6 p-descent on elliptic curves

6.1 Introduction

Classically, a 2-descent is the most widely used method to bound the rank of the Mordell-Weil group of an elliptic curve E over a number field. Originally, these methods required the existence of rational torsion points or a rational isogeny on E. In [2], Brumer and Kramer presented a method which works independently of the structure of the 2-torsion. As one of the applications, they have produced examples of cubic extensions of $\mathbf{Q}$ whose class group has large 2-torsion.

In some cases, the existence of the 2-part of the Tate-Shafarevich group makes it difficult to determine the rank exactly. It is then helpful to be able to use a prime $p>2$ in the descent computations. The goal of this chapter is to show that the basic ingredient for this, namely the injectivity of the Kummer map, holds in a large class of situations.

Let E/K be an elliptic curve and fix a prime $p\neq$ char (K). Take a field L with $K\subset L\subset\bar{K}$ over which there is a non-trivial p-torsion point $T\in E(L)[p]$. There is a *Kummer map* associated to T (cf. 6.2.1 below),

$$\alpha=\alpha_{T,L}:\ E(K)/pE(K)\ \longrightarrow\ L^*/L^{*p}\ .$$

If all of the p-torsion of E is already rational over $K=L$, the associated Kummer pairing

$$\alpha_{*,K}:\ E[p]\times E(K)/pE(K)\ \longrightarrow\ K^*/K^{*p}$$

is non-degenerate on the left. If K is a number field, the standard local methods give a bound for the size of the image of the Kummer pairing in L^*/L^{*p}. This gives the corresponding bound on $E(K)/pE(K)$ and, hence, on the Mordell-Weil rank of E.

In practice, however, the points of $E[p]=E(\bar{K})[p]$ are rarely defined over K. In fact, for a fixed non-CM elliptic curve, the Galois group $G_{\bar{K}/K}$ acts *irreducibly* on $E(\bar{K})[p]$ for all but finitely many primes p. Our main result is that precisely in this situation, the Kummer map is injective (Theorems 6.3.1, 6.4.2):

Theorem. *Let E/K be an elliptic curve, $p\neq\operatorname{char}K$ a prime and $T\in E[p]$ a non-zero torsion point. Assume that $E[p]$ is an irreducible $G_{\bar{K}/K}$-module. Then for any intermediate field $K(T)\subset L\subset K(E[p])$,*

$$\alpha_{T,L}:\ E(K)/pE(K)\longrightarrow L^*/L^{*p}$$

is injective.

This result extends [13], Exercise 10.9 where the Kummer map is defined and its properties are outlined. Note that the assumption $[L:K]=m^2-1$ of the exercise suggests that m is prime.

The outline of this chapter is as follows. We start by recalling both the cohomological definition of the Kummer map and the more practical geometric definition (Section 6.2).

It is also possible to give a yet equivalent description, in terms of $H^0(C, \mathcal{O}_C^*/\mathcal{O}_C^{*p})$ which makes sense for a non-singular projective curve C of arbitrary genus.

Then we turn to injectivity of the Kummer map starting with the case $L = K(E[p])$ (Section 6.3) and then deducing the general case as a corollary (Section 6.4).

In Section 6.5 we show that in many cases the image of the Kummer map is contained in the kernel of the norm map $N_{L/K}$. This can be used to bound the potential size of this image.

We also discuss the local properties of the image of $\alpha_{T,L}$ in case K is a number field (Section 6.6). The primary question we are interested in here is when for a given prime l of L, the image of α is "trivial at l". Using this one shows that in some cases there is a large part of $E(K)/pE(K)$ which maps into the subgroup of L^*/L^{*p} which corresponds to the p-part of the class group of L.

An example which illustrates our results is presented in Section 6.7.

Notation. The ground field K is assumed to be perfect. We let p denote a prime of $\mathbf{Q}$ different from char K. We denote by $E[p]$ the p-torsion of an elliptic curve E/K over the algebraic closure $\bar{K}$. For a point $T \in E(\bar{K})$ we denote by $K(T)$ the field extension of K inside $\bar{K}$ which is obtained by adjoining the coordinates of T. Similarly, $K(E[p])$ stands for the compositum of $K(T)$ for $T \in E[p]$. This is a finite Galois extension of K. The Galois group of a field extension L/K is denoted by $G_{L/K}$.

Remark. Results similar to those presented here have been obtained independently by Djabri, Schaefer and Smart [3]. The slight difference is that they study the algebra A obtained by adjoining the coordinates of a "generic p-torsion point" rather than the field $L = K(T)$. Thus they are able to prove the injectivity on the Kummer map without using the irreducibility assumption. An advantage of our method, however, is that it is possible to "vary L", which is useful in applying the results of Section 6.5, see Remark 6.5.4.

6.2 The Kummer map

Let E be an elliptic curve over a field K. Fix a prime $p \neq$ char (K). We recall the well-known cohomological description of $E(K)/pE(K)$. We refer to [13], Ch. X for details. Consider the exact sequence of $G_{\bar{K}/K}$-modules

$$0 \longrightarrow E[p] \longrightarrow E(\bar{K}) \xrightarrow{[p]} E(\bar{K}) \longrightarrow 0\,.$$

Taking $G_{\bar{K}/K}$-cohomology yields a long exact sequence, from which we extract

$$0 \longrightarrow E(K)/pE(K) \hookrightarrow H^1(G_{\bar{K}/K}, E[p]) \longrightarrow H^1(G_{\bar{K}/K}, E(\bar{K}))[p] \longrightarrow 0\,. \qquad (46)$$

What interests us here is the first injection. Tracing through the definition of the connecting homomorphism, one can produce the explicit description of this map:

Let $P \in E(K)$. Choose any $Q \in E(\bar{K})$ with $pQ = P$. Then

$$E(K)/pE(K) \ni P \quad \longmapsto \quad (\sigma \mapsto Q^\sigma - Q) \in H^1(G_{\bar{K}/K}, E[p])\,.$$

Note that a different choice of Q affects the cocycle $\sigma \mapsto Q^\sigma - Q$ by a 1-coboundary, so the map is well-defined.

We do a similar computation for the multiplicative group in place of the group of points of E. Take the $G_{\bar{K}/L}$-cohomology of

$$1 \longrightarrow \mu_p \longrightarrow \bar{K}^* \xrightarrow{[p]} \bar{K}^* \longrightarrow 1$$

(here $[p]$ is the p-th power map) and in the same way as above extract

$$1 \longrightarrow L^*/L^{*p} \longrightarrow H^1(G_{\bar{K}/L}, \mu_p) \longrightarrow H^1(G_{\bar{K}/L}, \bar{K}^*) \longrightarrow 1\,.$$

By the Hilbert '90 theorem, the group $H^1(G_{\bar{K}/L}, \bar{K}^*)$ is trivial. So $H^1(G_{\bar{K}/L}, \mu_p) \cong L^*/L^{*p}$.

Now take a point $T \in E[p]$ of order p. Choose an intermediate field $K \subset L \subset \bar{K}$ over which T is defined. Then the Weil pairing on $E[p]$ gives a homomorphism of $G_{\bar{K}/L}$-modules $E[p] \to \mu_p$,

$$E[p] \ni S \quad \longmapsto \quad e_p(S, T) \in \mu_p\,.$$

It induces the map on cohomology,

$$H^1(G_{\bar{K}/K}, E[p]) \longrightarrow H^1(G_{\bar{K}/L}, \mu_p)\,,$$

given explicitly by $\xi \mapsto (\sigma \mapsto e_p(\xi(\sigma), T))$.

The above maps can be combined to (cf. [13], Exc. 10.9)

$$E(K)/pE(K) \longrightarrow H^1(G_{\bar{K}/K}, E[p]) \xrightarrow{\text{Res}} H^1(G_{\bar{K}/L}, E[p]) \longrightarrow H^1(G_{\bar{K}/L}, \mu_p) \cong L^*/L^{*p}\,.$$

Here Res denotes the restriction homomorphism.

Definition 6.2.1. The *Kummer map* $\alpha_{T,L}$ is the composition of the above maps,

$$\alpha_{T,L}: \; E(K)/pE(K) \longrightarrow L^*/L^{*p}\,.$$

It is defined for any point $T \in E[p]$ of order p and a field L which contains $K(T)$.

There is a different description of the Kummer map, which is more geometric in nature and more suitable for actual computations. In case $p = 2$, it was already used by Mordell in the proof of his finiteness theorem ([5]; [6], Ch. 16). Start again with E/K and a non-trivial torsion point $T \in E(K)[p]$. The divisor

$$D = p(T) - p(O)$$

is principal, so there is a rational function $f \in K(E)$ which represents it. The evaluation map

$$e : E(K) \ni \; P \longmapsto f(P) \; \in K^*$$

is defined outside T and O and can be extended by linearity to

$$\operatorname{Div}' E(K) \longrightarrow K^* \, .$$

Here Div' stands for divisors whose support does not contain T or O. Moreover, by Weil reciprocity

$$f(\operatorname{div} g) = g(\operatorname{div} f) = g(p(T) - p(O)) = g((T) - (O))^p \in K^{*p}$$

for any g for which $\operatorname{div} g \in \operatorname{Div}'$. This allows to get rid of “′” in Div' and get a well-defined map which we still denote by e,

$$e : \operatorname{Pic} E(K) \longrightarrow K^*/K^{*p} \, .$$

It also follows that e is a group homomorphism. Finally, using the explicit definition of the Weil pairing, one can show that the map induced by e,

$$E(K)/pE(K) \longrightarrow K^*/K^{*p} \, ,$$

coincides with the Kummer map $\alpha_{T,K}$. For instance, this follows from [11], Theorem 2.3. It is also stated in [13], Exc. 10.9(a).

Also note that the above construction can be generalized to curves of arbitrary genus (see [8], Section 5 and [11], Lemma 2.1).

As an example, consider the $p = 2$ case. Let E be an elliptic curve over a field K with $\operatorname{char} K \neq 2$. Assume that E has a rational 2-torsion point over K and put E in the form

$$Y^2 = (X - t_1)(X - t_2)(X - t_3), \qquad t_1 \in K, \;\; t_2, t_3 \in \bar{K} \, .$$

Let $T = (t_1, 0)$. The function $X - t_1$ has the correct properties, so the Kummer map associated to T is given by

$$\begin{array}{rcc} e : E(K) & \longrightarrow & K^*/K^{*2} \\ (x, y) & \longmapsto & x - t_1 \end{array} \tag{47}$$

for $(x, y) \neq T$ and $\neq O$. It is easy to check that $e(O) = 1$ and $e(T) = (t_1 - t_2)(t_1 - t_3)$. This description is used in the actual computation for 2-descent.

The exceptional values $e(T)$ and $e(O)$ can be made less exceptional: in fact e is given on the whole of E *locally* by invertible regular functions. The functions

$$\begin{array}{rcl} f_1 = & X - t_1 & \text{on} \;\; U_1 = E \setminus \{(t_1, 0), O\} \\ f_2 = & \dfrac{1}{(X - t_2)(X - t_3)} & \text{on} \;\; U_2 = E \setminus \{(t_2, 0), (t_3, 0)\} \end{array}$$

have the property that

$$f_1(P) = f_2(P) \ \in K^*/K^{*2}$$

for every $P \in E(K)$ which lies in $U_1 \cap U_2$, since

$$f_1/f_2 = Y^2 \, .$$

In general, for a non-singular projective curve C/K and a prime p one might ask which maps

$$C(K) \longrightarrow K^*/K^{*p}$$

are locally given by invertible regular functions, defined over K and which differ by p-th powers on the intersections. We can make this precise (after all $C(K)$ might be empty) as follows.

Definition. Let C be a non-singular projective curve over a field K. A *p-map* is a global section of the sheaf $\mathcal{O}_C^*/\mathcal{O}_C^{*p}$. Here $\mathcal{O}_C$ denotes the structure sheaf.

Note that a p-map can be given by an open covering $\{U_i\}$ of C and invertible regular functions f_i on U_i with the property that $f_i/f_j \in H^0(U_i \cap U_j, \mathcal{O}_C^{*p})$.

It turns out that for an elliptic curve $C = E$ the p-maps are exactly the Kummer maps given by some K-rational p-torsion point $T \in E(K)[p]$. More generally, for a curve C of arbitrary genus the p-maps are classified by K-rational p-torsion points in the Picard group of C:

Proposition 6.2.2. *Let C be a non-singular projective curve over a perfect field K. Then*

$$H^0(C, \mathcal{O}_C^*/\mathcal{O}_C^{*p}) \ \cong \ \operatorname{Pic} C(K)[p] \, . \tag{48}$$

Proof. First assume K is algebraically closed. A short exact sequence of sheaves

$$0 \longrightarrow \mathcal{O}_X^*/\mu_p \longrightarrow \mathcal{O}_X^* \longrightarrow \mathcal{O}_X^*/\mathcal{O}_X^{*p} \longrightarrow 0$$

where the left map is taking a function to its p-th power gives a long cohomology sequence

$$0 \longrightarrow K^*/\mu_p \xrightarrow{\cong} K^* \longrightarrow H^0(C, \mathcal{O}_C^*/\mathcal{O}_C^{*p}) \longrightarrow H^1(C, \mathcal{O}_C^*/\mu_p) \longrightarrow H^1(C, \mathcal{O}_C^*) \, .$$

The sheaf μ_p on C is constant, hence flasque (Zariski topology), hence acyclic. Thus

$$0 \longrightarrow H^0(\mathcal{O}_C^*/\mathcal{O}_C^{*2}) \longrightarrow \mathrm{Pic} C \xrightarrow{[p]} \mathrm{Pic} C$$

which gives (48). The case of arbitrary K is obtained by taking $G_{\bar{K}/K}$-invariants. ∎

Example 6.2.3. As an illustration, consider the case $p = 3$. Assume that E/K is given by an equation

$$E: \; y^2 = x^3 + ax + b \, .$$

Let $T = (x_T, y_T) \in E[p]$ be a non-trivial 3-torsion point and let $L = K(T)$. Thus x_T is a root of the 3-division equation,

$$x_T^4 + 2ax_T^2 + 4bx_T - \frac{a^2}{3} = 0$$

and the extension $L/K(x_T)$ is given by

$$y_T^2 - (x_T^3 + ax_T + b) = 0 \, .$$

It is easy to find a function on E which has the divisor $3(T) - 3(O)$. Namely T is an inflection point of E so a linear function which defines the tangent line to T has the required properties. The Kummer map $\alpha_{T,L}$ is thus given (outside T and O) by

$$\alpha_{T,L} : \; E(K)/pE(K) \ni (X, Y) \;\longmapsto\; (Y - y_T) - \frac{3x_T^2 + a}{2y_T}(X - x_T) \;\in L^*/L^{*3} \, .$$

This is in agreement with the formula given in [14], p.309.

6.3 The case of an irreducible action on p-torsion points

Theorem 6.3.1. *Let E/K be an elliptic curve, $p \neq \mathrm{char}(K)$ a prime, $L = K(E[p])$ and $T \in E(\bar{K})$ a point of exact order p. Assume that $G_{\bar{K}/K}$ acts irreducibly on $E[p]$. Then the Kummer map*

$$\alpha_{T,L} : \; E(K)/pE(K) \longrightarrow L^*/L^{*p}$$

is injective.

Proof. First note that $E[p]$ is an irreducible $G_{\bar{K}/K}$-module means that $E[p]$ has no non-trivial $G_{\bar{K}/K}-$invariant subspace. Equivalently, $E[p]$ has no non-trivial $G_{L/K}-$invariant subspace. It is also equivalent to saying that E does not admit a $p-$isogeny defined over K.

The sequence (46) and the corresponding one for $G_{\bar{K}/L}$-cohomology fit into the commutative diagram

$$\begin{tikzcd}
\Phi \arrow[d, hook] & & \\
E(K)/pE(K) \arrow[r, hook] \arrow[d] & H^1(G_{\bar{K}/K}, E[p]) \arrow[r, two heads] \arrow[d, "\mathrm{Res}"] & H^1(G_{\bar{K}/K}, E(\bar{K}))[p] \arrow[d, "\mathrm{Res}"] \\
E(L)/pE(L) \arrow[r, hook] & H^1(G_{\bar{K}/L}, E[p]) \arrow[r, two heads] & H^1(G_{\bar{K}/L}, E(\bar{K}))[p] \, .
\end{tikzcd}$$

In particular, $\alpha_{T,L}$ also equals the composition

$$E(K)/pE(K) \longrightarrow E(L)/pE(L) \longrightarrow H^1(G_{\bar{K}/L}, E[p]) \longrightarrow H^1(G_{\bar{K}/L}, \mu_p) \cong L^*/L^{*p} .$$

Thus an obvious necessary condition for $\alpha_{T,L}$ to be injective is $\Phi = 0$ or, in other words

$$E(K) \cap pE(L) = pE(K) .$$

The fact that this is necessary is of course clear anyway: if $P \in E(K) \cap pE(L)$ then one can choose $Q \in E(L)$ with $pQ = P$, so

$$e_p(Q^\sigma - Q, T) = 1 \quad \text{for all} \quad \sigma \in G_{\bar{K}/L}$$

as $Q^\sigma = Q$ for all σ. Hence P is in the kernel of α. If $P \notin pE(K)$, then α is not injective.

Apply the snake lemma to the diagram above:

$$\begin{tikzcd}
\Phi \arrow[d] & H^1(G_{L/K}, E[p]) \arrow[d, "\mathrm{Inf}"] & H^1(G_{L/K}, E(L))[p] \arrow[d, "\mathrm{Inf}"] \\
E(K)/pE(K) \arrow[r, hook] \arrow[d] & H^1(G_{\bar{K}/K}, E[p]) \arrow[r, two heads] \arrow[d, "\mathrm{Res}"] & H^1(G_{\bar{K}/K}, E(\bar{K}))[p] \arrow[d, "\mathrm{Res}"] \\
E(L)/pE(L) \arrow[r, hook] \arrow[d] & H^1(G_{\bar{K}/L}, E[p]) \arrow[r, two heads] \arrow[d] & H^1(G_{\bar{K}/L}, E(\bar{K}))[p] \arrow[d] \\
E(L)/pE(L)+E(K) & C_1 & C_2
\end{tikzcd} .$$

The kernels form an exact sequence

$$0 \longrightarrow \Phi \hookrightarrow H^1(G_{L/K}, E[p]) \longrightarrow H^1(G_{L/K}, E(L))[p] .$$

So the natural constraint which would imply $\Phi = 0$ is $H^1(G_{L/K}, E[p]) = 0$. This is indeed the case since $G_{L/K}$ acts faithfully and irreducibly on $E[p] \cong \mathbf{F}_p \oplus \mathbf{F}_p$:

Lemma 6.3.2. *Let p be a prime and let $G \subset GL_2(\mathbf{F}_p)$ act irreducibly on a two-dimensional vector space V over $\mathbf{F}_p$ (via the natural action of GL_2). Then $H^1(G, V) = 0$.*

Proof. (cf. [3], Proposition 1). First note that if G does not contain an element of order p then $H^1(G, V)$ is automatically zero as it is annihilated both by $|G|$ and p. Thus assume this is not the case.

First assume $p = 2$. Then $GL_2(V) \cong S_3$ and the action is the usual action of S_3 on the set of 3 elements $V - \{0\}$. Since G acts irreducibly on V (so it has no fixed points on $V - \{0\}$) and it contains an element of order 2, the only possibility is $G = S_3$. The inflation-restriction sequence for the normal subgroup $A_3 \subset S_3$ reads:

$$H^1(S_3/A_3, V^{A_3}) \overset{\mathrm{Inf}}{\longrightarrow} H^1(S_3, V) \overset{\mathrm{Res}}{\longrightarrow} H^1(A_3, V) .$$

Since A_3 has no non-zero invariants on V (so that the group on the left is trivial) and $H^1(A_3, V)$ is trivial as well (being annihilated both by 2 and by 3), we see that $H^1(S_3, V) = 0$ as required.

Now let p be an odd prime. Since G acts irreducibly on V and G has an element of order p, a result of Serre ([12], 2.4, Proposition 15) asserts that G contains $SL_2(\mathbf{F}_p)$, thus $\{\pm 1\} \subset G$. We apply the inflation-restriction sequence for this (normal) subgroup:

$$H^1(G/\pm 1, V^{\pm 1}) \xrightarrow{\text{Inf}} H^1(G,V) \xrightarrow{\text{Res}} H^1(\pm 1, V)\,.$$

Again $\{\pm 1\}$ has no invariants on V and also $H^1(\pm 1, V)=0$ being annihilated both by p and by 2. So $H^1(G,V)=0$. ∎

We continue with the proof of the theorem. The map $\alpha_{T,L}$ becomes the composition

$$E(K)/pE(K) \hookrightarrow E(L)/pE(L) \longrightarrow H^1(G_{\bar{K}/L}, \mu_p)\,.$$

So it remains to show that the second map here is injective. This means that

$$e_p(Q^\sigma - Q, T) = 1 \quad \text{for all} \quad \sigma \in G_{\bar{K}/L}$$

implies $Q \in E(L)$. In other words, it can not happen that for some $Q \notin E(L)$,

$$Q^\sigma - Q \in <T> \subset E[p] \quad \text{for all} \quad \sigma \in G_{\bar{K}/L}\,.$$

If this would be the case, the set $V = \{Q^\sigma - Q \mid \sigma \in G_{\bar{K}/L}\}$ would form a proper nontrivial subspace of $E[p]$. However, the following lemma applied with

$$G = G_{\bar{K}/K}, \quad H = G_{\bar{K}/L}, \quad A = E[p] \quad \text{and} \quad \xi(\sigma) = Q^\sigma - Q$$

shows that V is $G_{L/K}$-invariant. This contradicts the irreducibility assumption. ∎

Lemma 6.3.3. *Let a group G act on an abelian group A, and let $H \lhd G$ act trivially on A. Then for any $\xi \in H^1(G,A)$, the subgroup of A*

$$V = V_\xi = \{\xi(h) \mid h \in H\}$$

is invariant under G (or G/H).

Proof. First note that $\mathrm{Res}(\xi) \in H^1(H,A) = \mathrm{Hom}(H,A)$, so ξ defines a homomorphism $H \to A$, whose image is V (in particular V is a subgroup of A). If we let G act on H by

$$g \cdot h = ghg^{-1}$$

then H becomes a G-module and the important thing is that the map $\xi : H \to A$ becomes a G-homomorphism (it commutes with this action of G). Clearly ξ factors as

$$\xi : \quad H \twoheadrightarrow V \hookrightarrow A\,.$$

Thus to show that V is invariant under G, take $v \in V \subset A$, take $h \in H$ such that $\xi(h) = v$. Then

$$g \cdot v = \xi(g \cdot h) \in V$$

as required. ∎

Remark. By a theorem of Serre ([12], 4.2, Théorème 2), for a curve E without complex multiplication, there are only finitely many primes p for which $G_{\bar{K}/K}$ does not act irreducibly on $E[p]$. Indeed, the theorem asserts that $G_{\bar{K}/K} \to \mathrm{Aut}(E[p])$ $(\cong GL_2(\mathbf{F}_p))$ is surjective for almost all primes. Thus the condition of Theorem 6.3.1 is satisfied for all but finitely many primes provided E has no CM.

6.4 A generalization for subfields of $K(E[p])$

Proposition 6.4.1. *Let E/K be an elliptic curve, p a prime different from* char K *and $T \in E[p]$ a non-trivial point of order p. Let $K(T) \subset L_1 \subset L_2 \subset \bar{K}$ be fields. Then the associated Kummer map α_{T,L_2} factors*

$$\alpha_{T,L_2}: \ E(K)/pE(K) \xrightarrow{\alpha_{T,L_1}} L_1^*/L_1^{*p} \longrightarrow L_2^*/L_2^{*p} \,.$$

Here the second map is induced by the inclusion $L_1 \hookrightarrow L_2$.

Proof. The defining map for α_{T,L_2}

$$E(K)/pE(K) \longrightarrow H^1(G_{\bar{K}/K}, E[p]) \xrightarrow{\mathrm{Res}} H^1(G_{\bar{K}/L_2}, E[p]) \longrightarrow H^1(G_{\bar{K}/L_2}, \mu_p) \cong L_2^*/L_2^{*p}$$

factors as (look at the explicit definition of $\alpha_{T,L}$)

$$\begin{aligned} E(K)/pE(K) \longrightarrow H^1(G_{\bar{K}/K}, E[p]) \xrightarrow{\mathrm{Res}} H^1(G_{\bar{K}/L_1}, E[p]) \longrightarrow \\ \longrightarrow H^1(G_{\bar{K}/L_1}, \mu_p) \xrightarrow{\mathrm{Res}} H^1(G_{\bar{K}/L_2}, \mu_p) \cong L_2^*/L_2^{*p} \,. \end{aligned}$$

It remains to remark that $H^1(G_{\bar{K}/L_1}, \mu_p) \cong L_1^*/L_1^{*p}$ and that the restriction map from $H^1(G_{\bar{K}/L_1}, \mu_p)$ to $H^1(G_{\bar{K}/L_2}, \mu_p)$ is indeed equivalent to the natural map $L_1^*/L_1^{*p} \to L_2^*/L_2^{*p}$ induced by the inclusion $L_1 \hookrightarrow L_2$. ∎

A direct corollary of this proposition is the following generalization of Theorem 6.3.1 to the subfields M of $L = K(E[p])$ over which α can still be defined.

Theorem 6.4.2. *Let E/K be an elliptic curve, p a prime different from* char K *and $T \in E[p]$ a non-trivial point of order p. Let $L = K(E[p])$ and let M be a subfield of L which contains $K(T)$. Assume that $G_{\bar{K}/K}$ acts irreducibly on $E[p]$. Then the Kummer map*

$$\alpha_{T,M}: \ E(K)/pE(K) \longrightarrow M^*/M^{*p}$$

is injective.

Proof. By the proposition above, $\alpha_{T,L}$ factors as

$$\alpha_{T,L}: \quad E(K)/pE(K) \longrightarrow M^*/M^{*p} \longrightarrow L^*/L^{*p} \,.$$

Since the composition is injective, the first map (which is $\alpha_{T,M}$) is injective as well. ∎

6.5 The norm map on the image of the Kummer map

Let E/K be an elliptic curve, $T \in E[p]$ a point of (exact) order p and L a subfield of $K(E[p])$ over which T is defined. We have defined the Kummer map

$$\alpha_{T,L}: \quad E(K)/pE(K) \hookrightarrow L^*/L^{*p}$$

and proved that it is injective under the irreducibility assumption. In this section we show that in many cases the image of $\alpha_{T,L}$ is contained in the kernel of the norm map

$$N_{L/K}: L^*/L^{*p} \longrightarrow K^*/K^{*p} \, .$$

In the next section we study the local behaviour of the image in case of a number field.

We start by describing the action of Galois on the target of the Kummer map.

Lemma 6.5.1. *Let $E/K, p$ and L be as above. For $\tau \in G_{\bar{K}/K}$ the composition*

$$E(K)/pE(K) \quad \overset{\alpha_{T,L}}{\longrightarrow} \quad L^*/L^{*p} \quad \overset{\tau}{\longrightarrow} \quad \tau(L)^*/\tau(L)^{*p} \tag{49}$$

is equal to the Kummer map $\alpha_{T^\tau,\tau(L)}$.

Proof. Recall the geometric description of the Kummer map. The map $\alpha_{T,L}$ is given (locally on E) by invertible regular functions f_i which are defined over L,

$$f_i: E(K) \supset U_i \ni P \longmapsto f(P) \in L^* \, .$$

The composition (49) is then given by the functions f_i^τ. Clearly these also form an element of $H^0(E, \mathcal{O}_E^*/\mathcal{O}_E^{*p})$. Moreover, the principal divisors (f_i^τ) are the conjugates $(f_i)^\tau$. It follows that $\{f_i^\tau\}$ corresponds to the Kummer map defined by T^τ, as required. ∎

Corollary 6.5.2. *Let $E/K, p$ and L be as above. Assume that $E[p](K) = \{O\}$. Then the image of $\alpha_{T,L}$ is contained in the kernel of the norm map (cf. [13], Exc. 10.9(b))*

$$N_{L/K}: L^*/L^{*p} \longrightarrow K^*/K^{*p} \, .$$

Proof. Extend each of the possible embeddings $\bar{\tau}_i : L \to \bar{K}$ to an automorphism $\tau_i \in G_{\bar{K}/K}$. Let $\alpha_{T,L}$ be given by a cocycle $\{f_i\} \in H^0(E, \mathcal{O}_E^*/\mathcal{O}_E^{*p})$. Then $N_{L/K}(\alpha_{T,L})$ is given by a cocycle $\{\prod_\tau f_i^\tau\}$. However this cocycle is defined over K, and hence corresponds to a Kummer map given by some p-torsion point $N \in E[p](K)$. The assumption that E has no non-trivial p-torsion defined over K gives $N = O$, so this Kummer map is trivial. ∎

Example 6.5.3. We continue Example 6.2.3, that is, the $p = 3$ case. Assume for simplicity that the Galois group of $K(E[3])/K$ is isomorphic to the full group $GL_2(\mathbf{F}_3)$. (This is the case for general $E/\mathbf{Q}$.) The chain of subfields

$$K \quad \overset{4}{\subset} \quad K(x_T) \quad \overset{2}{\subset} \quad K(x_T, y_T) = L \quad \overset{6}{\subset} \quad K(E[3])$$

corresponds (via Galois theory) to the chain

$$\begin{pmatrix} * & * \\ * & * \end{pmatrix} \overset{4}{\supset} \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \overset{2}{\supset} \quad \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \quad \overset{6}{\supset} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of subgroups of $GL_2(\mathbf{F}_3)$. The field $K(x_T)$ is the unique non-trivial intermediate field of the field extension L/K. More generally, every proper subgroup of $GL_2(\mathbf{F}_p)$ which contains $\left(\begin{smallmatrix}1 & * \\ 0 & *\end{smallmatrix}\right)$ is of the form $\left(\begin{smallmatrix}H & * \\ 0 & *\end{smallmatrix}\right)$ with H a subgroup of $(\mathbf{Z}/p\mathbf{Z})^*$. This follows from Serre [12], 2.4, Proposition 15.

Clearly $E[p](K(x_T))=0$. So an application of 6.5.2 shows that the Kummer map $\alpha_{T,L}$ lands into the kernel of the norm map

$$N_{L/K(x_T)}: \; L^*/L^{*3} \longrightarrow K(x_T)^*/K(x_T)^{*p}\,.$$

In fact, this can be verified explicitly. The unique non-trivial automorphism of the (quadratic Galois) extension $L/K(x_T)$ sends $T=(x_T,y_T)$ to $-T=(x_T,-y_T)$. The product $\alpha_{T,L}\alpha_{-T,L}$ maps

$$(X,Y) \longmapsto \left[(Y-y_T)-\frac{3x_T^2+a}{2y_T}(X-x_T)\right]\left[(Y+y_T)-\frac{3x_T^2+a}{-2y_T}(X-x_T)\right] = (X-x_T)^3\,.$$

The last equality is an easy symbolic computation. Clearly the map lands into $K(x_T)^{*3}$.

Remark 6.5.4. The result of 6.5.2 can be used to bound the size of the potential image of the Kummer map. More precisely, the image of $\alpha_{T,L}$ is contained in the intersection of the kernels of the norm maps $N_{L/K'}$ where K' varies through all the intermediate fields of the extension L/K over which E has no non-trivial p-torsion. This allows to decrease the amount of computation necessary to compute this image.

6.6 Local analysis of the image of $\alpha_{T,L}$

Let K be a number field, E/K an elliptic curve and $T\in E[p]$ a point of order p. Let L be any subfield of $K(E[p])$ containing $K(T)$. We have defined a map

$$\alpha_{T,L}: \quad E(K)/pE(K) \hookrightarrow L^*/L^{*p}$$

and proved that it is injective in certain cases. Now we study the image of this map. We start with recalling the result that for almost all primes l of L, this image is "trivial at l", i.e. it lands into

$$\{a \in L^*/L^{*p} \mid \operatorname{ord}_l(a) = 0 \mod p\}\,.$$

This is well-known, see for instance [8], Prop. 12.4.

Let L_l be the completion of L at l and K_v the completion of K at the unique prime v of K which l divides. Denote by L_l^{un} and K_v^{un} their unramified closures; thus L_l^{un} contains K_v^{un} and L and is their compositum. By $\mathbf{F}_v$ we will denote the residue field of K_v. We use $\mathcal{O}_v^{\text{un}}$ and m_v^{un} to denote the ring of integers of K_v^{un} and its maximal ideal respectively. Finally, Δ_v denotes the minimal discriminant of E at v.

The Kummer maps for E/K_v and E/K_v^{un} fit into a commutative diagram

$$\begin{tikzcd}
E(K)/pE(K) \arrow[r] \arrow[d] & L^*/L^{*p} \arrow[d] \\
E(K_v)/pE(K_v) \arrow[r] \arrow[d] & L_l^*/L_l^{*p} \arrow[d] \\
E(K_v^{\text{un}})/pE(K_v^{\text{un}}) \arrow[r] & L_l^{\text{un}*}/L_l^{\text{un}*p}
\end{tikzcd} .$$

Assume that for our chosen prime v of K, either $E(K_v)/pE(K_v)$ is trivial or that $E(K_v^{\text{un}})/pE(K_v^{\text{un}})$ is trivial. Then, by the commutativity of the diagram, for any $P \in E(K)/pE(K)$, the image $\alpha_{T,L}(P)$ in L is in $L_l^{\text{un}*p}$. This implies that (and for $l \not| p$ is equivalent to)

$$\text{ord}_l(\alpha_{T,L}(P)) = 0 \mod p\,.$$

Even if the groups $E(K_v)/pE(K_v)$ and $E(K_v^{\text{un}})/pE(K_v^{\text{un}})$ are not trivial, a bound on the size of either of them gives a lower bound on the size of the subgroup of $E(K)/pE(K)$ which lands into $L_l^{\text{un}*p}$. More precisely, we have the following result.

Theorem 6.6.1. *Let K be a number field, E/K an elliptic curve and p a prime. For a prime v of K denote*

$$\delta_v = \min\Big(\dim_{\mathbf{F}_p} E(K_v)/pE(K_v), \dim_{\mathbf{F}_p} E(K_v^{\text{un}})/pE(K_v^{\text{un}})\Big)\,.$$

Let $\delta = \sum_v \delta_v$. Then there is a subgroup $H \subset E(K)/pE(K)$ of $\mathbf{F}_p$-codimension at most δ which lands via the Kummer map

$$\alpha_{T,L}: \quad E(K)/pE(K) \longrightarrow L^*/L^{*p}$$

into the subgroup

$$\{a \in L^*/L^{*p} \mid \text{ord}_l(a) = 0 \mod p \text{ for all } l\}\,.$$

Proof. Clear. ▪

Let us investigate the groups $E(K_v)/pE(K_v)$ and $E(K_v^{\text{un}})/pE(K_v^{\text{un}})$. It turns out that the former group is useful for the primes above p while the latter gives a better estimate for the primes not dividing p.

For the standard structure results for the group of points of an elliptic curve over a complete field we refer to [13], Chapters IV, VII. Let E be defined by a minimal Weierstrass equation at v. There is a reduction map (which we denote by "~")

$$E(K_v) \longrightarrow \tilde{E}(\mathbf{F}_v)\,.$$

Here $\tilde{E}/\mathbf{F}_v$ is the reduced curve. It might be singular or not depending on whether E has good or bad reduction at v. In any case let

$$\tilde{E}_{\text{ns}}(\mathbf{F}_v) = \{R \in \tilde{E}(\mathbf{F}_v) \mid R \text{ is non-singular}\}$$

and

$$E_0(K_v) = \{P \in E(K_v) \mid \tilde{P} \in \tilde{E}_{\mathrm{ns}}(\mathbf{F}_v)\} .$$

Then the following sequences are exact ([13], VII.2.1, VII.2.2)

$$\begin{gathered} 0 \longrightarrow \hat{E}(m_v) \longrightarrow E_0(K_v) \longrightarrow \tilde{E}_{\mathrm{ns}}(\mathbf{F}_v) \longrightarrow 0 \\ 0 \longrightarrow \hat{E}(m_v^{\mathrm{un}}) \longrightarrow E_0(K_v^{\mathrm{un}}) \longrightarrow \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \longrightarrow 0 \ . \end{gathered} \tag{50}$$

Here $\hat{E}$ is the group associated to the formal group of E over K_v. To compare E with E_0, we will also make use of the exact sequences

$$\begin{gathered} 0 \longrightarrow E_0(K_v) \longrightarrow E(K_v) \longrightarrow E(K_v)/E_0(K_v) \longrightarrow 0 \\ 0 \longrightarrow E_0(K_v^{\mathrm{un}}) \longrightarrow E(K_v^{\mathrm{un}}) \longrightarrow E(K_v^{\mathrm{un}})/E_0(K_v^{\mathrm{un}}) \longrightarrow 0 \ . \end{gathered} \tag{51}$$

Finally, the size of the quotient E/E_0 is determined by the Kodaira-Néron theorem.

Theorem (Kodaira, Néron). Let E/K_v be an elliptic curve over a local field. If E has split multiplicative reduction, then $E(K_v)/E_0(K_v)$ is a cyclic group of order $\mathrm{ord}_v(\Delta_v){=}{-}\mathrm{ord}_v(j)$. In all other cases, $E(K_v)/E_0(K_v)$ is a finite group of order at most 4.

Proof. [7], §III.17. ∎

The two propositions below give estimates on the sizes of $E(K_v)/E_0(K_v)$ for arbitrary v and of $E(K_v^{\mathrm{un}})/E_0(K_v^{\mathrm{un}})$ for $v \not| p$.

Proposition 6.6.2. *Let E/K_v be an elliptic curve over a local field. Then*

$$\dim_{\mathbf{F}_p} E(K_v)/pE(K_v) = \dim_{\mathbf{F}_p} E(K_v)[p] + \begin{cases} v(p)\dim_{\mathbf{F}_p}\mathbf{F}_v, & v|p \\ 0, & v \not| p \end{cases} .$$

Proof. Let A be an abelian group for which $[p]: A \to A$ has finite kernel and finite cokernel. Define

$$P(A) = \dim_{\mathbf{F}_p} A/pA - \dim_{\mathbf{F}_p} A[p] .$$

For an exact sequence of abelian groups

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0 \, , \tag{52}$$

an application of the snake lemma to the multiplication by p map on (52) shows that

$$P(B) = P(A) + P(C) \, ,$$

provided $P(A)$ and $P(C)$ are defined. Note also that $P(C) = 0$ if C is finite. Hence $P(B){=}P(A)$ whenever $B \subset A$ is of finite index and $P(B)$ (equivalently $P(A)$) is defined.

For the group of points $A = E(K_v)$ we have a filtration by subgroups of finite index

$$\cdots \subset \hat{E}(m_v^r) \subset \cdots \subset \hat{E}(m_v^2) \subset \hat{E}(m_v) \subset E_0(K_v) \subset E(K_v)\,.$$

Indeed, the subgroup $E_0(K_v) \subset E(K_v)$ is of finite index by the Kodaira-Néron theorem, $E_0(K_v)/\hat{E}(K_v) \cong \tilde{E}_{\mathrm{ns}}(\mathbf{F}_v)$ is finite since $\mathbf{F}_v$ is finite and (cf. [13], IV.3.2a)

$$\hat{E}(m_v^r)/\hat{E}(m_v^{r+1}) \cong m_v^r/m_v^{r+1} \cong \mathbf{F}_v, \quad r \geq 1\,.$$

By [13], IV.6.4 there is an integer $r \geq 1$ for which

$$\hat{E}(m_v^r) \cong \hat{\mathbf{G}}_a(m_v^r) \cong (\mathcal{O}_v, +)\,.$$

Hence

$$P(E(K_v)) = P(\mathcal{O}_v) = \dim_{\mathbf{F}_p} \mathcal{O}_v/p\mathcal{O}_v - 0$$

which equals $v(p)\dim_{\mathbf{F}_p} \mathbf{F}_v$ if $v|p$ and zero otherwise. This gives the assertion of the proposition. ■

Note that the above result is well-known. Our proof in a more general setting can be found in [9], Lemma 3.8 and Prop. 3.9. For an alternative proof, see [8], Lemma 12.10.

Remark 6.6.3. Clearly $\dim_{\mathbf{F}_p} E(K_v)[p] \leq 2$. Moreover, in case $K_v = \mathbf{Q}_p$ and $p \neq 2$, this dimension is at most 1, since $\mu_p \not\subset \mathbf{Q}_p$. So

$$\dim_{\mathbf{F}_p} E(\mathbf{Q}_p)/pE(\mathbf{Q}_p) \leq 2$$

in this case.

Remark 6.6.4. The rough estimate $\dim_{\mathbf{F}_p} E(K_v)[p] \leq 2$ can often be improved. For example, one can apply the multiplication-by-p map to the exact sequences (50) and (51) and look at the kernels. One obtains

$$\dim_{\mathbf{F}_p} E(K_v)[p] \leq \dim_{\mathbf{F}_p} \hat{E}(m_v)[p] + \dim_{\mathbf{F}_p} \tilde{E}_{\mathrm{ns}}(\mathbf{F}_v)[p] + \dim_{\mathbf{F}_p} (E(K_v)/E_0(K_v))[p]\,.$$

For example if $K_v = \mathbf{Q}_p$ and $p \neq 2$, then $\hat{E}(m_v)$ has no p-torsion ([13], IV.6.1.1). If moreover, p is a prime of good reduction for E, then E/E_0 is trivial as well, so for such primes $p > 2$ one finds

$$\dim_{\mathbf{F}_p} E(K_v)[p] \leq \dim_{\mathbf{F}_p} \tilde{E}_{\mathrm{ns}}(\mathbf{F}_v)[p] = \begin{cases} 0, & \tilde{E} \text{ supersingular,} \\ 1, & \tilde{E} \text{ ordinary.} \end{cases}$$

Lemma 6.6.5. *Assume that $v \not| p$. Then $E_0(K_v^{\mathrm{un}})/pE_0(K_v^{\mathrm{un}})$ is trivial.*

Proof. Apply the multiplication-by-p map to the second sequence of (50). We get a commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & \hat{E}(m_v^{\mathrm{un}}) \arrow[r] \arrow[d, "\text{[p]}"] & E_0(K_v^{\mathrm{un}}) \arrow[r] \arrow[d, "\text{[p]}"] & \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \arrow[r] \arrow[d, "\text{[p]}"] & 0 \\
0 \arrow[r] & \hat{E}(m_v^{\mathrm{un}}) \arrow[r] & E_0(K_v^{\mathrm{un}}) \arrow[r] & \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \arrow[r] & 0
\end{tikzcd}$$
.

From the kernel-cokernel sequence extract an exact sequence of cokernels:

$$\hat{E}(m_v^{\mathrm{un}})/p\hat{E}(m_v^{\mathrm{un}}) \longrightarrow E_0(K_v^{\mathrm{un}})/pE_0(K_v^{\mathrm{un}}) \longrightarrow \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v)/p\tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v)\,. \tag{53}$$

The assumption char $\mathbf{F}_v \neq p$ implies that the multiplication-by-p map is an isomorphism $\hat{E}(m_v^{\mathrm{un}}) \to \hat{E}(m_v^{\mathrm{un}})$. So it suffices to show that

$$[p]: \quad \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \longrightarrow \tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v)$$

is surjective. We distinguish the following possibilities of reduction:

- Good reduction. In this case $\tilde{E}/\mathbf{F}_v$ is an elliptic curve, $\tilde{E}_{\mathrm{ns}} = \tilde{E}$ and $[p]$ is surjective on $\bar{\mathbf{F}}_v-$valued points, as it is a non-constant morphism of algebraic curves.
- Multiplicative reduction. Here
$$\tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \cong (\bar{\mathbf{F}}_v^*, *)$$
and $[p]$ is the p-th power map on $\bar{\mathbf{F}}_v^*$, thus surjective.
- Additive reduction. Here
$$\tilde{E}_{\mathrm{ns}}(\bar{\mathbf{F}}_v) \cong (\bar{\mathbf{F}}_v, +)$$
and $[p]$ is the multiplication-by-p map on $\bar{\mathbf{F}}_v$, again surjective (note that char $\mathbf{F}_v \neq p$).

This proves the lemma. ■

Proposition 6.6.6. *Assume that $v \not| p$. Let C denote $E(K_v^{\mathrm{un}})/E_0(K_v^{\mathrm{un}})$ and let Δ_v denote the minimal discriminant of E at v. Then $\dim_{\mathbf{F}_p} E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}}) = \dim_{\mathbf{F}_p} C/pC$ and*

$$\dim_{\mathbf{F}_p} C/pC \begin{cases} = 0, & E \text{ has good reduction at } v, \\ \leq 2, & p = 2, \\ \leq 1, & p = 3, \\ = 1, & p > 3,\ p|\mathrm{ord}_v\Delta_v > 0 \ \text{ and } E \text{ has multiplicative reduction}, \\ = 0, & p > 3,\ p\not|\mathrm{ord}_v\Delta_v > 0 \ \text{ or } E \text{ has additive reduction}. \end{cases}$$

Proof. Apply the multiplication-by-p map to the short exact sequence

$$0 \longrightarrow E_0(K_v^{\mathrm{un}}) \longrightarrow E(K_v^{\mathrm{un}}) \longrightarrow E(K_v^{\mathrm{un}})/E_0(K_v^{\mathrm{un}}) \longrightarrow 0$$

and look at the cokernels. Then

$$E_0(K_v^{\mathrm{un}})/pE_0(K_v^{\mathrm{un}}) = 0 \longrightarrow E(K_v^{\mathrm{un}})/pE(K_v^{\mathrm{un}}) \longrightarrow C/pC \longrightarrow 0\,. \tag{54}$$

The first equality of the lemma follows. The second equality is a direct consequence of the Kodaira-Néron theorem. ■

6.7 An example

We give an example which illustrates our results. The following elliptic curve was found by Fermigier [4] and has rank ≥ 22 over $K = \mathbf{Q}$.

$$\begin{aligned} E_{22}: \quad y^2 + xy + y = x^3 &- 940299517776391362903023121165864\,x \\ &+ 1070736307071974303342529551544927453465112501136 2\,. \end{aligned} \tag{55}$$

In order to apply our results, let us first collect the standard local information. The given model of E_{22} is minimal at all primes and

$$\Delta(E_{22}) = 2^2 3^9 5^2 7^6 13^6 17^4 37^3\, 47293\, p_1\, p_2$$

with

$$\begin{aligned} p_1 &= 2707048491451497 91, \\ p_2 &= 6079465787886433777566471267423137042712273438099 7\,. \end{aligned}$$

We would like to thank Herman te Riele for producing the above factorization. The curve E_{22} is semi-stable at all primes except 17. The reduction types are

$$2\!:\!I_2,\ \ 3\!:\!I_9,\ \ 5\!:\!I_2,\ \ 7\!:\!I_6,\ \ 13\!:\!I_6,\ \ 17\!:\!IV,\ \ 37\!:\!I_3,\ \ 47293\!:\!I_1,\ \ p_1\!:\!I_1,\ \ p_2\!:\!I_1\,.$$

A computation (as in Serre [12], Example 5.9.4) shows that the Galois group of $\bar{\mathbf{Q}}/\mathbf{Q}$ acts on $E[p]$ via the full group $GL_2(\mathbf{F}_p)$ for all p. For a non-trivial point $T \in E[p]$ consider the field $L = \mathbf{Q}(T)$. The degree $[L : \mathbf{Q}]$ is $p^2 - 1$, that is maximal possible. The injectivity theorem 6.4.2 applies for every p and the local result 6.6.1 immediately implies the following:

Proposition 6.7.1. *Let p be a prime and $T \in E_{22}[p]$ a non-trivial point of order p. Let $L = \mathbf{Q}(T)$ and define*

$$C_p = \{a \in L^*/L^{*p} \mid \operatorname{ord}_l(a) = 0 \bmod p, \text{ all } l\} \;\cong\; (\mathbf{Z}/p\mathbf{Z})^{c_p}\,.$$

Then

$$c_p \geq \begin{cases} 16, & p = 2, \\ 15, & p = 3, \\ 19, & p = 17, \\ 20, & p \neq 2, 3, 17. \end{cases}$$

It is interesting to note that such an elliptic curve $E/\mathbf{Q}$ with a large Mordell-Weil rank can be used to produce number fields whose class group has a large p-part. Such examples have been studied in detail for $p = 2$ (see [2]) and for $p = 3$ in case E possesses a rational 3-isogeny (see [14]). The group

$$C_p = \{a \in L^*/L^{*p} \mid \operatorname{ord}_l(a) = 0 \bmod p, \text{ all } l\} \;\cong\; (\mathbf{Z}/p\mathbf{Z})^{c_p}\,.$$

fits into an exact sequence

$$0 \longrightarrow U_L/U_L^p \longrightarrow C_p \longrightarrow H_L[p] \longrightarrow 0$$

where U_L is the group of units of L and H_L is the class group. Hence a lower bound on the size of C_p combined with the knowledge of the size of U_L gives a lower bound on the size of $H_L[p]$.

In our chosen example, this can be done as follows. The field L has 3 real embeddings for $p=2$ and $p-1$ real embeddings for an odd prime p. Moreover, L^* has no p-torsion for odd p. This follows from the fact the the Galois group acts via the full $GL_2(\mathbf{F}_p)$. We have by the Dirichlet unit theorem

$$\dim_{\mathbf{F}_p} U_L/U_L^p = \begin{cases} 3, & p=2, \\ (p^2+p-4)/2, & p>2. \end{cases}$$

A combination of this with the above proposition gives the following bounds for small primes p:

p	2	3	5	7
c_p	≥ 16	≥ 15	≥ 20	≥ 20
$\dim_{\mathbf{F}_p} U_L/U_L^p$	3	4	13	26
$\dim_{\mathbf{F}_p} H_L[p]$	≥ 13	≥ 11	≥ 7	—

These rough estimates become useless for primes $p \geq 7$. However, a more careful analysis on the possible image of the Kummer map, notably the use of 6.5.2, can be used to produce sharper bounds.

For example, take an intermediate field $\mathbf{Q} \subset K \subset L$ such that $E[p](K)=0$. By 6.5.2, the image of the Kummer map lands into the kernel of the norm map $N_{L/K} : L^*/L^{*p} \to K^*/K^{*p}$. In particular, the intersection of this image with the unit part U_L/U_L^p is actually contained in the kernel of

$$N_{L/K}: \ U_L/U_L^p \longrightarrow U_K/U_K^p\,. \tag{56}$$

In this way one can produce better lower bounds on the size of $H_L[p]$. Note, however, that the obvious idea to take $K=\mathbf{Q}$ works only for $p=2$, since U_K/U_K^p is trivial for $p>2$. So one has to consider different fields, such as for instance $K=\mathbf{Q}(x_T)$.

In our chosen example, this works as follows. Let $p>2$ and take $K=\mathbf{Q}(x_T)$ which is a subfield of $L=\mathbf{Q}(T)$ of degree 2. Since $E[p](K)$ is trivial, the image of the Kummer map inside the units is contained in the kernel of (56). The field K has $p-1$ real embeddings for an odd prime p. By the Dirichlet unit theorem,

$$\dim_{\mathbf{F}_p} U_K/U_K^p = \frac{1}{4}(p^2+2p-7)\,.$$

The norm map (56) is surjective. Indeed, consider the map $i: U_K/U_K^p \to U_L/U_L^p$ induced by the inclusion $K \to L$. Then the composition $N_{L/K} \circ i$ is multiplication by $[L:K]=2$, hence an isomorphism $(p>2)$.

A combination of these considerations with Proposition 6.7.1 gives the following bounds for small primes p:

p	2	3	5	7	11
c_p	≥ 16	≥ 15	≥ 20	≥ 20	≥ 20
$\dim_{\mathbf{F}_p} U_L/U_L^p$	3	4	13	26	64
$\dim_{\mathbf{F}_p} U_K/U_K^p$	3	2	7	14	34
$\dim_{\mathbf{F}_p} H_L[p]$	≥ 13	≥ 13	≥ 14	≥ 8	—

A similar argument can also be applied to bound the part of the Kummer map which lands outside the unit group. In this way it is possible to improve the bounds even further.

For instance, consider the family of elliptic curves over $\mathbf{Q}$

$$E_n : \ y^2 = x^3 + nx, \qquad n \in \mathbf{Z} \, .$$

Let $p = 3$, take a non-zero point $T \in E[3]$ and take $L_n = \mathbf{Q}(T)$ (a degree 8 extension of $\mathbf{Q}$). It is not difficult to show that

$$\dim_{\mathbf{F}_3} H_{L_n}[3] \geq \operatorname{rank}_{\mathbf{Q}}(E_n) - 1 \, . \tag{57}$$

This gives a non-trivial estimate already for those $E_n/\mathbf{Q}$ whose Mordell-Weil rank is at least 2. For instance, there are six E_n of rank 2 with $|n| \leq 50$, namely the ones with

$$n = -17, 14, 33, 34, 39, 46.$$

For each of these we have $H_{L_n}[3] \cong \mathbf{Z}/3\mathbf{Z}$, so in these cases the estimate (57) is in fact an equality.