Journal of Number Theory 169 (2016) 103–133

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Fields generated by torsion points of elliptic curves

Andrea Bandini [a,*], Laura Paladino [b,1]

[a] *Dipartimento di Matematica e Informatica, Università degli Studi di Parma, Parco Area delle Scienze, 53/A, 43124 Parma (PR), Italy*
[b] *Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo, 5, 56127 Pisa (PI), Italy*

A R T I C L E I N F O

Article history:
Received 21 May 2015
Received in revised form 3 November 2015
Accepted 18 May 2016
Available online 7 July 2016
Communicated by David Goss

MSC:
11G05
11F80

Keywords:
Elliptic curves
Torsion points
Galois representations

A B S T R A C T

Let K be a field of characteristic $\mathrm{char}(K) \neq 2, 3$ and let $\mathcal{E}$ be an elliptic curve defined over K. Let m be a positive integer, prime with $\mathrm{char}(K)$ if $\mathrm{char}(K) \neq 0$; 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 $\mathcal{E}[m]$. Let $P_i := (x_i, y_i)$ $(i = 1, 2)$ be a $\mathbb{Z}$-basis for $\mathcal{E}[m]$; then $K_m = K(x_1, y_1, x_2, y_2)$. We look for small sets of generators for K_m inside $\{x_1, y_1, x_2, y_2, \zeta_m\}$ trying to emphasize the role of ζ_m (a primitive m-th root of unity). In particular, we prove that $K_m = K(x_1, \zeta_m, y_2)$, for any odd $m \geqslant 5$. When $m = p$ is prime and K is a number field we prove that the generating set $\{x_1, \zeta_p, y_2\}$ is often minimal, while when the classical Galois representation $\mathrm{Gal}(K_p/K) \to \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is not surjective we are sometimes able to further reduce the set of generators. We also describe explicit generators, degree and Galois groups of the extensions K_m/K for $m = 3$ and $m = 4$.

* Corresponding author.
E-mail addresses: andrea.bandini@unipr.it (A. Bandini), paladino@mat.unical.it (L. Paladino).

[1] Partially supported by Istituto Nazionale di Alta Matematica, grant research *Assegno di ricerca Ing. G. Schirillo* and partially supported by European Social Funds: FSE 2007-2013, POR Calabria 2007-2013.

http://dx.doi.org/10.1016/j.jnt.2016.05.004
0022-314X/

1. Introduction

Let K be a field of characteristic $\mathrm{char}(K) \neq 2, 3$ and let $\mathcal{E}$ be an elliptic curve defined over K. Let m be a positive integer, prime with $\mathrm{char}(K)$ if $\mathrm{char}(K) \neq 0$. 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 points of $\mathcal{E}[m]$, i.e., the field obtained by adding to K the coordinates of the m-torsion points of $\mathcal{E}$. As usual, for any point $P \in \mathcal{E}$, we let $x(P)$, $y(P)$ be its coordinates and we indicate its m-th multiple simply by mP. We denote by $\{P_1, P_2\}$ a $\mathbb{Z}$-basis for $\mathcal{E}[m]$; then $K_m = K(x(P_1), x(P_2), y(P_1), y(P_2))$. To ease notation, we put $x_i := x(P_i)$ and $y_i := y(P_i)$ $(i = 1, 2)$. By Artin's primitive element theorem the extension K_m/K is monogeneous and one can find a single generator for K_m/K by combining the above coordinates. On the other hand, by the properties of the Weil pairing e_m, we have that $e_m(P_1, P_2) \in K_m$ is a primitive m-th root of unity (we denote it by ζ_m). We want to emphasize the importance of ζ_m as a generator of K_m/K and look for minimal (i.e., with the smallest number of elements) sets of generators contained in $\{x_1, x_2, y_1, y_2, \zeta_m\}$. This kind of information is useful for describing the fields in terms of degrees and Galois groups, as we shall explicitly show for $m = 3$ and $m = 4$. Other applications are local–global problems (see, e.g., [5] or the particular cases of [11] and [12]), descent problems (see, e.g., [14] and the references there or, for a particular case, [2] and [3]), Galois representations, points on modular curves (see Section 4.4) and points on Shimura curves.

It is easy to prove that $K_m = K(x_1, x_2, \zeta_m, y_1)$ (see Lemma 2.1) and we expected a close similarity between the roles of the x-coordinates and y-coordinates; this turned out to be true in relevant cases. Indeed in Section 3 (mainly by analyzing the possible elements of the Galois group $\mathrm{Gal}(K_m/K)$) we prove that $K_m = K(x_1, \zeta_m, y_1, y_2)$ at least for odd $m \geqslant 5$. This leads to the following (for more precise and general statements see Theorems 2.8, 3.1 and 3.6)

Theorem 1.1. *If $m \geqslant 3$, then $K_m = K(x_1 + x_2, x_1x_2, \zeta_m, y_1)$. Moreover if $m \geqslant 4$, then*

$$K_m = K(x_1, \zeta_m, y_1, y_2) \Longrightarrow K_m = K(x_1, \zeta_m, y_2)\ .$$

In particular $K_m = K(x_1, \zeta_m, y_2)$ for any odd integer $m \geqslant 5$.

Note that, by Theorem 1.1, we have $K_p = K(x_1, \zeta_p, y_2)$, for any prime $p \geqslant 5$. The set $\{x_1, \zeta_p, y_2\}$ seems a good candidate (in general) for a minimal set of generators for K_p/K. Indeed, when K is a number field and $\mathcal{E}$ has no complex multiplication, by Serre's open image theorem (see [15]), we expect that the natural representation

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

provides an isomorphism $\mathrm{Gal}(K_p/K) \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for almost all primes p, and there are hypotheses on x_1, ζ_m and y_2 (see Theorem 4.3) which guarantee that