Twists of Elliptic Curves

Max KRONBERG [†], *Muhammad Afzal SOOMRO* [‡] *and Jaap TOP* [†]

[†] *Johan Bernoulli Institute for Mathematics and Computer Science,*
Nijenborgh 9, 9747 AG Groningen, The Netherlands
E-mail: *m.c.kronberg@rug.nl*, *j.top@rug.nl*

[‡] *Quaid-e-Awam University of Engineering, Science & Technology (QUEST),*
Sakrand Road, Nawabshah, Sindh, Pakistan
E-mail: *m.a.soomro@quest.edu.pk*

Received July 10, 2017, in final form October 23, 2017; Published online October 25, 2017
https://doi.org/10.3842/SIGMA.2017.083

Abstract. In this note we extend the theory of twists of elliptic curves as presented in various standard texts for characteristic not equal to two or three to the remaining characteristics. For this, we make explicit use of the correspondence between the twists and the Galois cohomology set $H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big)$. The results are illustrated by examples.

Key words: elliptic curve; twist; automorphisms; Galois cohomology

2010 Mathematics Subject Classification: 11G05; 11G25; 14G17

Dedicated to Noriko Yui. The third author of this note was a postdoc with her at Queen's University during 1989–1990.

1 Introduction

Throughout this paper K will be a perfect field and we always fix a separable closure of K, which we denote by $\overline{K}$. For the absolute Galois group of $\overline{K}$ over K we write $\mathrm{G}_{\overline{K}/K}$. Let E/K be an elliptic curve over K. A twist of E is an elliptic curve E^{tw}/K that is isomorphic to E over $\overline{K}$. In other words, it is an elliptic curve over K with j-invariant $j(E)$. Two such twists are considered equal if they are isomorphic over K. We denote the set of twists by $\mathrm{Twist}(E/K)$. For the automorphism group of E we write $\mathrm{Aut}_{\overline{K}}(E)$. The elements of $\mathrm{Twist}(E/K)$ are in one-to-one correspondence with the classes in $H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big)$ [21, Chapter X, Section 2]. We want to remark that our notation differs from the notation used by Silverman. He denotes the set of twists by $\mathrm{Twist}(E/K, O)$.

Recently there has been quite some interest in twists of not only elliptic curves, but also curves in general and even in twists of algebraic varieties over various fields [1, 7, 8, 11, 12, 14, 24]. And besides twists of varieties, twists of maps appear to have an increasing role in arithmetic dynamics [9, 13, 19, 23], [20, Section 4.9].

The simplest nontrivial example of twists is provided by the case of elliptic curves, where an early account of it was given by J.W.S. Cassels in [5, Part II, Section 9]. We briefly recall some of this theory here; in the case that the automorphism group of the elliptic curve is cyclic this is covered in various standard textbooks on elliptic curves. Although it is certainly known to most experts how to extend this theory to the cases where the automorphism group is noncyclic (and hence not even abelian), there seems to be no adequate reference for this and we hope to fill this gap. Note, by the way, that Ian Connell at McGill University (Montreal) in the late

This paper is a contribution to the Special Issue on Modular Forms and String Theory in honor of Noriko Yui. The full collection is available at http://www.emis.de/journals/SIGMA/modular-forms.html

1990's wrote extensive unpublished lecture notes on elliptic curves, including a long chapter on twists [6]. Inspired by those notes John Cremona implemented various algorithms for dealing with twists of elliptic curves in sage; see the lines 557–604 of [4] for sage code related to Section 2 of the present paper, and the lines 507–554 of [4] for sage code related to our Section 3.

For a positive integer n coprime to the characteristic of K we denote by $\mu_n(\overline{K})$ the group of n-th roots of unity in $\overline{K}^\times$ and by ζ_n a generator of this group. In [21], Silverman only presents an explicit description of the twists of an elliptic curve E/K in $\operatorname{char} K \neq 2, 3$. The main reason is that this condition implies $\operatorname{Aut}_{\overline{K}}(E) \cong \mu_n(\overline{K})$, for some $n \in \{2, 4, 6\}$, even as $\mathrm{G}_{\overline{K}/K}$-modules. In characteristic 2 the group $\operatorname{Aut}_{\overline{K}}(E)$ is either isomorphic to $\mathbb{Z}/2\mathbb{Z}$ or to a non-abelian group of order 24. In characteristic three the group $\operatorname{Aut}_{\overline{K}}(E)$ is either equals $\mu_2(\overline{K}) \cong \mathbb{Z}/2\mathbb{Z}$ or it is a non-abelian group of order 12. By explicitly describing $H^1\big(\mathrm{G}_{\overline{K}/K}, \operatorname{Aut}_{\overline{K}}(E)\big)$ in these remaining cases, we complete the description presented in [21].

We start by considering twists of elliptic curves with j-invariant equal to zero in characteristic three and two. We then consider the twists corresponding to normal subgroups of $\operatorname{Aut}_{\overline{K}}(E)$. The possible subgroups correspond to quadratic, cubic and sextic twists.

The main results of this note can be found in Propositions 2.1 and 3.1 which describe twists over finite fields of characteristic three respectively two, provided the automorphism group of the elliptic curve is non-abelian, and in Propositions 2.2 and 3.2, where we count the number of twists of any elliptic curve over a finite field. Sections 2 and 3 also indicate how these twists can be given explicitly in various non-trivial cases. Next, Propositions 4.1, 5.1 and 6.1 answer the question under what conditions a potentially quadratic or cubic twist of a given elliptic curve is in fact still isomorphic to the curve one starts with.

Parts of the results of this paper originate from the PhD thesis of the second author [22, Section 2.6].

2 Twists in characteristic three

We start by considering elliptic curves over finite fields $\mathbb{F}_{3^n}$. This is done by analysing the following central example. By [14], the twists of an elliptic curve E over a finite field $\mathbb{F} = \mathbb{F}_q$ of cardinality q are in one-to-one correspondence with the Frobenius conjugacy classes in $\operatorname{Aut}_{\overline{\mathbb{F}}}(E)$. By definition a Frobenius conjugacy class is obtained by fixing some $\tau \in \operatorname{Aut}_{\overline{\mathbb{F}}}(E)$, then its Frobenius conjugacy class consists of all

$$\big\{\sigma^{-1}\tau\big({}^{\mathrm{Fr}}\sigma\big)\big\}.$$

Here Fr is the field automorphism of $\overline{\mathbb{F}}$ raising any element to its qth power. It acts on an automorphism σ of E by acting on the coefficients of the rational functions defining σ. We will compute these Frobenius conjugacy classes for all possible actions of the absolute Galois group.

Proposition 2.1. *The elliptic curve*

$$E/\mathbb{F}_3\colon\ y^2 = x^3 - x$$

has $j(E) = 0$, and it has precisely twelve automorphisms. These are given by

$$\begin{array}{rccc} \Phi_{u,r}\colon & E & \longrightarrow & E, \\ & (x, y) & \longmapsto & \big(u^2x + r, u^3y\big), \end{array}$$

where $u^4 = 1$ and $r \in \mathbb{F}_3$. Let $n \geq 1$ and $q = 3^n$. For $u \in \mathbb{F}_9$ with $u^4 = 1$ and $r \in \mathbb{F}_3$, put

$$C_{u,r} = \big\{\Phi^{-1}_{u',r'} \circ \Phi_{u,r} \circ \Phi_{u'^q,r'^q} \,|\, (u')^4 = 1,\ r' \in \mathbb{F}_3\big\}$$

(this is the Frobenius conjugacy class of $\Phi_{u,r}$ over $\mathbb{F}_q$).

If n is odd, then the Frobenius conjugacy classes of $E/\mathbb{F}_q$ are

$$C_{1,0} = \{\Phi_{1,0}, \Phi_{-1,0}\}, \qquad C_{1,1} = \{\Phi_{1,1}, \Phi_{-1,-1}\}, \qquad C_{1,-1} = \{\Phi_{1,-1}, \Phi_{-1,1}\},$$
$$C_{i,0} = \{\Phi_{u,r} \,|\, u^2 = -1,\, r \in \mathbb{F}_3\}.$$

In particular there are precisely three non-trivial twists of E over $\mathbb{F}_q$ in case n is odd, which are given as follows.

Consider the cocycle defined by $\mathrm{Fr} \mapsto \Phi_{u,0}$*. The corresponding twist is given by*

$$E^{\mathrm{tw}}\colon\; y^2 = x^3 + x$$

and the corresponding isomorphism is defined over a quadratic extension.

Analogously the cocycle $\mathrm{Fr} \mapsto \Phi_{1,1}$ *corresponds to the twist*

$$E^{\mathrm{tw}}\colon\; y^2 = x^3 - x - 1$$

and the cocycle $\mathrm{Fr} \mapsto \Phi_{1,-1}$ *corresponds to the twist*

$$E^{\mathrm{tw}}\colon\; y^2 = x^3 - x + 1,$$

where both isomorphisms are defined over a cubic extension.

In case n is even, fix $i \in \mathbb{F}_q$ with $i^2 = -1$. The Frobenius conjugacy classes of $E/\mathbb{F}_q$ are

$$C_{1,0} = \{\Phi_{1,0}\}, \qquad C_{-1,0} = \{\Phi_{-1,0}\}, \qquad C_{1,1} = \{\Phi_{1,1}, \Phi_{1,-1}\},$$
$$C_{-1,1} = \{\Phi_{-1,1}, \Phi_{-1,-1}\}, \qquad C_{i,0} = \{\Phi_{i,r} \,|\, r \in \mathbb{F}_3\}, \qquad C_{-i,0} = \{\Phi_{-i,r} \,|\, r \in \mathbb{F}_3\}.$$

The corresponding isomorphisms are defined over a field extension of degree 1, 2, 3, 6, 4, 4, *respectively.*

Equivalently, since we are considering here the number of $\mathbb{F}_{3^n}$-isomorphism classes of elliptic curves with j-invariant 0*, i.e., of supersingular elliptic curves over $\mathbb{F}_{3^n}$, this shows there are* 4 *supersingular curves when n is odd and* 6 *such curves when n is even. This is of course well known; it is consistent with the tables presented in* [15].

Proof. The statements about the j-invariant and about the number of automorphisms are easy; compare, e.g., [21, Appendix A, Proposition 1.2].

Since $\Phi_{u,r}^{-1} = \Phi_{u^{-1},-u^2r}$ and ${}^{\mathrm{Fr}}\Phi_{u,r} = \Phi_{u^3,r^3} = \Phi_{u^{-1},r}$, one can directly calculate the Frobenius conjugacy class of $\Phi_{u,r}$, depending on q being an even or an odd power of 3.

To verify that indeed the curves presented in the statement of the proposition correspond to the given Frobenius conjugacy classes, one needs to use an isomorphism $\psi\colon E \to E^{\mathrm{tw}}$ and check that $\left({}^{\mathrm{Fr}}\psi\right)^{-1} \circ \psi$ is in the Frobenius conjugacy class. For example, with $E^{\mathrm{tw}}\colon y^2 = x^3 + x$ one can use $\psi\colon E \to E^{\mathrm{tw}}$ is given by $(x, y) \mapsto (ix, -iy)$ (with $i^2 = -1$). A direct computation shows that $\left({}^{\mathrm{Fr}}\psi\right)^{-1} \circ \psi = \Phi_{i,0}$. The other cases are done similarly. ■

Note that we only presented explicit equations for the twists in the case of an extension of $\mathbb{F}_3$ of odd degree. If the degree is even, such an equation will in general (as expected) depend on the field $\mathbb{F}_q$.

Since we are considering here the number of $\mathbb{F}_{3^n}$-isomorphism classes of elliptic curves with j-invariant 0, i.e., of supersingular elliptic curves over $\mathbb{F}_{3^n}$, the proposition shows there are 4 supersingular curves when n is odd and 6 such curves when n is even. This is of course well known; it is consistent with the tables presented in [15].

We now more generally consider the case that E/K is an elliptic curve defined over a field K with $\mathrm{char}(K) = 3$ such that $\#\operatorname{Aut}_{\overline{K}}(E) = 12$. This means (compare [21, Appendix A]) that $j(E) = 0$ and E is given by an equation $y^2 = x^3 + ax + b$, where $a, b \in K$. Thus, there exists an isomorphism $\psi\colon E \to E'$, where $E'\colon y^2 = x^3 - x$. We are interested in the possibilities for the field extension where the isomorphism is defined. By [21, Appendix A, Proposition 1.2], we have $\psi(x,y) = (u^2x + r, u^3y)$, where $u^4 = -\frac{1}{a}$ and $r^3 + ar + b = 0$. Thus, we see that the degree of the field extension depends on the existence of a K-rational 2-torsion point on E.

In the case that $E[2](K)$ is trivial, we have $b \neq 0$. As $\psi^{-1}(x,y) = (v^2x + w, v^3y)$ where $v = u^{-1}$ and $w^3 - w - v^6b = 0$, both ψ and ψ^{-1} are defined over the Artin–Schreier extension of $K(u)$ defined by $w^3 - w - v^6b = 0$.

In the case that $E[2](K)$ is non-trivial, we may assume $b = 0$ and any such isomorphism is defined over $K(u)$.

The field $K(u)$ depends in both cases only on a and is a degree four extension if a is not a square in K.

To complete the picture in characteristic three, note that any elliptic curve E/K in characteristic 3 with $j(E) \neq 0$ satisfies $\mathrm{Aut}_{\overline{K}}(E) = \pm 1$ and therefore $H^1(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)) \cong K^\times/K^{\times 2}$. In particular, summarizing most of the discussion above for the special case of a finite field, one obtains the following.

Proposition 2.2. *Let $q = 3^n$ and suppose $E/\mathbb{F}_q$ is an elliptic curve. Then*

$$\#\,\mathrm{Twist}(E/\mathbb{F}_q) = \begin{cases} 2 & \textit{if } j(E) \neq 0, \\ 4 & \textit{if } j(E) = 0 \textit{ and } n \textit{ is odd}, \\ 6 & \textit{if } j(E) = 0 \textit{ and } n \textit{ is even}. \end{cases}$$

3 Twists in characteristic two

In order to describe twists in characteristic two, we start by considering the central example of a supersingular elliptic curve over the field with two elements. As in the case of characteristic three, this is done by computing the Frobenius conjugacy classes in all possible cases for the action of $\mathrm{G}_{\overline{K}/K}$ on $\mathrm{Aut}_{\overline{K}}(E)$. After this description we turn to isomorphisms between an arbitrary elliptic curve over a field with characteristic two and this particular example. Just is was done for characteristic three, the example is formulated as a proposition, as follows.

Proposition 3.1. *The elliptic curve*

$$E/\mathbb{F}_2\colon\ y^2 + y = x^3$$

has $j(E) = 0$ and it has exactly 24 automorphisms. These are described as

$$\begin{array}{rccc} \Phi_{u,r,t}\colon & E & \longrightarrow & E, \\ & (x,y) & \longmapsto & \big(u^2x + r, y + u^2r^2x + t\big), \end{array}$$

where $u \in \mathbb{F}_4^*$, $r \in \mathbb{F}_4$ and $t^2 + t + r^3 = 0$. The action of the Galois group $\mathrm{G}_{\overline{\mathbb{F}_q}/\mathbb{F}_q}$ on $\mathrm{Aut}_{\overline{\mathbb{F}_q}}(E)$ is trivial in case n is even, and nontrivial if n is odd.

In case n is odd, there are exactly three Frobenius conjugacy classes $C_{u,r,t}$ in $\mathrm{Aut}_{\overline{\mathbb{F}}_q}(E)$, namely the conjugacy class $C_{1,0,0}$ containing the identity, the class $C_{1,\omega,\omega}$ containing $\Phi_{1,\omega,\omega}$, and the class C_{1,ω,ω^2} containing Φ_{1,ω,ω^2}. Here $\omega \in \mathbb{F}_4$ is a primitive 3rd root of unity. The two Frobenius conjugacy classes corresponding to non-trivial twists of E over $\mathbb{F}_q$ yield twists of E over $\mathbb{F}_q$ which are isomorphic to E over a degree eight extension of $\mathbb{F}_q$.

In case n is even, the Frobenius conjugacy classes coincide with the usual conjugacy classes in $\mathrm{Aut}_{\overline{\mathbb{F}_q}}(E)$, which are (with $C_{u,r,t}$ denoting the conjugacy class containing $\Phi_{u,r,t}$ and $\omega \in \mathbb{F}_4$ a chosen primitive 3rd root of unity)

$$C_{1,0,0},\ C_{1,0,1},\ C_{\omega^2,0,1},\ C_{\omega,0,1},\ C_{\omega,0,0},\ C_{\omega^2,0,0},\ C_{1,1,\omega}.$$

The twists of $E/\mathbb{F}_q$ corresponding to these conjugacy classes are isomorphic to E over an extension of $\mathbb{F}_q$ of degree 1, 2, 6, 6, 3, 3, 4, *respectively.*

In particular $E/\mathbb{F}_{2^n}$ has two non-trivial twists if n is odd, and six non-trivial twists in case n is even.

Proof. The statements about $j(E)$ and $\mathrm{Aut}(E)$ are immediate; compare [21, Appendix A].

In any automorphism $\Phi_{u,r,t}$ one has $r \in \mathbb{F}_4$ hence $r^3 = 1$ if $r \neq 0$ and $r^3 = 0$ for $r = 0$. So the equality $t^2 + t + r^3$ shows $t \in \mathbb{F}_2$ for $r = 0$ and $t \in \mathbb{F}_4$ for $r \neq 0$. Therefore all automorphisms are defined over $\mathbb{F}_4$.

To obtain the Frobenius conjugacy classes we first assume n is odd, and we write $C_{u,r,t}$ for the Frobenius conjugacy class containing $\Phi_{u,r,t}$. Let $\omega \in \mathbb{F}_4$ be a fixed primitive 3rd root of unity. A direct calculation shows

$$\begin{aligned} C_{1,0,0} &= \left\{\Phi_{u,r,t}^{-1}\Phi_{1,0,0}\Phi_{u^2,r^2,t^2} \,\middle|\, u \in \mathbb{F}_4^*,\ r \in \mathbb{F}_4,\ t^2 + t + r^3 = 0\right\} \\ &= \left\{\Phi_{u^2,ur^2+r,ur} \,\middle|\, u \in \mathbb{F}_4^*,\ r \in \mathbb{F}_4\right\}, \end{aligned}$$

so $C_{1,0,0}$ consists of

$$\begin{aligned} &\big\{\Phi_{1,0,0}, \Phi_{1,0,1}, \Phi_{1,1,\omega}, \Phi_{1,1,\omega^2}, \Phi_{\omega^2,0,0}, \Phi_{\omega^2,\omega^2,\omega}, \\ &\ \Phi_{\omega^2,\omega^2,\omega^2}, \Phi_{\omega^2,0,1}, \Phi_{\omega,0,0}, \Phi_{\omega,\omega,\omega^2}, \Phi_{\omega,0,1}, \Phi_{\omega,\omega,\omega}\big\}. \end{aligned}$$

The other two Frobenius conjugacy classes are given by

$$\begin{aligned} C_{1,\omega,\omega} &= \big\{\Phi_{1,\omega,\omega}, \Phi_{\omega,\omega^2,\omega}, \Phi_{\omega,1,\omega^2}, \Phi_{\omega,\omega,\omega}, \Phi_{\omega^2,1,\omega}, \Phi_{1,\omega^2,\omega^2}\big\}, \\ C_{1,\omega,\omega^2} &= \big\{\Phi_{1,\omega,\omega^2}, \Phi_{\omega,\omega^2,\omega^2}, \Phi_{\omega^2,1,\omega^2}, \Phi_{\omega^2,\omega,\omega}, \Phi_{\omega,1,\omega}, \Phi_{1,\omega,\omega^2}\big\}. \end{aligned}$$

To see that a twist of $E/\mathbb{F}_q$ corresponding to one of the latter two Frobenius conjugacy classes is indeed isomorphic to E over $\mathbb{F}_{q^8}$ and not over a smaller extension of $\mathbb{F}_q$, consider a cocycle defined by $\mathrm{Fr} \mapsto \Phi$ (with Φ in one of the given classes $C_{u,r,s}$). Using the cocycle condition one finds that the cocycle sends Fr^j (for $j \geq 1$) to ${}^{(\mathrm{id}+\mathrm{Fr}+\cdots+\mathrm{Fr}^{j-1})}\Phi$. This is a nontrivial automorphism for $j \leq 7$ and the trivial one for $j = 8$. The assertion about the twists follows.

We now consider the case n is even. The conjugacy classes in $\mathrm{Aut}(E)$ are

$$\begin{aligned} C_{1,0,0} &= \{\Phi_{1,0,0}\}, \\ C_{1,0,1} &= \{\Phi_{1,0,1}\}, \\ C_{\omega^2,0,1} &= \big\{\Phi_{\omega^2,0,1}, \Phi_{\omega^2,1,\omega}, \Phi_{\omega^2,\omega^2,\omega}, \Phi_{\omega^2,\omega,\omega}\big\}, \\ C_{\omega,0,1} &= \big\{\Phi_{\omega,0,1}, \Phi_{\omega,1,\omega^2}, \Phi_{\omega,\omega^2,\omega^2}, \Phi_{\omega,\omega,\omega^2}\big\}, \\ C_{\omega,0,0} &= \big\{\Phi_{\omega,0,0}, \Phi_{\omega,1,\omega}, \Phi_{\omega,\omega^2,\omega}, \Phi_{\omega,\omega,\omega}\big\}, \\ C_{\omega^2,0,0} &= \big\{\Phi_{\omega^2,0,0}, \Phi_{\omega^2,1,\omega^2}, \Phi_{\omega^2,\omega^2,\omega^2}, \Phi_{\omega^2,\omega,\omega^2}\big\}, \\ C_{1,1,\omega} &= \big\{\Phi_{1,1,\omega}, \Phi_{1,1,\omega^2}, \Phi_{1,\omega,\omega}, \Phi_{1,\omega,\omega^2}, \Phi_{1,\omega^2,\omega}, \Phi_{1,\omega^2,\omega^2}\big\}. \end{aligned}$$

So indeed there are exactly 6 non-trivial twists of $E/\mathbb{F}_q$ in this case. The statement about the extension of $\mathbb{F}_q$ over which they will be isomorphic to E is shown exactly as the analogous statement for the odd n case (in fact in the present situation it simply refers to the order of the elements in a certain conjugacy class). ■

We present some comments regarding the argument above. First take $n = 1$, so $q = 2^n = 2$. Since $-1 = \Phi_{1,0,1}$ is in the same Frobenius conjugacy class as the identity, the elliptic curve $E/\mathbb{F}_2$ has no non-trivial quadratic twist. Let us now consider the cubic twists of E. Again we can see that the automorphisms of order 3 are in the same conjugacy class of the identity and thus,

$E/\mathbb{F}_2$ has no non-trivial cubic twists (and as the proposition states, any non-trivial twist of $E/\mathbb{F}_2$ will only be isomorphic to E over extensions of $\mathbb{F}_2$ of degree a multiple of 8).

Explicit equations for the two non-trivial twists of $E/\mathbb{F}_q$, in the case $q = 2^n$ with n odd, are as follows. Let

$$E_1\colon\ y^2 + y = x^3 + x$$

and

$$E_2\colon\ y^2 + y = x^3 + x + 1.$$

These elliptic curves indeed satisfy $j(E_1) = j(E_2) = j(E) = 0$. Moreover counting points over $\mathbb{F}_{2^n}$ (compare [21, Section V.2]) one finds $\#E(\mathbb{F}_{2^n})$ and $\#E_1(\mathbb{F}_{2^n})$ and $\#E_2(\mathbb{F}_{2^n})$ are three distinct numbers whenever n is odd. So indeed the curves E_j are distinct and nontrivial twists of $E/\mathbb{F}_q$. Of course the same conclusion can be obtained by exhibiting an explicit isomorphism $\psi\colon E \to E_j$ and then determining the Frobenius conjugacy class containing ${}^{\mathrm{Fr}}\psi^{-1} \circ \psi$.

We will not try to present equations for all non-trivial twists of $E/\mathbb{F}_q$ in the case $q = 2^n$ with n even. They depend on q. Instead we treat one example.

Let $q = 4$. In this case $\mathrm{Fr} \mapsto -1 = \Phi_{1,0,1}$ defines a non-trivial cocycle class. The corresponding twist is given by

$$E^{\mathrm{tw}}\colon\ y^2 + y = x^3 + \omega$$

(with ω a primitive 3rd root of unity), since

$$\psi\colon\ (x, y) \mapsto (x, y + \tau),$$

with $\tau \in \mathbb{F}_4$ satisfying $\tau^2 + \tau + \omega = 0$, defines an isomorphism $\psi\colon E \to E^{\mathrm{tw}}$, and

$$\left({}^{\mathrm{Fr}}\psi\right)^{-1} \circ \psi = -1.$$

Thus, $E/\mathbb{F}_4$ has a non-trivial quadratic twist.

Let K be an field with $\mathrm{char}(K) = 2$ and consider the elliptic curves $E\colon y^2 + ay = x^3 + bx + c$ with $a \neq 0$ and $E'\colon y^2 + y = x^3$. Since $j(E) = 0 = j(E')$ these elliptic curves are isomorphic and, by Silverman [21, Appendix A, Proposition 1.2], for an isomorphism $\psi\colon E \to E'$ we have $\psi(x, y) = (u^2x + s^2, ay + u^2s + t)$, where $u^3 = a$, $s^4 + as + b = 0$ and $t^2 + at + s^6 + bs^2 + c = 0$. Moreover from the information presented in Proposition 3.1 it follows that in case K is a finite field, such u, s, t exist in an extension of degree at most 8 resp. 6, depending on the action of the Galois group on the automorphism group of E.

Again, we summarize the main results given here for the case of a finite field, as follows. Here as before a crucial remark is that for E/K an elliptic curve in characteristic 2, the automorphism group over the separable closure is ± 1 unless $j(E) = 0$.

Proposition 3.2. *Let $q = 2^n$ and suppose $E/\mathbb{F}_q$ is an elliptic curve. Then*

$$\#\,\mathrm{Twist}(E/\mathbb{F}_q) = \begin{cases} 2 & \textit{if } j(E) \neq 0, \\ 3 & \textit{if } j(E) = 0 \textit{ and } n \textit{ is odd}, \\ 7 & \textit{if } j(E) = 0 \textit{ and } n \textit{ is even}. \end{cases}$$

4 Capitulation of quadratic twists

Let K be a field and $\overline{K}$ a separable closure of K. Given an elliptic curve E/K, the inclusion $\langle -1\rangle \subset \mathrm{Aut}_{\overline{K}}(E)$ induces a map

$$H^1\big(\mathrm{G}_{\overline{K}/K}, \langle -1\rangle\big) \longrightarrow H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big).$$

The set of quadratic twists of E, i.e.,

$$QT(E) = \big\{E^{\mathrm{tw}}/K \,|\, \exists\, L/K \text{ with } [L:K]=2 \text{ such that } E^{\mathrm{tw}} \cong_L E\big\}/_{\cong_K}$$

is a subset of $\mathrm{Twist}(E/K)$; this subset of quadratic twists corresponds to the image of $H^1\big(\mathrm{G}_{\overline{K}/K}, \langle -1\rangle\big)$ in $H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big)$ under the map just given. Here we consider the question whether $E^{\mathrm{tw}} \in QT(E)$ can be isomorphic to E over the ground field. In other words, when does E^{tw} correspond to the trivial element in $H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big)$, under the assumption that it comes from a non-trivial element in the group $H^1\big(\mathrm{G}_{\overline{K}/K}, \langle -1\rangle\big) = \mathrm{Hom}\,\big(\mathrm{G}_{\overline{K}/K}, \mathbb{Z}/2\mathbb{Z}\big)$.

This question is analogous to a similar question in algebraic number theory and in function field arithmetic, namely the so-called capitulation (or principalization) problem for ideals, see, e.g., [2, 3, 10, 16].

Here is a result concerning capitulation of quadratic twists.

Proposition 4.1. *Let E/K be an elliptic curve such that $\mathrm{Aut}_{\overline{K}}(E)$ is abelian. Then the map*

$$i\colon\; H^1\big(\mathrm{G}_{\overline{K}/K}, \langle -1\rangle\big) \longrightarrow H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big)$$

is injective except in the case when $\mathrm{char}(K) \notin \{2,3\}$, $j(E) = 12^3$ and $\mathrm{G}_{\overline{K}/K}$ acts non-trivially on $\mathrm{Aut}_{\overline{K}}(E)$.

Proof. We have the following long exact sequence of groups:

$$\begin{tikzcd}
1 \arrow[r] & H^0\big(\mathrm{G}_{\overline{K}/K}, \langle -1\rangle\big) \arrow[r] & H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) \arrow[dll, "\pi"] \\
H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/\!_{\langle -1\rangle}\big) \arrow[r] & H^1\big(\mathrm{G}_{\overline{K}/K}, \langle -1\rangle\big) \arrow[dl, "i"] & \\
H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) \arrow[r] & H^1\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/\!_{\langle -1\rangle}\big). &
\end{tikzcd}$$

Note that $H^0\big(\mathrm{G}_{\overline{K}/K}, \langle -1\rangle\big) = \mathbb{Z}/2\mathbb{Z}$. By [21, Chapter III, Corollary 10.2], we have the following automorphism groups of an elliptic curve:

1) $\mathrm{Aut}_{\overline{K}}(E) = \langle -1\rangle \cong \mathbb{Z}/2\mathbb{Z}$, when $j(E) \neq 0, 12^3$;
2) $\mathrm{Aut}_{\overline{K}}(E) \cong \mu_4(\overline{K})$, when $j(E) = 12^3$ and $\mathrm{char}(K) \notin \{2,3\}$;
3) $\mathrm{Aut}_{\overline{K}}(E) \cong \mu_6(\overline{K})$, when $j(E) = 0$ and $\mathrm{char}(K) \notin \{2,3\}$.

We consider each case separately.

1. Since $\#\,\mathrm{Aut}_{\overline{K}}(E) = 2$, the Galois group $\mathrm{G}_{\overline{K}/K}$ acts trivially on $\mathrm{Aut}_{\overline{K}}(E)$. Therefore, $\#H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/\!_{\langle -1\rangle}\big) = 1$. Hence, the map i is injective. This proves the proposition in this case.

2. First, suppose $\mathrm{G}_{\overline{K}/K}$ acts trivially on $\mathrm{Aut}_{\overline{K}}(E) \cong \mu_4 = \{1, \zeta_4, \zeta_4^2, \zeta_4^3\}$. Again, here we see $\#H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!\big/_{\langle -1\rangle}\big) = 2$. Hence, the first four groups in the long exact sequence presented in the first lines of this proof have order as indicated in the following diagram

$$1 \longrightarrow 2 \longrightarrow 4 \xrightarrow{\pi} 2 \longrightarrow .$$

This implies that π is surjective; therefore, i is injective. The proposition follows in this case.

Now, suppose $\mathrm{G}_{\overline{K}/K}$ acts non-trivially on $\mathrm{Aut}_{\overline{K}}(E)$. Thus, there exists an automorphism $\sigma \in \mathrm{G}_{\overline{K}/K}$ such that

$$\sigma(1) = 1, \qquad \sigma(\zeta_4) = \zeta_4^3.$$

Therefore, $\#H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) = 2$. Now, the action of σ on

$${}^{\mathrm{Aut}_{\overline{K}}(E)}\!\big/_{\langle -1\rangle} \cong \big\{\{1, \zeta_4^2\}, \{\zeta_4, \zeta_4^3\}\big\}$$

is

$$\sigma\big(\{1, \zeta_4^2\}\big) = \{1, \zeta_4^2\}, \qquad \sigma\big(\{\zeta_4, \zeta_4^3\}\big) = \{\zeta_4, \zeta_4^3\}.$$

We conclude that $\#H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!\big/_{\langle -1\rangle}\big) = 2$. Hence, the first four groups in the long exact sequence presented at the beginning of this proof have order as indicated in the following diagram

$$1 \longrightarrow 2 \longrightarrow 2 \xrightarrow{\pi} 2 \longrightarrow .$$

Thus, π is the constant map; therefore, $\#\mathrm{Ker}(i) = 2$ and i is not injective. The proposition follows in this case.

3. First, if $\mathrm{G}_{\overline{K}/K}$ acts trivially on $\mathrm{Aut}_{\overline{K}}(E) \cong \mu_6 = \langle \zeta_6 \rangle$, then we have $\#H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) = 6$ and $\#H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!\big/_{\langle -1\rangle}\big) = 3$. The first four groups in the long exact sequence from the start of this proof therefore have order

$$1 \longrightarrow 2 \longrightarrow 6 \xrightarrow{\pi} 3 \longrightarrow .$$

This implies that π is surjective; therefore, because the sequence is exact, i is injective.

Now, suppose $\mathrm{G}_{\overline{K}/K}$ acts non-trivially on $\mathrm{Aut}_{\overline{K}}(E)$. Let $\sigma \in \mathrm{G}_{\overline{K}/K}$ acts non-trivially on $\mathrm{Aut}_{\overline{K}}(E)$. Then we have

$$\sigma(1) = 1, \qquad \sigma(\zeta_6) = \zeta_6^5.$$

Thus we get $\#H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) = 2$. The action of σ on

$${}^{\mathrm{Aut}_{\overline{K}}(E)}\!\big/_{\langle -1\rangle} \cong \big\{\{1, \zeta_6^3\}, \{\zeta_6, \zeta_6^4\}, \{\zeta_6^2, \zeta_6^5\}\big\}$$

is given by

$$\sigma\big(\{1, \zeta_6^3\}\big) = \{1, \zeta_6^3\}, \qquad \sigma\big(\{\zeta_6, \zeta_6^4\}\big) = \{\zeta_6^2, \zeta_6^5\}, \qquad \sigma\big(\{\zeta_6^2, \zeta_6^5\}\big) = \{\zeta_6, \zeta_6^4\},$$

implying that $\#H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!\big/_{\langle -1\rangle}\big) = 1$. The first four groups in the long exact sequence used throughout this argument have orders

$$1 \longrightarrow 2 \longrightarrow 2 \xrightarrow{\pi} 1 \longrightarrow .$$

We conclude that π is surjective; hence, i is injective. This completes the proof of the proposition. ■

The condition in Proposition 4.1 that the automorphism group of E should be abelian, means that one excludes only the cases $j(E) = 0$ in $\operatorname{char}(K) \in \{2,3\}$. We briefly consider these two excluded cases here.

Suppose $\operatorname{char}(K) = 2$ and take $E/K\colon y^2 + y = x^3$. As in Section 3 one finds that $\mathrm{G}_{\overline{K}/K}$ acts trivially on $\operatorname{Aut}_{\overline{K}}(E)$ precisely when $\mathbb{F}_4 \subset K$. In that case no capitulation of quadratic twists occurs. However, when Galois acts non-trivially on this automorphism group, then as in the case of a finite field studied in Section 3 where we saw that -1 and 1 are in the same Frobenius conjugacy class, capitulation occurs.

Similarly, suppose $\operatorname{char}(K) = 3$ and take $E\colon y^2 = x^3 - x$. Again, there is capitulation of quadratic twists precisely when the Galois action on the automorphism group is non-trivial, which happens precisely when $\mathbb{F}_9 \not\subset K$.

Example 4.2. Take

$$E/\mathbb{Q}\colon\ y^2 = x^3 - x.$$

Then

$$\operatorname{Aut}_{\overline{\mathbb{Q}}}(E) = \{\pm 1, \pm\iota\},$$

where $\iota\colon E \to E$ is defined by $(x,y) \mapsto (-x, iy)$ for a fixed choice of a primitive 4th root of unity $i \in \overline{\mathbb{Q}}$.

For $d \in \mathbb{Q}^*$ write

$$E^{(d)}\colon\ y^2 = x^3 - d^2x.$$

Then $E^{(d)}$ is a twist of $E/\mathbb{Q}$, since $\psi_d\colon E \to E^{(d)}$ defined as

$$\psi_d(x,y) = \bigl(dx, d\sqrt{d}y\bigr)$$

is an isomorphism between E and $E^{(d)}$.

If $\sigma \in \mathrm{G}_{\overline{\mathbb{Q}}/\mathbb{Q}}$, then

$$\bigl({}^{\sigma}\psi_d\bigr)^{-1} \circ \psi_d = \begin{cases} 1 & \text{if } \sigma\bigl(\sqrt{d}\bigr) = \sqrt{d}, \\ -1 & \text{if } \sigma\bigl(\sqrt{d}\bigr) = -\sqrt{d}. \end{cases}$$

So $E^{(d)}$ corresponds to the cocycle class of

$$\sigma \mapsto \frac{\sigma\bigl(\sqrt{d}\bigr)}{\sqrt{d}} \in \operatorname{Aut}_{\bar{\mathbb{Q}}}(E).$$

In the case $d = -1$, this cocycle is a coboundary, since

$$\frac{\sigma\bigl(\sqrt{-1}\bigr)}{\sqrt{-1}} = ({}^{\sigma}\iota)^{-1} \circ \iota.$$

So $E^{(-1)} \cong E$ over $\mathbb{Q}$, which is, of course, evident from the equation.

Example 4.3. Take q a power of an odd prime, and

$$E/\mathbb{F}_q\colon\ y^2 = x^3 - x.$$

The Galois group $\mathrm{G}_{\overline{\mathbb{F}_q}/\mathbb{F}_q}$ acts non-trivially on $\operatorname{Aut}_{\overline{\mathbb{F}_q}}(E)$ if and only if -1 is not a square in $\mathbb{F}_q$. We have

$$\sqrt{-1} \notin \mathbb{F}_q \iff q \equiv 3 \pmod 4.$$

For $d \in \mathbb{F}_q^*$, define $E^{(d)}/\mathbb{F}_q$ as before. This provides a quadratic twist as in Example 4.2.

If d is not a square and $q \equiv 1 \pmod 4$, then $E^{(d)}$ is the (unique) non-trivial quadratic twist of $E/\mathbb{F}_q$.

If d is not a square and $q \equiv 3 \pmod 4$, then $-d$ is a square. Therefore, we have $E^{(d)} = E^{(-d)} \cong E$ over $\mathbb{F}_q$. So for $q \equiv 3 \pmod 4$, a non-trivial quadratic twist of $E/\mathbb{F}_q$ does not exist.

5 Capitulation of cubic twists

Let E/K be an elliptic curve such that $\mathrm{Aut}_{\overline{K}}(E)$ contains a subgroup C_3 of order 3. This implies $j(E) = 0$ by [21, Chapter III, Corollary 10.2]. Thus, we restrict ourselves in this section to elliptic curves E with $j(E) = 0$. Note that in the case of $\mathrm{char}(K) = 2, 3$ the group $\mathrm{Aut}_{\overline{K}}(E)$ is not abelian; thus, the considered exact sequence is an exact sequence of pointed sets. The non-abelian cohomology needed to describe twists in this situation, is, e.g., described in Serre's books [18, Chapter I, Section 5] and [17, Chapter XIII].

Proposition 5.1. *Let E/K be an elliptic curve with $j(E) = 0$. There is a unique (and therefore normal) subgroup $C_3 \subset \mathrm{Aut}_{\overline{K}}(E)$ of order 3. The map*

$$i\colon\ H^1\big(\mathrm{G}_{\overline{K}/K}, C_3\big) \longrightarrow H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big)$$

is injective except possibly when $\mathrm{char}(K) = 2$.

Proof. 1. First we consider the case $\mathrm{char}(K) \neq 2, 3$. Then $\mathrm{Aut}_{\overline{K}}(E)$ is cyclic of order 6, so indeed C_3 as desired exists and is unique. If $\mathrm{G}_{\overline{K}/K}$ acts trivially on $\mathrm{Aut}_{\overline{K}}(E)$ we have

$$\#H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/_{\mu_3}\big) = 2.$$

In the long exact sequence

$$\begin{tikzcd}
1 \arrow[r] & H^0\big(\mathrm{G}_{\overline{K}/K}, C_3\big) \arrow[r] & H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) \arrow[dll, "\pi"] \\
H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/_{C_3}\big) \arrow[r] & H^1\big(\mathrm{G}_{\overline{K}/K}, C_3\big) \arrow[dl, "i"] & \\
H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) \arrow[r] & H^1\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/_{C_3}\big) &
\end{tikzcd}$$

the orders of the first few groups are

$$1 \longrightarrow 3 \longrightarrow 6 \xrightarrow{\pi} 2 \longrightarrow$$

and thus, π is surjective which implies i is injective.

If on the other hand $\mathrm{G}_{\overline{K}/K}$ acts non-trivially on $\mathrm{Aut}_{\overline{K}}(E)$ then since Galois fixes the -1-map, any $\sigma \in \mathrm{G}_{\overline{K}/K}$ that acts non-trivially has to interchange the two non-trivial elements of C_3. This implies that $\mathrm{G}_{\overline{K}/K}$ acts trivially on ${}^{\mathrm{Aut}_{\overline{K}}(E)}\!/_{\mu_3}$ and thus, in the long exact sequence presented earlier in this proof π is surjective since $\#H^0\big(\mathrm{G}_{\overline{K}/K}, \mu_3\big) = 1$ and $\#H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) = 1$. So again one concludes that i is injective.

2. Let $\mathrm{char}(K) = 3$. This implies $\mathrm{Aut}_{\overline{K}}(E)$ is a semi-direct product $C_3 \rtimes C_4$ of cyclic groups of order 3 and 4 (see [21, Appendix A, Example A.1]). In particular it follows that the

automorphism group has a unique subgroup C_3 of order 3. If $\mathrm{G}_{\overline{K}/K}$ acts trivially on $\mathrm{Aut}_{\overline{K}}(E)$, then i is injective. If $\mathrm{G}_{\overline{K}/K}$ acts non-trivially on $\mathrm{Aut}_{\overline{K}}(E)$ we will consider several cases.

First we consider the case that $\mathrm{G}_{\overline{K}/K}$ acts trivially on C_3. This implies that any non-trivially acting $\sigma \in \mathrm{G}_{\overline{K}/K}$ interchanges the two elements of order 4 in C_4. This implies $\#H^0\big(\mathrm{G}_{\overline{K}/K}, C_3\big) = 3$ and $\#H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) = 6$ and $\#H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/\!_{C_3}\big) = 2$. This gives us the sequence of orders

$$\begin{tikzcd} 1 \arrow[r] & 3 \arrow[r] & 6 \arrow[r, "\pi"] & 2 \arrow[r] & {} \end{tikzcd}$$

from which it follows that π is surjective and thus i is injective.

Now consider the case that all elements of C_4 are fixed under the action of $\mathrm{G}_{\overline{K}/K}$. This implies that any $\sigma \in \mathrm{G}_{\overline{K}/K}$ acting non-trivially on $\mathrm{Aut}_{\overline{K}}(E)$ has to interchange the non-trivial elements of C_3. Therefore, we get

$$\begin{aligned}
&\#H^0\big(\mathrm{G}_{\overline{K}/K}, C_3\big) = 1,\\
&\#H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) = 4,\\
&\#H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/\!_{C_3}\big) = 4.
\end{aligned}$$

Similar to the previous situation this implies that i is injective.

In the case that neither C_3 nor C_4 are elementwise fixed under the action of $\mathrm{G}_{\overline{K}/K}$, we easily get the following sequence of orders

$$\begin{tikzcd} 1 \arrow[r] & 1 \arrow[r] & 2 \arrow[r, "\pi"] & 1 \arrow[r] & {} \end{tikzcd}$$

and thus again, i is injective. ■

So the result says that capitulation of cubic twists does not occur, except possibly in characteristic 2. In fact Proposition 3.2 implies that it also does not occur over finite fields in characteristic two.

6 Capitulation of sextic twists

Let E/K be an elliptic curve such that $\mathrm{Aut}_{\overline{K}}(E)$ has a normal subgroup of order 6. This implies $j(E) = 0$ and $\mathrm{char}(K) \neq 2$. A result analogous to Proposition 5.1 is the following.

Proposition 6.1. *Suppose* $\mathrm{char}(K) \neq 2$ *and let* E/K *be an elliptic curve with* $j(E) = 0$*. There is a unique (and therefore normal) subgroup* $C_6 \subset \mathrm{Aut}_{\overline{K}}(E)$ *of order* 6*. The map*

$$i\colon\ H^1\big(\mathrm{G}_{\overline{K}/K}, C_6\big) \longrightarrow H^1\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big)$$

is injective except in the two cases

1) $\mathrm{char}(K) = 3$ *and* $\mathrm{G}_{\overline{K}/K}$ *acts trivially on* C_6*;*
2) $\mathrm{char}(K) = 3$ *and the only elements in* $\mathrm{Aut}_{\overline{K}}(E)$ *fixed by* $\mathrm{G}_{\overline{K}/K}$ *are* ± 1*.*

Proof. In the case $\mathrm{char}(K) \neq 2, 3$ we have for E as above that $\mathrm{Aut}_{\overline{K}}(E)$ is cyclic of order 6. So the result is trivial in this case.

Now assume $\mathrm{char}(K) = 3$. In this case $\#\,\mathrm{Aut}_{\overline{K}}(E) = 12$ and this automorphism group contains a unique subgroup C_6 of order 6. It is generated by the unique element of order 2 and the subgroup C_3 of order 3 in $\mathrm{Aut}_{\overline{K}}(E)$. In the case that $\mathrm{G}_{\overline{K}/K}$ acts trivially on $\mathrm{Aut}_{\overline{K}}(E)$ we get once again that i is injective. Thus, we now assume that the Galois action is non-trivial.

First case: the Galois action on C_3 is trivial. Then analogously to the case of cubic twists here $\#H^0(\mathrm{G}_{\overline{K}/K}, C_6) = 6$ and $\#H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) = 6$. Obviously, $\mathrm{G}_{\overline{K}/K}$ fixes the residue classes modulo C_6. Thus the group $H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/_{C_6}\big)$ has order 2. This gives us the sequence of orders

$$\begin{tikzcd} 1 \arrow[r] & 6 \arrow[r] & 6 \arrow[r, "\pi"] & 2 \arrow[r] & {} \end{tikzcd} ,$$

implying in the same way as in earlier cases that i is not injective, and the map

$$\pi\colon\ H^0\big(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)\big) \to H^0\big(\mathrm{G}_{\overline{K}/K}, {}^{\mathrm{Aut}_{\overline{K}}(E)}\!/_{H}\big)$$

is constant.

Second case: the Galois action fixes the points in a cyclic order 4 subgroup of automorphisms. Then $\#H^0(\mathrm{G}_{\overline{K}/K}, C_6) = 2$ and $\#H^0(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{K}}(E)) = 4$. Furthermore the action on ${}^{\mathrm{Aut}_{\overline{K}}(E)}\!/_{C_6}$ is trivial, which gives us the sequence of orders

$$\begin{tikzcd} 1 \arrow[r] & 2 \arrow[r] & 4 \arrow[r, "\pi"] & 2 \arrow[r] & {} \end{tikzcd} .$$

As before we conclude that i is injective.

Third case: Neither C_3 nor an order 4 subgroup C_4 are pointwise fixed under the action of $\mathrm{G}_{\overline{K}/K}$. Then only ± 1 are fixed in $\mathrm{Aut}_{\overline{K}}(E)$ and C_6. Further, we see that the action on the quotient group again is trivial. This implies for the orders in the long exact sequence

$$\begin{tikzcd} 1 \arrow[r] & 2 \arrow[r] & 2 \arrow[r, "\pi"] & 2 \arrow[r] & {} \end{tikzcd} .$$

So reasoning as before, π is constant and i is not injective. This case concludes the proof in characteristic 3. ■

In fact a slightly different proof of the same result may be obtained by observing that a sextic twist may be regarded as a cubic twist of a quadratic one. We will not pursue this here.

7 Other twists

Although the techniques used in the previous sections require the (cyclic and Galois stable) subgroup used there to be normal, also in the non-normal cases one can draw conclusions.

We restrict ourselves to providing two examples.

Example 7.1. Take $q = 3^n$ and consider $E/\mathbb{F}_q$ given by $y^2 = x^3 - x$. The automorphism $\Phi_{i,0}\colon (x, y) \mapsto (-x, \sqrt{-1}y)$ generates a Galois stable subgroup H of $\mathrm{Aut}_{\overline{\mathbb{F}_q}}(E)$ of order 4. Then $\mathrm{Fr} \mapsto \Phi_{i,0}$ defines a cocycle in $H^1(\mathrm{G}_{\overline{K}/K}, H)$ and in $H^1(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{\mathbb{F}_q}}(E))$. In Proposition 2.1 we saw that this corresponds to a non-trivial twist.

Example 7.2. Similarly we put $q = 2^n$ and $E/\mathbb{F}_q$ given by $y^2 + y = x^3$. With $\omega \in \overline{\mathbb{F}_q}$ a primitive third root of unity, the automorphism $\Phi_{\omega^2,0,1}\colon (x, y) \mapsto (\omega x, y + 1)$ generates a Galois stable subgroup H of $\mathrm{Aut}_{\overline{\mathbb{F}_q}}(E)$ of order 6, and $\mathrm{Fr} \mapsto \Phi_{\omega^2,0,1}$ defines a cocycle in $H^1(\mathrm{G}_{\overline{K}/K}, H)$ and in $H^1(\mathrm{G}_{\overline{K}/K}, \mathrm{Aut}_{\overline{\mathbb{F}_q}}(E))$.

Proposition 3.1 shows that for odd n this results in a trivial twist, and for n even one obtains a non-trivial twist.

Acknowledgements

It is a pleasure to thank Joe Silverman, John Cremona, Nurdagül Anbar Meidl, and Jan Steffen Müller for helpful comments, advise, and support while preparing this paper. We are especially grateful for the many useful suggestions of the two referees of the first draft of this, which we hope have improved the readability of the text a lot.

References

[1] Badr E., Bars F., Lorenzo García E., On twists of smooth plane curves, *Math. Comp.*, to appear, arXiv:1603.08711.

[2] Bond R.J., Capitulation in abelian extensions of number fields, *Acta Arith.* **179** (2017), 201–232.

[3] Bosca S., Principalization of ideals in abelian extensions of number fields, *Int. J. Number Theory* **5** (2009), 527–539, arXiv:0803.4147.

[4] Bradshaw R., Cremona J., Stein W., Lenox M., Elliptic curves over finite fields, 2005–2011 (sage code), available at `https://github.com/sagemath/sage/blob/master/src/sage/schemes/elliptic_curves/ell_finite_field.py`.

[5] Cassels J.W.S., Diophantine equations with special reference to elliptic curves, *J. London Math. Soc.* **41** (1966), 193–291.

[6] Connell I., Elliptic curve handbook, 1999, Unpublished lecture notes, Chapter 4 discusses twists of elliptic curves, available at `http://www.math.rug.nl/~top/ian.pdf`.

[7] Gouvêa F.Q., Yui N., Arithmetic of diagonal hypersurfaces over finite fields, *London Mathematical Society Lecture Note Series*, Vol. 209, Cambridge University Press, Cambridge, 1995.

[8] Karemaker V., Pries R., Fully maximal and fully minimal abelian varieties, arXiv:1703.10076.

[9] Levy A., Manes M., Thompson B., Uniform bounds for preperiodic points in families of twists, *Proc. Amer. Math. Soc.* **142** (2014), 3075–3088, arXiv:1204.4447.

[10] Li Y., Hu S., Capitulation problem for global function fields, *Arch. Math. (Basel)* **97** (2011), 413–421.

[11] Lombardo D., Lorenzo García E., Computing twists of hyperelliptic curves, arXiv:1611.0485.

[12] Lorenzo García E., Twists of non-hyperelliptic curves of genus 3, arXiv:1604.02410.

[13] Manes M., $\mathbb{Q}$-rational cycles for degree-2 rational maps having an automorphism, *Proc. Lond. Math. Soc.* **96** (2008), 669–696.

[14] Meagher S., Top J., Twists of genus three curves over finite fields, *Finite Fields Appl.* **16** (2010), 347–368.

[15] Schoof R., Nonsingular plane cubic curves over finite fields, *J. Combin. Theory Ser. A* **46** (1987), 183–211.

[16] Schoof R., Washington L.C., Visibility of ideal classes, *J. Number Theory* **130** (2010), 2715–2731, arXiv:0809.5209.

[17] Serre J.-P., Local fields, *Graduate Texts in Mathematics*, Vol. 67, Springer-Verlag, New York – Berlin, 1979.

[18] Serre J.-P., Galois cohomology, *Springer Monographs in Mathematics*, Springer-Verlag, Berlin, 2002.

[19] Silverman J.H., The field of definition for dynamical systems on $\mathbf{P}^1$, *Compositio Math.* **98** (1995), 269–304.

[20] Silverman J.H., The arithmetic of dynamical systems, *Graduate Texts in Mathematics*, Vol. 241, Springer, New York, 2007.

[21] Silverman J.H., The arithmetic of elliptic curves, *Graduate Texts in Mathematics*, Vol. 106, 2nd ed., Springer, Dordrecht, 2009.

[22] Soomro M.A., Algebraic curves over finite fields, Ph.D. Thesis, University of Groningen, 2013, available at `http://hdl.handle.net/11370/024430b9-3e8e-497f-8374-326f014a26e7`.

[23] Stout B.J., A dynamical Shafarevich theorem for twists of rational morphisms, *Acta Arith.* **166** (2014), 69–80.

[24] Top J., Verschoor C., Counting points on the Fricke–Macbeath curve over finite fields, *J. Théor. Nombres Bordeaux*, to appear.