University, Cambridge, MA, 2003.

[**7**] P. Clark and X. Xarles, *Local bounds for torsion points on abelian varieties*, Canad. J. Math. **60** (2008), 532–555.

[**8**] R. Dvornicich and A. Paladino, *Local-global questions for divisibility in commutative algebraic groups*, arXiv:1706.03726v4, preprint, 2018.

[**9**] R. Dvornicich and U. Zannier, *Local-global divisibility of rational points in some commutative algebraic groups*, Bull. Soc. Math. France **129** (2001), 317–338.

[**10**] R. Dvornicich and U. Zannier, *On local-global principle for the divisibility of a rational point by a positive integer*, Bull. Lond. Math. Soc. **39** (2007), 27–34.

[**11**] E. González-Jiménez and Á. Lozano-Robledo, *Elliptic curves with abelian division fields*, Math. Z. **283** (2016), 835–859.

[**12**] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Ann. of Math. Stud., **108**, Princeton Univ. Press, Princeton, NJ, 1985.

[**13**] A. W. Knapp, *Elliptic curves*, Math. Notes, **40**, Princeton Univ. Press, Princeton, NJ, 1992.

[**14**] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, (French), Invent. Math. **124** (1996), 437–449.

[**15**] L. Paladino, *Local-global divisibility by* 4 *in elliptic curves defined over* $\mathbb{Q}$, Ann. Mat. Pura Appl. (4) **189** (2010), 17–23.

[**16**] L. Paladino, *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** (2010), 139–160.

[**17**] L. Paladino, G. Ranieri and E. Viada, *On minimal set for counterexamples to the local-global principle*, J. Algebra **415** (2014), 290–304.

[**18**] V. Rotger and C. de Vera-Piquero, *Galois representations over fields of moduli and rational points on Shimura curves*, Canad. J. Math. **66** (2014), 1167–1200.

[**19**] J.-J. Sansuc, *Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres*, (French), J. Reine Angew. Math. **327** (1981), 12–80.

[**20**] E. F. Schaefer and M. Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), 1209–1231.

[**21**] G. Shimura, *On the real points of an arithmetic quotient of a bounded symmetric domain*, Math. Ann. **215** (1975), 135–164.

[**22**] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, NJ, 1994.

[**23**] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math., **106**, Springer, Dordrecht, 2009.

[**24**] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math., **151**, Springer-Verlag, New York, 1994.

[**25**] S. Wong, *Power residues on Abelian varieties*, Manuscripta Math. **102** (2000), 129–137.

Laura Paladino
University of Calabria
Ponte Bucci, Cubo 30B
Rende, 87036, Italy
e-mail: paladino@mat.unical.it