PRIME TORSION IN THE BRAUER GROUP OF AN ELLIPTIC CURVE

By

Charlotte Ure

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Mathematics — Doctor of Philosophy

2019

ABSTRACT

PRIME TORSION IN THE BRAUER GROUP OF AN ELLIPTIC CURVE

By

Charlotte Ure

The Brauer group is an invariant in algebraic geometry and number theory, that can be associated to a field, variety, or scheme. Let k be a field of characteristic different from 2 or 3, and let E be an elliptic curve over k. The Brauer group of E is a torsion abelian group with elements given by Morita equivalence classes of central simple algebras over the function field $k(E)$. The Merkurjev-Suslin theorem implies that any such element can be described by a tensor product of symbol algebras. We give a description of elements in the d-torsion of the Brauer group of E in terms of these tensor products, provided that the d-torsion of E is k-rational and k contains a primitive d-th root of unity. Furthermore, if $d = q$ is a prime, we give an algorithm to compute the q-torsion of the Brauer group over any field k of characteristic different from 2,3, and q containing a primitive q-th root of unity.

To my family.

ACKNOWLEDGMENTS

These past six years of graduate school have been an incredible experience for me. I am still amazed to see how much I have grown both personally and academically with the encouragement and support I received from the people I encountered.

First and foremost, I would like to thank my advisor Rajesh Kulkarni, without whom this thesis would not exist in this form. Thank you for always having an open door and for guiding me throughout this process. Thank you for letting me struggle when I needed to, but especially for encouraging me when I wanted to surrender. Thank you for being not only my advisor and mentor, but also becoming a good friend.

The faculty and staff at Michigan State University have been a constant source of support over the years. I wouldn't have come to Michigan State University without Casim Abbas who originally made me aware of the program. My study was partially supported by the Studienstiftung des Deutschen Volkes. At Michigan State University, I am especially grateful for the work of my committee members: Igor Rapinchuk, Michael Shapiro, Aaron Levin, and George Pappas.

I have encountered numerous wonderful people without whom the days in Wells Hall would have been very dull. Thank you Reshma and Hitesh for countless conversations. Thank you Àkos for always brightening my days with your jokes. Thank you to my first American roommates and good friends Samantha and Allison for making East Lansing feel like home. Thank you Christine, Christos, Dimitris, Michael, Mollee, Rami, Rani, Sami, Sarah, Sebastian, Sugil, Tyler, and countless others for a great time together. Finally, thank you to all my fellow participants of the Student Algebra Seminar at MSU who inspired me to work harder.

I would also like to thank my family for their continued support and for their unconditional belief in my abilities. Here is to my parents Ina and Ewald who are my role models for life long learning. Thank you to my sister Lena for being there whenever I needed her. Thank you Omi Inge, who is always interested in my stories and whose independence continues to be an inspiration to me. Thank you Oma Maria and Opa Seppl, whose unconditional support means the world to me.

My special thanks goes to my fiancé Stevie who can always make me smile!

TABLE OF CONTENTS

KEY TO SYMBOLS

d, q	d integer ≥ 2, q is an odd prime
k	base field of characteristic different from 2 or 3, coprime to d, q
ρ	primitive d-th or q-th root of unity in k
$\overline{F}$	a separable closure of the field F
G_F	the absolute Galois group of the field F
E	an elliptic curve over k
$\oplus, \ominus$	denote the point addition and subtraction on E
$[d], [q]$	multiplication by d or q map on $E(\overline{k})$
M	d-torsion or q-torsion of $E(\overline{k})$
e(.,.)	the Weil pairing on M, section 2.1.3
P, Q	generators of M with $\mathrm{e}(P, Q) = \rho$
$k(E)$	Function field of E
$H^i(F, A)$	the i-th group cohomology of G_F with coefficients in the G_F-module A, section 2.2
res	the restriction map, example 2.2.3
cor	the corestriction map, example 2.2.6
inf	the inflation map, example 2.2.4
$[.]_\rho$	for $\rho^i \in \mu_d$, let $\left[\rho^i\right]_\rho = i \in \mathbb{Z}/d\mathbb{Z}$.
$[.]_\rho^{\mathbb{Z}}$	for $\rho^i \in \mu_d$, let $\left[\rho^i\right]_\rho^{\mathbb{Z}} = i \in \{0, \ldots, d-1\} \subset \mathbb{Z}$.

Chapter 1

Introduction

The Brauer group is an important invariant associated with a field, ring, variety, or a scheme in general. Over a field, its elements are given by Morita equivalence classes of central simple algebras. First introduced by Brauer in the 1920's, the Brauer groups of global fields were completely described by Albert, Brauer, Hasse, and Noether [BNH32]. The Brauer groups of purely transcendental extensions of global fields are easier to understand. They were calculated by the authors in [FSS79]. They deduce that all rational function fields over a fixed global field have isomorphic Brauer groups, independently of their transcendence degree. The definition of a Brauer group was generalized to commutative rings by Auslander and Goldman [AG60]. In the 1960's, Grothendieck described a version of the Brauer group of a scheme using étale cohomology [Gro68a]. It is defined to be $H^2_{\text{ét}}(X, \mathbb{G}_m)$, where $\mathbb{G}_m$ is the sheaf of multiplicative units of the ring of regular functions on X. The Brauer group also has an algebraic incarnation that we denote by $\text{Br}(X)$. Its elements are Morita equivalence classes of sheaves of Azumaya algebras. These are sheaves of $\mathcal{O}_X$-algebras that are étale locally isomorphic to matrix algebras. This realization describes the Brauer group as a torsion abelian group. If a scheme X admits an ample invertible sheaf, the torsion of the cohomological Brauer group coincides with the group of equivalence classes of Azumaya algebras [dJ]. Elements in the Brauer group may also be thought of as transcendental cycles – complements to algebraic cycles. We are interested in $\text{Br}(E)$ for E an elliptic curve.

The Brauer group has proven useful in studying geometric properties of varieties. For example, Artin and Mumford utilized it to give a negative answer to the Lüroth problem in dimension three. They constructed unirational varieties that are not rational using Brauer classes over the function field of the projective space $\mathbb{P}^2$ [AM72]. The Brauer group can also detect arithmetic properties of the underlying variety. Manin defined an obstruction lying in the Brauer group that measures the failure of the Hasse principle for varieties [Man71, Sko01]. Using geometric constructions of Brauer classes, Viray and Creutz described the Brauer-Manin obstruction explicitly in the case of hyperelliptic curves. Using this, they constructed an infinite family of abelian surfaces over $\mathbb{Q}$ with nontrivial Tate-Shafarevich group [CV15].

Throughout this note, let k be a field of characteristic different from 2 and 3 and let E be an elliptic curve over k. We will explore the Brauer group of E. First, recall that the Brauer group of E is a torsion abelian group and therefore it will be enough to describe the torsion ${}_d\mathrm{Br}(E)$, where $d \geq 2$ is a prime power. The Brauer group of E is naturally isomorphic to the unramified Brauer group of the function field $k(E)$ (section 2.2.6 and [CTS07, Theorem 5.11]). Furthermore, Merkurjev and Suslin relate the second Milnor K_2 with the Brauer group in the following theorem from [MS82] and [Mer86].

Theorem 1.0.1 (Merkurjev-Suslin)**.** *Let F be a field and let $d \geq 2$ be an integer. Assume additionally that F contains a primitive d-th root of unity ρ. There is an isomorphism*

$$K_2(F)/dK_2(F) \to {}_d\mathrm{Br}(F)$$

that takes a symbol $\{a, b\}$ *to the symbol algebra*

$$(a,b)_{d,F} = (a,b)_{d,F,\rho} = F\left\langle x, y : x^d = a, y^d = b, xy = \rho yx \right\rangle.$$

We apply this theorem to the case $F = k(E)$ and deduce that every element in the Brauer group of $k(E)$ can be written as a tensor product of symbol algebras over $k(E)$. Our main goal is the following.

Goal 1.0.2. *Let* k *be a field of characteristic different from* 2 *and* 3. *Fix an elliptic curve* E *over* k. *Let* $d \geq 2$ *be an integer coprime to the characteristic of* k *and assume additionally that* k *contains a primitive* d*-th root of unity. Describe generators and relations of* ${}_d\mathrm{Br}(E)$ *as tensor product of symbol algebras over the function field* $k(E)$.

Such a description is available for certain integers d and fields k. In [CG01], Chernousov and Guletskiĭ describe generators and relations of ${}_2\mathrm{Br}(E)$ for any elliptic curve over any field of characteristic different from 2. In particular, they prove the following theorem [CG01, Theorem 3.6].

Theorem 1.0.3. *Let* k *be a field of characteristic different from* 2 *and let* E *be an elliptic curve over* k *defined by the affine equation*

$$y^2 = (x-a)(x-b)(x-c)$$

with $a, b, c \in k$. *Then* ${}_2\mathrm{Br}(E) = {}_2\mathrm{Br}(k) \oplus I$ *and every element in* I *can be presented by a tensor product* $(r, x-b)_{2,k(E)} \otimes (s, x-c)_{2,k(E)}$ *of quaternion algebras with* $r, s \in k^\times$. *Any such algebra is trivial in* I *if and only if it is similar to one of the following*

- $(u-c, x-b)_{2,k(E)} \otimes (u-b, x-c)_{2,k(E)}$, *where* u *is the* x*-coordinate of a point in* $E(k)$ *such that* $u-b \neq 0$ *and* $u-c \neq 0$,
- $(b-c, x-b)_{2,k(E)} \otimes ((b-c)(b-a), x-c)_{2,k(E)}$, *or*
- $((c-a)(c-b), x-b)_{2,k(E)} \otimes (c-b, x-c)_{2,k(E)}$.

Chernousov and Guletskiĭ further describe ${}_2\mathrm{Br}(E)$ if the affine equation $y^2 = f(x)$ for E has one or no roots over k. Note that the two torsion of $E(\overline{k})$ is k-rational if and only if $f(x)$ admits three roots in k. The authors in [CRR16, Section 6] give generators of the d-torsion of the Brauer group of the Jacobian of a curve using a different method. They prove the following theorem.

Theorem 1.0.4. *Let* C *be a smooth projective geometrically irreducible curve of genus* g *over a field* k*. Let* $d \geq 2$ *be an integer coprime to the characteristic of* k *and suppose that* k *contains a primitive* d*-th root of unity. Denote the Jacobian of* C *by* J*. Suppose that* ${}_dJ(\overline{k})$ *is* k*-rational. Fix a basis* $P_1, \dots P_{2g}$ *of* ${}_dJ(k) \cong (\mathbb{Z}/d\mathbb{Z})^{2g}$*. Pick a divisor* $\hat{P}_i$ *representing* P_i *and let* $t_{P_i} \in k(C)$ *be the element with divisor* $d\hat{P}_i$*. Then*

$$ {}_d\mathrm{Br}(k(C))_{ur} = {}_d\mathrm{Br}(k) \oplus I $$

and every element in I *can be written as a tensor product*

$$ \left(a_1, t_{P_1}^{m_1}\right)_{d,k(C)} \otimes \cdots \otimes \left(a_{2g}, t_{P_{2g}}^{m_{2g}}\right)_{d,k(c)}, $$

for some $a_1, \dots, a_{2g} \in k^\times$ *and some integers* $m_1, \dots, m_{2g}$.

In this thesis, we will give a description of ${}_d\mathrm{Br}(E)$ in the following cases:

1. Any d coprime to the characteristic of k, assuming that k contains a primitive d-th root of unity and the d-torsion M of $E(\overline{k})$ is k-rational (theorem 1.0.5).

2. $d = q$ an odd prime, that is coprime to the characteristic of k, assuming only that k contains a primitive q-th root of unity (chapter 6).

Note that we recover the result from [CG01] if the elliptic curve is split and also the result from [CRR16] in the case of an elliptic curve. We now proceed to give our description in the first case.

Theorem 1.0.5. *Let k be a field of characteristic different from 2 and 3. Fix an integer $d \geq 2$ coprime to the characteristic of k and assume that k contains a primitive d-th root of unity. Let E be an elliptic curve over k with k-rational d-torsion M. Fix two generators P and Q of M, and let $t_P, t_Q \in k(E)$ with $\mathrm{div}(t_P) = d(P) - d(0)$ and $\mathrm{div}(t_Q) = d(Q) - d(0)$. Additionally, assume that $t_P \circ [d], t_Q \circ [d] \in \left(k(E)^\times\right)^d$. Then*

$$ {}_d\mathrm{Br}(E) = {}_d\mathrm{Br}(k) \oplus I $$

and every element in I can be represented by a tensor product $(a, t_P)_{d,k(E)} \otimes (b, t_Q)_{d,k(E)}$ for some $a, b \in k^\times$. Furthermore, such a tensor product is trivial if and only if it is similar to one of the following

- $\left(t_Q(P), t_P\right)_{k(E)} \otimes \left(\frac{t_P(P \oplus Q)}{t_P(Q)}, t_Q\right)_{k(E)}$,
- $\left(\frac{t_Q(P \oplus Q)}{t_Q(P)}, t_P\right)_{k(E)} \otimes \left(t_P(Q), t_Q\right)_{k(E)}$, *or*
- $\left(t_Q(R), t_P\right)_{k(E)} \otimes \left(t_P(R), t_Q\right)_{k(E)}$ *for some* $R \in E(k) \setminus \{0, P, Q\}$.

Remark 1.0.6. *We may drop the assumption that* $t_P \circ [d], t_Q \circ [d] \in \left(k(E)^\times\right)^d$ *in the previous theorem. In this case our relations become*

$$\left(\frac{t_Q(R \oplus S)}{t_Q(S)}, t_P\right)_{k(E)} \otimes \left(\frac{t_P(R \oplus S)}{t_P(S)}, t_Q\right)_{k(E)}$$

for some $R \in E(k)$ *and* $S \in E(\overline{k})$ *is any point so that the fraction exists and is nonzero.*

Proof. Let $t_P, t_Q \in k(E)$ with $\mathrm{div}(t_P) = d(P) - d(0)$ and $\mathrm{div}(t_Q) = d(Q) - d(0)$. Fix some point $P' \in E(\overline{k})$ with $[d]P' = E(k)$. There exists $g_P \in \overline{k}(E)$ with $\mathrm{div}\,(g_P) = [d]^*(P) - [d]^*(0) = \sum_{R \in M} \left(P' \oplus R\right)$. Note that the divisor is invariant under the action of the Galois group G_k and therefore we may choose $g_P \in k(E)$. Furthermore, since the divisors coincide, there is some $\lambda \in \overline{k}$ so that $g_P^d = \lambda t_P \circ [d] \in k(E)^d$. For any $R \in E(k)$

$$\lambda t_P(R) = \frac{\lambda t_P(R \oplus S)}{\lambda t_P(S)} = \frac{t_P(R \oplus S)}{t_P(S)},$$

where S is any other point so that t_P is nonzero and well-defined. □

Now, let q be an odd prime not equal to the characteristic of k and suppose that k contains a primitive q-th root of unity. We give an algorithm to describe ${}_q\mathrm{Br}(E)$ explicitly in chapter 6. Consider the standard Galois representation

$$\Psi : G_k \to \mathrm{Aut}(M) = GL_2\left(\mathbb{F}_q\right)$$

and denote the fixed field of its kernel by L. Then L is the smallest Galois extension of k so that M is L-rational. Note that the degree of L over k divides the order of $GL_2\left(\mathbb{F}_q\right)$, which is $(q+1)^2 q(q-1)$. We consider three cases for the degree of L over k:

1. $q \nmid [L : k]$

   We describe generators and relations in ${}_q\mathrm{Br}(E)$ using that restriction followed by corestriction is an isomorphism (section 4.2 and section 5.2).

2. $q = [L : k]$

   In this case, the composition of restriction and corestriction is the zero map. We use instead the inflation restriction exact sequence to determine generators and relations of ${}_q\mathrm{Br}(E)$ (section 4.3 and section 5.3).

3. $q \mid [L : k]$

   We combine the results from the previous two cases to get a description of ${}_q\mathrm{Br}(E)$ (section 4.4 and section 5.4).

We now proceed to review the main ideas we will use to determine the Brauer group. For any integer $d \geq 2$, there is a split exact sequence

$$0 \longrightarrow {}_d\mathrm{Br}(k) \longrightarrow {}_d\mathrm{Br}(E) \longrightarrow {}_qH^1(k, E(\overline{k})) \longrightarrow 0\,, \tag{1.1}$$

which is induced by the Hochschild-Serre spectral sequence (for more details, see section 2.3). We need an explicit splitting to this sequence on the right. Consider the Kummer sequence

$$0 \longrightarrow M \longrightarrow E(\overline{k}) \xrightarrow{[d]} E(\overline{k}) \longrightarrow 0 \tag{1.2}$$

and the induced sequence on group cohomology

$$0 \longrightarrow E(k)/[d]E(k) \longrightarrow H^1(k, M) \xrightarrow{\delta} {}_qH^1(k, E(\overline{k})) \longrightarrow 0\,. \tag{1.3}$$

We will define a map $\epsilon : H^1(k, M) \to {}_d\mathrm{Br}(E)$ that induces the desired split. This map is given by the following composition

$$\epsilon : \begin{array}{c} H^1(k,M) \xrightarrow{\sim} H^1_{\text{ét}}(\mathrm{Spec}(k), M) \xrightarrow{p^*} H^1_{\text{ét}}(E,M) \\ \xrightarrow{-\cup[\mathcal{T}]} H^2_{\text{ét}}(E, M\otimes M) \xrightarrow{\mathrm{e}} H^2_{\text{ét}}(E,\mu_d) \longrightarrow {}_d\mathrm{Br}(E) \end{array}, \tag{1.4}$$

where p^* is the morphism induced by the structure map $p : E \to \mathrm{Spec}\, k$, $\mathcal{T}$ is the torsor given by multiplication by d on the elliptic curve (see chapter 3), and e is the map induced by the Weil-pairing (see section 2.1.3). Denote by I the image of ϵ. We deduce that

$$ {}_d\mathrm{Br}(E) = {}_d\mathrm{Br}(k) \oplus I.$$

Further, an element in $H^1(k, M)$ becomes trivial under ϵ if and only if it is in the image of δ from sequence 1.1.

In [Sko01] and [Sko99], the author describes the map ϵ abstractly in the more general setting of an abelian variety X and any torsor $\mathcal{T}$ on X. He further proves that such an ϵ induces the desired split. We review his abstract proof in section 3.3. In this thesis, we make this construction explicit and prove directly that the map ϵ induced by the cup-product induces a split.

This thesis is organized as follows. In chapter 2, we review background material that will be used throughout this work. For example, we discuss some facts about elliptic curves, cohomology, Brauer groups, and symbol algebras as necessary for the proofs in the following chapters. We also fix notation that will be used throughout this work. In chapter 3, we

describe the torsor given by multiplication by d on the elliptic curve. We also calculate the cocycle corresponding to this torsor at the generic point. Furthermore, we describe the general theory behind our main result and justify it using derived categories. In chapter 4, we explore the algorithm to calculate generators of the Brauer group. We describe these generators provided that M is k-rational. We then proceed to describe the generators of the prime torsion in various cases. Finally, in chapter 5 we give the relations in the torsion of the Brauer group. We summarize our results and give a complete algorithm to determine the odd prime torsion in the Brauer group in chapter 6. Lastly, we determine the prime torsion of the Brauer group in various examples in chapter 7.

Chapter 2

Background

This chapter contains background material that will be used throughout this work. We first discuss properties of isogenies of elliptic curves and the Weil pairing. In a second part, we review some general results on group cohomology and étale cohomology. We further connect these to the notions of torsors and the Brauer group. We proceed to define the unramified Brauer group of a field. Finally, we describe an exact sequence, that will prove useful to determine the Brauer group of an elliptic curve.

2.1 Elliptic Curves

Let E be an elliptic curve defined over a field k of characteristic different from 2 and 3. Then E can be described by an affine equation

$$y^2 = x^3 + Ax + B$$

with $A, B \in k$. The discriminant $\Delta = -16\left(4A^3 + 27B^2\right)$ of E is nonzero. Furthermore, E is an abelian variety with identity the point $0 = [0 : 1 : 0]$ at infinity. We denote the pointwise addition on $E(\overline{k})$ by $\oplus$ and the pointwise subtraction by $\ominus$.

2.1.1 Torsion Points

Let d be a natural number and fix an algebraic closure $\overline{k}$ of k. We denote by

$$[d] : E(\overline{k}) \to E(\overline{k})$$

$$R \mapsto \underbrace{R \oplus \cdots \oplus R}_{d\text{-times}}$$

the multiplication by d map on the elliptic curve. The kernel of $[d]$ are the d-torsion points of $E(\overline{k})$, which is denoted by M. We extend our definition of multiplication to $[-d] = [-1] \circ [d]$. Further, $[0]$ is the constant map to 0.

We now review division polynomials, which are a computational tool to determine M.

Proposition/Definition 2.1.1. *For any integer d, $d \geq 2$ and $P = (x_1, y_1) \in E(k)$, there are polynomials $\psi_n \in k[x, y]$ for $n \in \mathbb{Z}_+$ so that*

$$[d]P = \left(x_1 - \frac{\psi_{d-1}(x_1, y_1)\psi_{d+1}(x_1, y_1)}{\psi_d^2(x_1, y_1)}, \frac{\psi_{2d}(x_1, y_1)}{2\psi_d^4(x_1, y_1)} \right).$$

These polynomials are explicitly given by

$$\begin{aligned}
\psi_1(x, y) &= 1, \\
\psi_2(x, y) &= 2y, \\
\psi_3(x, y) &= 3x^4 + 6Ax^2 + 12Bx - A^2, \\
\psi_4(x, y) &= 4y \left(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3 \right), \\
\psi_{2m+1}(x, y) &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \qquad \textit{for } m \geq 2 \textit{ and} \\
\psi_{2m}(x, y) &= \left(\frac{\psi_m}{2y} \right) \left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 \right), \qquad \textit{for } m \geq 3.
\end{aligned}$$

Proof. See for instance [Lan78, Ch. 2 §1]. □

Example 2.1.2. *Let $P = (x_1, y_1) \in E(\overline{k})$. Then P is a two-torsion point if and only if $P = -P$. If E is given by the affine equation $y^2 = (x-a_1)(x-a_2)(x-a_3)$ with $a_1, a_2, a_3 \in k$, then*

$$_2E(\overline{k}) = \{0, (a_1, 0), (a_2, 0), (a_3, 0)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Example 2.1.3. *Let $P = (x_1, y_1) \in E(\overline{k})$. Then P is a three-torsion point if and only if $P = -[2]P$. This is equivalent to*

$$x_1 = x_1 - \frac{3x_1^4 + 6Ax_1^2 + 12Bx_1 - A^2}{4y_1^2} = x_1 - \frac{3x_1^4 + 6Ax_1^2 + 12Bx_1 - A^2}{4\left(x_1^3 + Ax_1 + B\right)},$$

which is true if and only if

$$3x_1^4 + 6Ax_1^2 + 12Bx_1 - A^2 = 0.$$

Let $x_1, \ldots, x_4$ be the four distinct zeros of this polynomial, and let $y_i = \sqrt{x_i^3 + Ax_i + B}$, then

$$_3E(\overline{k}) = \{0, (x_i, y_i), (x_i, -y_i) : 1 \leq i \leq 4\} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

2.1.2 Isogenies

Let E_1 and E_2 be two elliptic curves defined over a field k. An isogeny is a morphism $\phi : E_1 \to E_2$ of curves such that $\phi(0) = 0$. It follows that an isogeny is a group homomorphism on the set of points [Sil09, Chapter III, Theorem 4.8]. We denote by $\phi^* : k(E_2) \to k(E_1)$ the induced map on function fields. If ϕ is constant, we set the degree of ϕ to be zero. If it

is not constant, the degree of ϕ is the degree of the field extension

$$\deg \phi = [k(E_1) : \phi^* k(E_2)] .$$

Furthermore, we denote by $\deg_s \phi$ the separable degree of the field extension and by $\deg_i \phi$ the inseparable degree. Finally, let $P \in E_1(\overline{k})$. The ramification index of ϕ at P, denoted by $e_\phi(P)$ is

$$e_\phi(P) = \operatorname{ord}_P \left(\phi^* t_{\phi(P)} \right),$$

where $t_{\phi(P)}$ is a uniformizer at $\phi(P)$. The following classical theorem can for instance be found in [Sil09, Theorem 4.10].

Proposition 2.1.4. *Let $\phi : E_1 \to E_2$ be a nonzero isogeny between elliptic curves.*

1. *For every $Q \in E_2(k)$, the number of preimages of Q under ϕ is equal to the degree $\deg_s \phi$. Furthermore, for every $P \in E_1(k)$, $e_\phi(P) = \deg_i \phi$.*

2. *There is an isomorphism*

$$\ker(\phi) \to \operatorname{Aut}\left(\overline{k}(E_1)/\phi^*\overline{k}(E_2)\right) : T \mapsto \tau_T^*,$$

   where τ_T is the translation by T map, $\tau_T : E(\overline{k}) \to E(\overline{k}) : R \mapsto R \oplus T$.

3. *Suppose that ϕ is separable, then ϕ is unramified, the number of elements in the kernel is equal to the degree of ϕ, and $\overline{k}(E_1)$ is a Galois extension of $\phi^*\overline{k}(E_2)$.*

Example 2.1.5. *Let $d \geq 2$ be an integer and suppose that the characteristic of k is coprime to d. Denote the d-torsion of $E(\overline{k})$ by $M \cong \mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/d\mathbb{Z}$. Multiplication by $[d]$ is a degree d^2 map and $\overline{k}(E)/[d]^*\overline{k}(E)$ is a Galois extension of degree d^2 (for more details, see also*

[Sil09, Chapter III]). Furthermore, $k(E)/[d]^*k(E)$ is Galois of degree d^2 provided that M is k-rational.

2.1.3 Weil Pairing

Let E be an elliptic curve over k and let $D = \sum n_R R \in \mathrm{Div}(E)$ be a divisor. By [Sil09, Chapter III, Corollary 3.5], D is a principal divisor if and only if $\sum_{R \in E(\overline{k})} n_R = 0$ and $\sum_{R \in E(\overline{k})} [n_R]R = 0$, where the first sum is regular addition in the integers and the second sum is given by addition on the elliptic curve.

A key tool in the study of elliptic curves is the Weil pairing whose construction we will now review. For more details, see also [Sil09, Section III.8]. Let $d \geq 2$ be an integer and let P be a d-torsion point on E. As before, denote by M the d-torsion of $E(\overline{k})$. As discussed before, there exists some $f_P \in \overline{k}(E)$ so that

$$\mathrm{div}(f_P) = d(P) - d(0).$$

Now let $P' \in E(\overline{k})$ such that $[d]P' = P$. Since $\sum_{R \in M}(P' \oplus R) = [d^2]P' = [d]P = 0$, there exists some $g_P \in \overline{k}(E)$ such that

$$\mathrm{div}(g_P) = [d]^*(P) - [d]^*(0) = \sum_{R \in M} \left((P' \oplus R) - (R)\right).$$

Since the divisors coincide, we may assume that $f_P \circ [d] = g_P^d$. For $Q \in M$ define the Weil-pairing of P and Q as

$$\mathrm{e}(Q, P) = \frac{g_P(X \oplus Q)}{g_P(X)},$$

where $X \in E(k)$ is any point so that $g_P(X)$ and $g_P(X \oplus Q)$ is defined and nonzero. The Weil-pairing takes values in the set of d-th roots of unity.

Example 2.1.6 (example 2.1.5, contd.)**.** *Let $P, Q \in M$ and let g_P and g_Q be defined as before, then*

$$\tau_Q^*(g_P) = \mathrm{e}(P, Q) g_P, \tag{2.1}$$

where τ_Q is the translation by Q map, $\tau_Q : E(\overline{k}) \to E(\overline{k}) : R \mapsto R \oplus Q$.

2.2 Cohomology

In this section, we set up our cohomological notation. For more details, see [Ser79, Ch. VII §5], [NSW08], or [GS17].

2.2.1 Group Cohomology for abstract groups

Throughout this section let G be a group and let A be an abelian group. Assume that G acts on A on the left via $g.a$.

Let C_i be the set of of maps $\bigtimes_{i=1}^{n} G \to A$. The coboundary map $d : C_i \to C_{i+1}$ is given by

$$\begin{aligned} df\left(g_1, \ldots, g_{i+1}\right) &= g_1 . f\left(g_2, \ldots, g_{i+1}\right) \\ &+ \sum_{j=1}^{j=i} (-1)^j f\left(g_1, \ldots, g_j g_{j+1}, \ldots, g_{i+1}\right) + (-1)^{i+1} f\left(g_1, \ldots, g_i\right). \end{aligned} \tag{2.2}$$

A direct computation shows that $d^2 = 0$ and thus (C_i, d) is a complex. Elements in the image of d are called cocycles and elements in the kernel of d are cochains. The i-th group cohomology, denoted $H^i(G, A)$, is the quotient of cocycles by cochains in C_i.

Example 2.2.1. *A 1-cocycle is a map $f : G \to A$ satisfying $f(gh) = g.f(h) + f(g)$ for all $g, h \in G$. We also call these elements crossed homomorphism. A crossed homomorphism is trivial if there exists some $a \in A$ such that $f(g) = g.a - a$ for all $g \in G$.*

Example 2.2.2. *A 2-cocycle is a map $f : G \times G \to A$ such that $g.f(g', g'') - f(gg', g'') + g(g, g'g'') - f(g, g') = 0$ for all $g, g', g'' \in G$. Such a cocycle is trivial if and only if there is a map $\tilde{f} : G \to A$ such that $f(g, h) = g.\tilde{f}(h) - \tilde{f}(gh) + f(g)$ for all $g, h \in G$.*

2.2.2 Maps on Group Cohomology

Let G and G' be finite groups. Fix a G-module A and a G'-module A'. Let $\phi : G \to G'$ and $\psi : A \to A'$ be group homomorphisms. We say that ϕ and ψ are compatible if

$$\psi\left(\phi(g).a\right) = g.\psi(g)$$

for all $g \in G$ and $a \in A$. A pair (ϕ, ψ) of compatible morphisms induces a map on cohomology given by post- and precomposition

$$(\phi, \psi)_i^* : \ H^i(G, A) \xrightarrow{f \mapsto f \circ \phi} H^i(G', \phi^* A) \xrightarrow{f \mapsto \psi \circ f} H^i(G', A') \ .$$

Example 2.2.3 (Restriction)**.** *Suppose that H is a subgroup of G. The inclusion of H into G is compatible with the identity on A. The induced homomorphism* $\mathrm{res} : H^i(G, A) \to H^i(H, A)$ *is called the restriction homomorphism.*

Example 2.2.4 (Inflation)**.** *If H is a normal subgroup of G, we denote by A^H the subgroup of A of elements fixed by H. The identity on G is compatible with the inclusion of A^H*

into A. The induced homorphism $\inf : H^i\left(G/H, A^H\right) \to H^i(G, A)$ *is called the inflation homomorphism.*

Example 2.2.5 (Conjugation, action on H^n)**.** *Let $H \subset G$ be a subgroup, A a G-module, and B an H-submodule of A. For any fixed $\sigma \in G$ the morphisms $\sigma^{-1}H\sigma \to H : h \mapsto \sigma h \sigma^{-1}$ and $B \to \sigma^{-1}B : b \mapsto \sigma^{-1}b$ are compatible and induce isomorphisms*

$$\sigma_* : H^n(H, B) \to H^n(\sigma^{-1}H\sigma, \sigma^{-1}B)$$

called conjugation*. This defines an action of G (or if H is normal in G of G/H) on $H^n(H, A)$.*

Example 2.2.6 (Corestriction)**.** *Suppose that H is a subgroup of G. For every right coset $c \in H\backslash G$ fix a coset representative $\overline{c} \in c \subset G$. On the level of cocycles the corestriction* $\mathrm{cor} : C^i(H, A) \to C^i(G, A)$ *is given by*

$$\mathrm{cor}(f)(g_1, \ldots, g_i) = \sum_{c \in H\backslash G} \overline{c}^{-1} f\left(\overline{c}g_1\overline{cg_1}^{-1}, \ldots, \overline{c}g_i\overline{cg_i}^{-1}\right).$$

The following propositions relating inflation, restriction, and corestriction will be useful for our calculations in chapter 4.

Proposition 2.2.7. *Let H be a normal subgroup of G and let A be a G-module. Then the following sequence is exact*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{\inf} H^1(G, H) \xrightarrow{\mathrm{res}} H^1(H, A).$$

Proof. See [Ser79, Ch. VII §6, Proposition 4]. □

Proposition 2.2.8. *Let H be a subgroup of G of finite index and let A be a G-module. Then the composition*

$$H^i(G, A) \xrightarrow{\text{res}} H^i(H, A) \xrightarrow{\text{cor}} H^i(G, A)$$

coincides with multiplication by $[G : H]$.

Proof. See [Ser79, Ch. VII §7, Proposition 6]. □

Definition 2.2.9 (cup-product)**.** *Let G be a group and A and B be G-modules. The* cup-product *on the level of cocycles is given by*

$$H^n(G, A) \times H^m(G, B) \to H^{n+m}(G, A \otimes B)$$

$$f \cup g\,(\sigma_1, \ldots \sigma_{n+m}) = f\,(\sigma_1, \ldots, \sigma_n)\,\sigma_n g\,(\sigma_{n+1}, \ldots \sigma_{m+n})\,.$$

2.2.3 Group Cohomology for Profinite Groups

In this section, we extend the previous definitions of group cohomology to profinite groups. Recall that a profinite group G is the inverse limit $\varprojlim G_\alpha$ of an inverse system of finite groups $\{G_\alpha\}$. Without loss of generality we may take G_α to be a quotient G/U_α of G by an open normal subgroup U_α.

Example 2.2.10. *Let K over k be a Galois extension. The Galois group* $\mathrm{Gal}(K/k)$ *is the inverse limit of the inverse system of the Galois groups of finite subextensions and as such is a profinite group.*

A profinite group $G = \varprojlim G_\alpha$ admits a natural topology as follows. Consider the discrete topology on G_α and the induced product topology on $\prod G_\alpha$. We endow G with the subspace topolgy of the product. A continuous G-module is a G-module A so that the stabilizer of each $a \in A$ is open in G.

Definition 2.2.11. *Let $G = \varprojlim G_\alpha$ be a profinite group with $G_\alpha = G/U_\alpha$ and let A be a continuous G-module. Then A^{U_α} is a G_α-module. Consider the inflation maps*

$$\inf_\alpha^\beta : H^i\left(G_\alpha, A^{U_\alpha}\right) \to H^i\left(G_\beta, A^{U_\beta}\right)$$

as in example 2.2.4. Define the i-th group cohomology $H^i_{cont}(G, A)$ as the direct limit of the system $\left(H^i\left(G_\alpha, A^{U_\alpha}\right), \inf_\alpha^\beta\right)$.
For the absolute Galois group G_k of a field k, we denote $H^i(k, A) = H^i_{cont}(G_k, A)$.

Remark that by construction of direct limits as a quotient of the direct sum, for every $f \in H^i_{\text{cont}}(G, A)$ there exists some α so that $f \in H^i\left(G_\alpha, A^{U_\alpha}\right)$. We use this identification throughout the following chapters, particularly for $H^i(k, A)$.

Let H be a closed subgroup of a profinite group G and A a continuous G-module. The restriction map $\text{res} : H^i_{\text{cont}}(G, A) \to H^i_{\text{cont}}(H, A)$ is defined as the direct limit of the usual restriction on group cohomology (example 2.2.3). If H is open in G, the continuous corestriction is defined similarly and if H is a closed normal subgroup, we can construct continuous inflation maps. Furthermore, there is a continuous cup product induced by the cup product in definition 2.2.9. Finally, propositions 2.2.7 and 2.2.8 can be recovered for profinite cohomology [GS17, Chapter 4.2 and 4.3].

2.2.4 Torsors and H^1

We now proceed to describe the correspondence between torsors and elements in the first cohomology group. For more details, see [Sko01]. Let A be an algebraic group defined over a field k. A k-torsor under A is a non-empty k-variety T equipped with a right-action of A

so that $T(\overline{k})$ is a principal homogeneous space under $A(\overline{k})$. This means, that the map

$$T(\overline{k}) \times A(\overline{k}) \to T(\overline{k}) \times T(\overline{k})$$

$$(t, a) \mapsto (t, t.a)$$

is an isomorphism.

There is a bijection

$$H^1(k, A) \leftrightarrow \left\{ \begin{array}{c} k\text{-torsors under } A \\ \\ \text{up to isomorphism} \end{array} \right\}$$

that is explicitly given as follows. Let T be a k-torsor under A. Choose a $\overline{k}$-point x_0 of T. By the definition of k-torsor, for any $\sigma \in G_k$, there exists a unique $a_\sigma \in A(\overline{k})$ so that $\sigma(x_0) = x_0.a_\sigma$. The map $\sigma \mapsto a_\sigma$ defines the cocycle in $H^1(k, A)$ corresponding to T.

Let X be a variety over k. An X-torsor under an X-group scheme $\mathcal{A}$ is a scheme $\mathcal{T}$ over X together with an $\mathcal{A}$-action compatible with the projection to X that is étale-locally trivial. As before, there is a one-to-one correspondence between X-torsors under $\mathcal{A}$ and elements of the étale cohomology $H^1_{\text{ét}}(X, \mathcal{A})$.

Theorem 2.2.12 (Colliot-Thélène–Sansuc)**.** *Assume that $\overline{k}[X]^\times = \overline{k}^\times$. Let $\mathcal{S}$ be a G_k-module and denote by $\mathcal{M} = Hom_{k-groups}(\mathcal{S}, \mathbb{G}_m)$ the dual of $\mathcal{S}$. There is an exact sequence*

$$0 \longrightarrow H^1_{ét}(\operatorname{Spec} k, \mathcal{M}) \xrightarrow{p^*} H^1_{ét}(\mathcal{A}, \mathcal{M}) \xrightarrow{\mathsf{type}} Hom_k\left(\mathcal{M}, \operatorname{Pic}(\overline{\mathcal{A}})\right) \longrightarrow H^2_{ét}(\operatorname{Spec} k, \mathcal{M}),$$

where p^* is the map induced by the structure morphism $p : \mathcal{A} \to \operatorname{Spec} k$.

If $\mathsf{type}(\mathcal{T}) = \lambda$ for a torsor $\mathcal{T}$, we say that $\mathcal{T}$ has type λ.

Proof. This is the sequence of low degree terms for the spectral sequence of local to global Ext. For more details, see for instance [CTS87, Theorem 1.5.1 and Equation 2.0.2] or [Sko01, Theorem 2.3.6 and Corollary 2.3.9]. □

Example 2.2.13. *A d-covering of an abelian variety X is a pair $(\mathcal{T}, \psi)$, where $\mathcal{T}$ is a k-torsor under X and $\psi : \mathcal{T} \to X$ is a morphism such that $\psi(x.t) = dx + \psi(t)$ for any $t \in \mathcal{T}(\overline{k}), x \in X(\overline{k})$. Let λ be the composition*

$$\lambda : {}_dX^\vee(\overline{k}) \longrightarrow X^\vee(\overline{k}) = \mathrm{Pic}^0(\overline{X}) \longrightarrow \mathrm{Pic}(\overline{X})$$

of the natural injection followed by the inclusion, where $X^\vee$ denotes the dual abelian variety of X. By [Sko01, Proposition 3.3.4 (a)], any d-covering is an X-torsor under ${}_dX$ of type *λ, and vice versa.*

Example 2.2.14. *Multiplication by d on X determines a d-covering $(X, [d])$, and therefore an X-torsor of* type *λ by the previous proposition.*

2.2.5 The Brauer Group, Symbol Algebras, and H^2

In this section, we describe the correspondence between the Brauer group and the second cohomology group. Let F be a field and let $d \geq 2$. We say that two central simple algebras A and B are Morita equivalent if there exist some $n, m \in \mathbb{N}_0$ so that $A \otimes M_n(F)$ and $B \otimes M_m(F)$ are isomorphic as F-algebras. Elements in the Brauer group are given by equivalence classes of central simple algebras modulo Morita equivalence and the group structure is given by the tensor product. There is a group isomorphism between $\mathrm{Br}(F)$ and $H^2(F, \overline{F}^\times)$. We will describe the correspondence for a finite Galois extension K/F. For further details see for instance [GS17].

Definition 2.2.15 (Crossed Product Algebra)**.** *Let K/F be a finite Galois extension with Galois group G and let f be a cocycle representing an element in $H^2(G, K^\times)$. Consider the F-vector space $A = F\langle x_g : g \in G\rangle$ with multiplication $\lambda x_g = x_g g(a)$ and $x_g x_h = f(g,h)x_{gh}$. This turns A into a finite dimensional central simple algebra over F.*

From now on suppose that the field F contains a primitive d-th root of unity ρ. Fix an isomorphism $[.]_\rho : \mu_d \to \mathbb{Z}/d\mathbb{Z}$ with $\left[\rho^i\right]_\rho = i$. Furthermore, identify $\mathbb{Z}/d\mathbb{Z}$ with the subset $\{0, \ldots, d-1\}$ of the integers and denote the image of ρ^i under the composition by $\left[\rho^i\right]_\rho^{\mathbb{Z}} = i \in \mathbb{Z}$.

Definition 2.2.16. *Let $a, b \in F^\times$. The symbol algebra is the F-algebra*

$$(a,b)_{d,F} = (a,b)_{d,F,\rho} := F\left\langle x, y : x^d = a, y^d = b, xy = \rho yx \right\rangle.$$

It is easy to show that $(a,b)_{d,F}$ is a central simple algebra over F.

Example 2.2.17. *Let $a, b \in F^\times$. The element in $H^2(F, \overline{F}^\times)$ corresponding to the symbol algebra $(a,b)_{d,F,\rho}$ can be represented by the cocycle*

$$(\gamma, \tau) \mapsto \begin{cases} a & \text{if } \left[\frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} + \left[\frac{\tau\left(\sqrt[d]{b}\right)}{\sqrt[d]{b}}\right]_\rho^{\mathbb{Z}} \geq d \\ 1 & \text{else} \end{cases}.$$

For more details, see [Rei03, Chapter 7 §29].

The following cocycle representing the symbol algebra $(a,b)_{d,F}$ will prove more useful for our purposes.

Proposition 2.2.18. *Let M be the d-torsion of an elliptic curve E with generators P and Q. Assume that the Weil-pairing satisfies $\mathrm{e}(P,Q) = \rho$. Let $a, b \in F^\times$, then the symbol algebra $(a,b)_{d,F}$ can be represented by the cocycle*

$$(\gamma, \tau) \mapsto \mathrm{e}\left(\frac{\gamma\left(\sqrt[d]{a}\right)}{\left(\sqrt[d]{a}\right)} P, \frac{\gamma\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)} Q \right)^{-1}.$$

Proof. Consider the map

$$g : \gamma \to \sqrt[d]{a}^{\left[\frac{\gamma\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)}\right]_\rho^{\mathbb{Z}}}.$$

The differential of g is

$$\begin{aligned} dg(\gamma,\tau) &= \gamma\left(\sqrt[d]{a}^{\left[\frac{\tau\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)}\right]_\rho^{\mathbb{Z}}} \right) \sqrt[d]{a}^{\left[\frac{\gamma\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)}\right]_\rho^{\mathbb{Z}}} \sqrt[d]{a}^{-\left[\frac{\gamma\tau\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)}\right]_\rho^{\mathbb{Z}}} \\ &= \begin{cases} a\left(\frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}\right)^{\left[\frac{\tau\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)}\right]_\rho} & \text{if } \left[\frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} + \left[\frac{\tau\left(\sqrt[d]{b}\right)}{\sqrt[d]{b}}\right]_\rho^{\mathbb{Z}} \geq d \\ \left(\frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}\right)^{\left[\frac{\tau\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)}\right]_\rho} & \text{else} \end{cases} \\ &= \begin{cases} a\,\mathrm{e}\left(\frac{\gamma\left(\sqrt[d]{a}\right)}{\left(\sqrt[d]{a}\right)} P, \frac{\gamma\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)} Q\right) & \text{if } \left[\frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} + \left[\frac{\tau\left(\sqrt[d]{b}\right)}{\sqrt[d]{b}}\right]_\rho^{\mathbb{Z}} \geq d \\ \mathrm{e}\left(\frac{\gamma\left(\sqrt[d]{a}\right)}{\left(\sqrt[d]{a}\right)} P, \frac{\gamma\left(\sqrt[d]{b}\right)}{\left(\sqrt[d]{b}\right)} Q\right) & \text{else} \end{cases} \end{aligned}$$

Subtracting this trivial cocycle from the cocycle in example 2.2.17 gives the desired result. □

As mentioned before, these definitions can be generalized to the Brauer group of a variety

or a scheme, see [Mil80, Chapter IV] for details. A famous result of Gabber [dJ] states that the Brauer group defined as equivalence classes of Azumaya algebras coincides with the torsion of $H^2_{\text{ét}}(X, \mathbb{G}_m)$ if X can be endowed with an ample invertible sheaf.

2.2.6 The unramified Brauer group

An important subgroup of the Brauer group of a field, is the unramified Brauer group. In this section, we review its definition and some basic facts about it. For more details, see [Sal99, Chapter 10]. First, let R be a discrete valuation domain domain with field of fractions K. Denote by $v : K^\times \to \mathbb{Z}$ the valuation defined by R. Let π be a prime with $v(\pi) = 1$. Denote by $\hat{K}$ the completion of K with respect to v. Let $\overline{R} = R/\pi R$ and denote by p the characteristic of $\overline{R}$. Let K_{ur} be the maximal unramified extension of the completion $\hat{K}$. The following result given in [Sal99, Theorem 10.1] will help us define the ramification map.

Theorem 2.2.19. *Any element in* $\mathrm{Br}(\hat{K})$ *of order prime to* p *is split by* K_{ur}.

For a prime p and an abelian group A, denote by A' the prime-to-p part. Extend the valuation v to $v : K_{ur} \to \mathbb{Z}$. By [Ser79, p. 28] the valuation map is compatible with the action of $\mathrm{Gal}\left(K_{ur}/\hat{K}\right)$, where the action on $\mathbb{Z}$ is trivial. Define the ramification map as the composition

$$\begin{aligned}
&\mathrm{Br}(K)' \longrightarrow \mathrm{Br}(\hat{K})' \xrightarrow[\text{theorem 2.2.19}]{\sim} H^2\left(\mathrm{Gal}\left(K_{ur}/\hat{K}\right), K_{ur}^\times\right)' \\
\mathrm{ram}_R : \quad &\xrightarrow{v} H^2\left(\mathrm{Gal}\left(K_{ur}/\hat{K}\right), \mathbb{Z}\right)' \xrightarrow{\sim} H^1\left(\mathrm{Gal}\left(K_{ur}/\hat{K}\right), \mathbb{Q}/\mathbb{Z}\right)' \\
&\xrightarrow{\sim} \mathrm{Hom}\left(\mathrm{Gal}\left(K_{ur}/\hat{K}\right), \mathbb{Q}/\mathbb{Z}\right)',
\end{aligned}$$

where the second to last map is the inverse of the coboundary induced by the exact sequence $0 \to \mathbb{Z} \to \mathbb{Z} \to \mathbb{Q}/\mathbb{Z} \to 0$. It can be shown [Sal99, Theorem 10.3] that the ramification fits

in the exact sequence

$$0 \longrightarrow \mathrm{Br}(R)' \longrightarrow \mathrm{Br}(K)' \xrightarrow{\mathrm{ram}_R} \mathrm{Hom}\left(\mathrm{Gal}\left(K_{ur}/\hat{K}\right), \mathbb{Q}/\mathbb{Z}\right)' \longrightarrow 0\,.$$

We will now return to the general setting. Let k be a fixed ground field, and let F be a field extension of k. Let $\mathcal{R}_F$ be the set of discrete valuation rings containing k that have field of fraction F.

Definition 2.2.20. *The unramified Brauer group of F (with respect to k) is*

$$\mathrm{Br}_{ur}(F) = \bigcap_{R \in \mathcal{R}_F} (\textit{Image of } \mathrm{Br}(R) \to \mathrm{Br}(F))\,.$$

We will use the following identification throughout this work.

Theorem 2.2.21. *Let X be a projective regular variety over k with function field $k(X)$. Then $\mathrm{Br}(X)$ equals $\mathrm{Br}_{ur}\, k(X)$.*

Proof. See for instance [CTS07, Theorem 5.11] or [Sal99, Proposition 10.5 (c)]. □

2.3 An exact sequence

In this section, we describe the maps in the exact sequence 1.1 explicitly. Consider the Hochschild-Serre spectral sequence [Mil80, III.2.20]

$$H^i\left(k, H^j\left(\overline{E}, \mathbb{G}_m\right)\right) \Rightarrow H^{i+j}\left(E, \mathbb{G}_m\right).$$

Its sequence of low degree terms is

$$0 \longrightarrow \mathrm{Br}(k) \xrightarrow{i} \mathrm{Br}(E) \xrightarrow{r} H^1\left(k, E\left(\overline{k}\right)\right) \longrightarrow 0\,, \tag{2.3}$$

where the first map sends the class of a central simple algebra A to the class of $A \otimes k(E)$. For more details on this sequence, see also [Fad56] and [Lic69]. The second map is more complicated. Let $\alpha \in \mathrm{Br}(E)$. Using Tsen's theorem we view α as an element in $H^2\left(G_k, \overline{k}(E)^\times\right) \cong \mathrm{Br}\, k(E)$. Consider the exact sequence

$$0 \longrightarrow \overline{k}(E)^\times \longrightarrow \mathrm{Prin}(\overline{E}) \longrightarrow \mathrm{Div}(\overline{E}) \longrightarrow 0\,,$$

where $\mathrm{Prin}(\overline{E})$ denotes the set of pricipal divisors on $\overline{E}$ and $\mathrm{Div}(\overline{E})$ is the set of divisors on $\overline{E}$. The sequence induced on group cohomology is

$$H^2(G_k, \overline{k}(E)^\times) \longrightarrow H^2(G_k, \mathrm{Prin}(\overline{E})) \longrightarrow H^2(G_k, \mathrm{Div}(\overline{E}))\,,$$

where the first map takes α to some α' in the kernel of the second map. Now consider the degree sequence

$$0 \longrightarrow \mathrm{Div}^0(\overline{E}) \longrightarrow \mathrm{Div}(\overline{E}) \longrightarrow \mathbb{Z} \longrightarrow 0\,,$$

where $\mathrm{Div}^0(\overline{E})$ is the group of degree zero divisors. Note that $H^1(G_k, \mathbb{Z}) = 0$ and therefore the map

$$H^2(G_k, \mathrm{Div}^0(\overline{E})) \longrightarrow H^2(G_k, \mathrm{Div}(\overline{E}))$$

is injective. Finally, the exact sequence

$$0 \longrightarrow \mathrm{Prin}(\overline{E}) \longrightarrow \mathrm{Div}^0(\overline{E}) \longrightarrow E(\overline{k}) \longrightarrow 0$$

induces an exact sequence

$$1 \longrightarrow H^1(G_k, E(\overline{k})) \longrightarrow H^2(G_k, \mathrm{Prin}(\overline{E})) \longrightarrow H^2(G_k, \mathrm{Div}^0(\overline{E}))\ .$$

The element α' is in the kernel of the second map, and therefore there exists a unique $\alpha'' \in H^1(G_k, E(\overline{k}))$ with image α'. Set $r(\alpha) = \alpha''$.

This completes the description of the exact sequence (2.3). We will use this explicit description to prove that the map ϵ induced by the cup product (eq. (4.1)) induces a split.

Chapter 3

Torsor given by multiplication by d

Let k be a field of characteristic different from 2 or 3. Let $d \geq 2$ be an integer coprime to the characteristic of k. Assume additionally that k contains a primitive d-th root of unity ρ. Fix an isomorphism $[.]_\rho : \mu_d \to \mathbb{Z}/d\mathbb{Z}$ with $\left[\rho^i\right] = i$. Furthermore, for $\rho^i \in \mu_d$, let $\left[\rho^i\right]_\rho^{\mathbb{Z}} = i \in \{0, \ldots, d-1\} \subset \mathbb{Z}$. Let E be an elliptic curve over k and denote its d-torsion by M. This chapter contains a cocycle description of the torsor given by multiplication by d on E. Fix two generators P and Q of M. Denote by $\mathrm{e}(.,.)$ the Weil pairing (section 2.1.3) and assume that $\mathrm{e}(P,Q) = \rho$. Let $t_P, t_Q \in \overline{k}(E)$ with $\mathrm{div}(t_P) = d(P) - d(0)$ and $\mathrm{div}(t_Q) = d(Q) - d(0)$.

3.1 Over a field with rational torsion

Assume throughout this section that M is k-rational. We may assume that $t_P, t_Q \in k(E)$ since its divisor is invariant under the Galois action of G_k. Let $\mathcal{T}$ be the torsor given by multiplication by d on E as defined in section 2.2.4.

Proposition 3.1.1. *The pull-back $\eta^*(\mathcal{T})$ along the generic point $\eta : \mathrm{Spec}\, k(E) \to E$ corresponds to the element in $H^1(k(E), M)$ given by the cocycle*

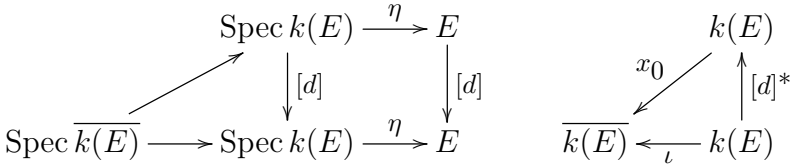
$$\gamma \mapsto \left[\frac{\gamma(\alpha_Q)}{\alpha_Q}\right]_\rho P - \left[\frac{\gamma(\alpha_P)}{\alpha_P}\right]_\rho Q,$$

where $\alpha_P, \alpha_Q \in \overline{k(E)}$ with $\alpha_P^d = t_P$ and $\alpha_Q^d = t_Q$.

Proof. For the correspondence between torsors and elements in H^1 see section 2.2.4. Let $P' \in E(\overline{k})$ so that $[d]P' = P$. Then there is some $g_P \in \overline{k}(E)$ with

$$\operatorname{div}(g_P) = [d]^*(P) - [d]^*(0) = \sum_{R \in M} \left((P' \oplus R) - (R)\right).$$

Note that we may choose $g_P \in k(E)$ since the divisor is invariant under the action of the absolute Galois group of k. Now $\operatorname{div}\left(g_P^d\right) = \operatorname{div}([d]^* t_P)$ and thus we may assume that $g_P^d = [d]^* t_P$. Similarly we find $g_Q \in k(E)$ with $g_Q^d = [d]^* t_Q$. Now consider the pullback of $\mathcal{T}$ along the generic point $\eta : \operatorname{Spec} k(E) \to \operatorname{Spec} k$. Fix a $\overline{k(E)}$-point x_0 of this pullback, i.e. a map of algebras so that $x_0 \circ [d]^* = \iota$, where $\iota : k(E) \to \overline{k(E)}$ is the inclusion.



After possibly renaming α_P and α_Q, we may assume that $x_0(g_P) = \alpha_P$ and $x_0\left(g_Q\right) = \alpha_Q$. By proposition 2.1.4 there is a group isomorphism

$$M \to \operatorname{Gal}(k(E)/[d]^* k(E)) : R \mapsto \tau_R^*,$$

where $\tau_R : E \to E$ is the translation by R-map; $\tau_R : E \to E : S \mapsto S \oplus R$. By the definition of the Weil-pairing $\mathrm{e}(R, P) = \frac{g_P(X \oplus S)}{g_P(X)} = \frac{\tau_S^*(X)}{g_P(X)}$, for any $R \in M$, $X \in E(\overline{k})$ any point so that $g_P(X)$ and $g_P(X \oplus S)$ are defined. The analogous result holds for g_Q as well. Finally,

we calculate

$$x_0 \circ \tau^*_{\left[\frac{\gamma(\alpha_Q)}{\alpha_Q}\right]_\rho P - \left[\frac{\gamma(\alpha_P)}{\alpha_P}\right]_\rho Q}(g_P) = x_0\left(\mathrm{e}\left(\left[\frac{\gamma(\alpha_Q)}{\alpha_Q}\right]_\rho P - \left[\frac{\gamma(\alpha_P)}{\alpha_P}\right]_\rho Q, P\right) g_P\right)$$
$$= x_0\left(\mathrm{e}\left(-\left[\frac{\gamma(\alpha_P)}{\alpha_P}\right]_\rho Q, P\right) g_P\right)$$
$$= x_0\left(\frac{\gamma(\alpha_P)}{\alpha_P} g_P\right)$$
$$= \frac{\gamma(\alpha_P)}{\alpha_P}\alpha_P = \gamma(\alpha_P)$$

and

$$x_0 \circ \tau^*_{\left[\frac{\gamma(\alpha_Q)}{\alpha_Q}\right]_\rho P - \left[\frac{\gamma(\alpha_P)}{\alpha_P}\right]_\rho Q}(g_Q) = x_0\left(\mathrm{e}\left(\left[\frac{\gamma(\alpha_Q)}{\alpha_Q}\right]_\rho P - \left[\frac{\gamma(\alpha_P)}{\alpha_P}\right]_\rho Q, Q\right) g_Q\right)$$
$$= x_0\left(\mathrm{e}\left(\left[\frac{\gamma(\alpha_Q)}{\alpha_Q}\right]_\rho P, Q\right) g_Q\right)$$
$$= x_0\left(\frac{\gamma(\alpha_Q)}{\alpha_Q} g_Q\right)$$
$$= \frac{\gamma(\alpha_Q)}{\alpha_Q}\alpha_Q = \gamma(\alpha_Q).$$

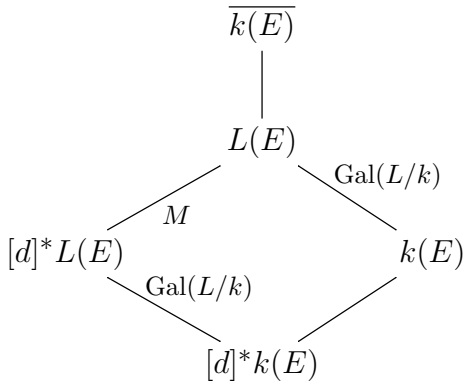
The statement follows since $k(E)/[d]^*k(E)$ is generated by g_P and g_Q. □

3.2 Over any field

Let k be any field. Consider the Galois representation

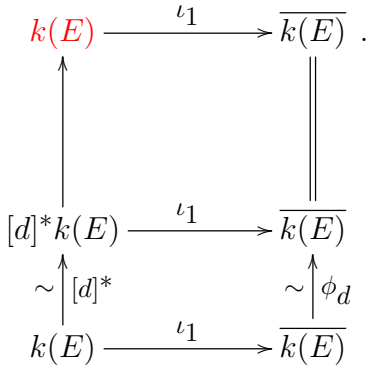
$$\Psi : G_k \to \mathrm{Aut}(M) = GL_2(\mathbb{F}_d)$$

given by the action on M and denote the fixed field of its kernel by L. Consider the tower of field extensions



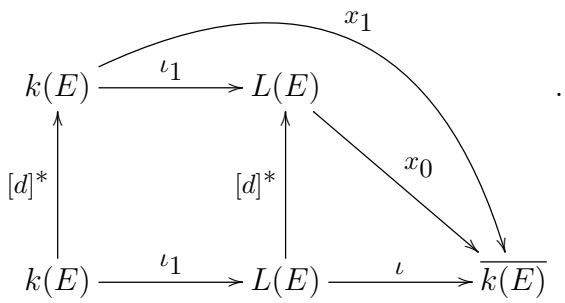
Fix a set $\tilde{G}_{L/k} \subset G_{k(E)}$ of coset representatives of $G_{k(E)}/G_{L(E)} \cong \mathrm{Gal}(L/k)$. Note that $\tilde{G}_{L/k}$ is also a set of coset representatives of $G_{[d]^*k(E)}/G_{[d]^*L(E)} \cong \mathrm{Gal}(L/k)$ and every $\tilde{\sigma} \in \tilde{G}_{L/k}$ fixes $k(E)$. Let $\gamma \in G_{[d]^*k(E)}$, then γ decomposes as $\gamma = \gamma'\tilde{\sigma}$ for some $\gamma' \in G_{[d]^*L(E)}$ and some $\tilde{\sigma} \in \tilde{G}_{L/k}$.

Let $\mathcal{T}$ be the torsor given by multiplication by d on E. Consider the pullback $\eta^*k(E)$ of $\mathcal{T}$ to the generic point. Note that fixing a $\overline{k(E)}$-point of $\eta^*\mathcal{T}$ is the same as fixing an isomorphism $\phi_0 : \overline{k(E)} \to \overline{k(E)}$ making the following diagram commute – or equivalently an element in $\mathrm{Gal}\,(k(E)/[d]^*k(E))$.



We will identify $G_{[d]^*k(E)}$ with $G_{k(E)}$ and $G_{[d]^*L(E)}$ with $G_{L(E)}$. Fix a set of coset representatives $\tilde{G}_{L/k}$ as before. Then every $\gamma \in G_{k(E)}$ can be decomposed as $\gamma'\tilde{\sigma}$ for some $\gamma' \in G_{L(E)}$ and some $\tilde{\sigma} \in \tilde{G}_{L/k}$. Furthermore, $\tilde{\sigma}$ fixes the image of $k(E)$ (top left corner of the diagram) by construction.

We want to describe the cocycle corresponding to the pullback of $\mathcal{T}$ along the generic point using the correspondence in section 2.2.4. Let x_1 be a $\overline{k(E)}$ point. We may assume, that $x_0 = \iota_1 \circ x_0$ for some x_0 as in the following commutative diagram.



Any $\gamma = \gamma'\tilde{\sigma} \in G_{k(E)}$ with $\gamma' \in G_{L(E)}, \tilde{\sigma} \in \tilde{G}_{L/k}$ acts on x_1 by

$$\gamma.x_1 = \gamma' \circ \tilde{\sigma}x_0 \circ \iota_1 = \gamma'.x_1.$$

Finally, $\gamma'.x_1$ can be computed as in proposition 3.1.1. Summarizing this we conclude the following proposition.

Proposition 3.2.1. *The pull-back of $\mathcal{T}$ to the generic point corresponds to the element in $H^1(k(E), M)$ given by the cocycle*

$$G_{k(E)} \to M : \gamma \mapsto \left[\frac{\gamma'(\alpha_Q)}{\alpha_Q}\right]_\rho P - \left[\frac{\gamma'(\alpha_P)}{\alpha_P}\right]_\rho Q,$$

where $\gamma = \gamma'\tilde{\sigma}$ *as above, for some* $\tilde{\sigma} \in \tilde{G}_{L/k}$ *and* $\gamma' \in G_{L(E)}$, $\alpha_P, \alpha_Q \in \overline{k(E)}$ *so that* $\alpha_P^d = t_P$ *and* $\alpha_Q^d = t_Q$.

We now proceed to give an explicit discription of the elements t_P and t_Q. Remark that these can be chosen in $k(E)^\times$ if M is k-rational. For more details on the construction, see also [Mil04, Section 4.1]. For any two points $R, S \in E(k)$, denote by $L_{R,S}$ the normalized function such that $L_{R,S} = 0$ gives the equation of the line through R and S. Its divisor is $\operatorname{div}(L_{R,S}) = (R)+(S)+(\ominus(R\oplus S))-3(0)$. Define an element $h_{R,S} = \frac{L_{R,S}}{L_{R\oplus S,-(R\oplus S)}} \in k(E)^\times$ with $\operatorname{div} h_{R,S} = (R) + (S) - (R \oplus S) - (0)$. Now the function $t_P = \prod_{i=1}^{d} h_{P,[i]P} \in k(E)$ has divisor

$$\begin{aligned}\operatorname{div}(t_P) &= \sum_{i=1}^{d-1}(P) + ([i]P) - ([i+1]P) - (0) \\ &= (d-1)(P) + P - ([d]P) - (d-1)(0) \\ &= d(P) - d(0).\end{aligned}$$

Similarly, we construct t_Q. Note that in the case $q = 3$, we can choose the normalized function $t_P, t_Q \in k(E)^\times$ such that $t_P = 0$ and $t_Q = 0$ give the tangent lines at P, and Q respectively.

3.3 General Argument that ϵ induces the correct split

In this section we review an abstract argument given in [Sko01, Chapter 4] to prove that the map ϵ defined before induces the desired split. We will reprove this in chapter 4 in our specific case using explit methods.

Let k be a field with algebraic closure $\overline{k}$ and let X be a k-variety. Denote the structure map by $p : X \to \operatorname{Spec} k$. Further, let $\overline{X} = X \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k}$. Assume that M is a G_k-module that is finitely generated as an abelian group. Assume that the order of the torsion of M is coprime to the characteristic of k. Denote by $S = \operatorname{Hom}(S, \mathbb{G}_m)$ the dual k-group of M. Let $\mathcal{T}$ be an X-torsor of $\mathsf{type}\,\lambda$ for some λ in $\operatorname{Hom}_k\left(M, \operatorname{Pic}(\overline{X})\right)$ (theorem 2.2.12) and assume that $\overline{k}[X]^\times = \overline{k}^\times$. Consider the long exact sequence from the spectral sequence of Ext's

$$\begin{aligned} 0 \longrightarrow \operatorname{Pic}(X) \longrightarrow \operatorname{Pic}(\overline{X})^{G_k} \longrightarrow \operatorname{Br}(k) \\ \longrightarrow \operatorname{Br}_1(X) \xrightarrow{r} H^1(k, \operatorname{Pic}(\overline{X})) \longrightarrow H^3(k, \mathbb{G}_m)\ , \end{aligned}$$

where $\operatorname{Br}_1(X)$ denotes the kernel of the natural map $\operatorname{Br}(X) \to \operatorname{Br}(\overline{X})^{G_k}$. Define

$$\operatorname{Br}_\lambda(X) := r^{-1}\lambda_*\left(H^1(k, M)\right) \subseteq \operatorname{Br}_1(X).$$

Theorem 3.3.1. *The cup-product $p^*(\alpha) \cup [\mathcal{T}]$ is an element of $\operatorname{Br}_\lambda(X)$ for any $\alpha \in H^1(k, M)$ and*

$$r\left(p^*(\alpha) \cup [\mathcal{T}]\right) = \lambda_*(\alpha) \in H^1\left(k, \operatorname{Pic}(\overline{X})\right).$$

That is, the following diagram commutes

$$\begin{array}{ccccccc} & & & & H^1(k, M) & & \\ & & & \overset{p^*(.)\cup[\mathcal{T}]}{\swarrow} & \downarrow{\scriptstyle \lambda_*} & & \\ \longrightarrow \operatorname{Br}(k) & \longrightarrow & \operatorname{Br}_1(X) & \xrightarrow{r} & H^1(k, \operatorname{Pic}(\overline{X})) & \longrightarrow & H^3(k, \mathbb{G}_m) \end{array} \quad . \tag{3.1}$$

Furthermore, any $A \in \operatorname{Br}_\lambda(X)$ can be written as

$$A = p^*(\alpha) \cup [\mathcal{T}] + p^*(A_0)$$

for some $\alpha \in H^1(k, M)$ *and some* $A_0 \in \mathrm{Br}(k)$.

This is [Sko01, Theorem 4.11]. We will review the proof here for completion. Note that it is enough to show that the following diagram commutes

$$\begin{array}{ccc} H^1(X,S) = \!= \mathrm{Ext}^1_X(p^*M, \mathbb{G}_m) & \xrightarrow{\mathsf{type}} & \mathrm{Hom}_k(M, \mathrm{Pic}(\overline{X})) \\ \downarrow d & & \downarrow d \\ \mathrm{Br}_1(X) & \xrightarrow{\quad r \quad} & H^1(k, \mathrm{Pic}(\overline{X})) \end{array} , \tag{3.2}$$

where d is the connecting homomorphism of the long exact sequence of Ext. The proof will require some facts on the derived category of X from [Wei94], that we will review first.

3.3.1 Digression to Derived Categories

Let X be a k-variety. Consider the categories $Sh(X)$ of étale sheaves on X, G_k-mod of G_k modules, and Ab of abelian groups. Denote by $\mathcal{D}^+(X), \mathcal{D}^+(k)$, and $\mathcal{D}^+(Ab)$ the corresponding derived categories of bounded below complexes. Note that all these categories have enough injectives. For M in one of these categories, let $M^\bullet$ be the element in the derived category with

$$M^i = \begin{cases} M & i = 0 \\ 0 & \text{else} \end{cases} .$$

For any $n \in \mathbb{Z}$, we denote by $\tau_{\leq n}$ and $\tau_{\geq n}$ the truncation functors. That is, for a complex F we define $\tau_{\geq n}(F)$ as the complex

$$\cdots \to 0 \to F^n/\mathrm{Im}(d) \to F^{n+1} \to \cdots$$

Furthermore, denote $\tau_{[m,n]}(F) = \tau_{\geq m}\tau_{\leq n}(F)$ and $\tau_{[n]}(F) = \tau_{[n,n]}(F)$.

Let $0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$ be an exact sequence of G_k-modules and let F be an object in $\mathcal{D}^+(k)$. Then the following diagram in $\mathcal{D}^+(Ab)$ commutes

$$\begin{array}{ccc} \mathbf{R}\operatorname{Hom}_k\left(A, \tau_{\leq 1}(F)\right) & \longrightarrow & \mathbf{R}\operatorname{Hom}_k\left(A, \tau_{[1]}(F)\right) \\ \Big\downarrow d & & \Big\downarrow d \\ \mathbf{R}\operatorname{Hom}_k\left(C, \tau_{\leq 1}(F)\right)[1] & \longrightarrow & \mathbf{R}\operatorname{Hom}_k\left(C, \tau_{[1]}(F)\right)[1] \end{array} , \tag{3.3}$$

where the vertical maps are the connecting homomorphisms induced by the exact sequence.

Consider the structure morphism $p : X \to \operatorname{Spec} k$. The direct image functor p_* assigns to an étale sheaf on X an étale sheaf on $\operatorname{Spec} k$. Fix the geometric point $\overline{s} : \operatorname{Spec} \overline{k} \to \operatorname{Spec} k$ induced by the inclusion $k \subseteq \overline{k}$. By [Sta19, Lemma 54.58.1, Tag 04JQ], the stalk functor $\mathcal{F} \mapsto \mathcal{F}_{\overline{s}}$ induces an equivalence of categories between the category of étale sheaves over X and the category of G_k-modules. Consider the composition of p_* with this equivalence of categories. Abusing notation, we will denote this composition by p_* as well. Furthermore, there is a functor $\operatorname{Hom}_k(M, \cdot) : G_k\text{-mod} \to Ab$. For $M = \mathbb{Z}$, this functor is given by sending a G_k-module N to its G_k-invariants N^{G_k}. Denote the associated derived functors by $\mathbf{R}\, p_*, \mathbf{R}\operatorname{Hom}_k(M, \cdot)$, and $\mathbf{H}(k, \cdot) = \mathbf{R}\operatorname{Hom}_k(\mathbb{Z}, \cdot)$. Recall, that under our equivalence of categories given by the stalk functor $\mathcal{F} \mapsto \mathcal{F}_{\overline{s}}$, the sheaf $\mathbf{R}^i\, p_*\mathbb{G}_m$ corresponds to the G_k-module

$$\widetilde{H^i(X, \mathbb{G}_m)}_{\overline{s}} = H^i(\overline{X}, \mathbb{G}_m), \tag{3.4}$$

by [Har77, III Proposition 8.5] and the second equality holds true, because taking stalks

commutes with cohomology.

The functor p_* admits a left-adjoint p^* so that $\mathrm{Hom}_k(M, p_*F) = \mathrm{Hom}_X(p^*M, F)$ for any G_k-module M and any étale sheaf F on X. We will use the following identities of adjoint functors throughout

$$\mathbf{R}\,\mathrm{Hom}_k(M, \cdot) \circ \mathbf{R}\,p_* = \mathbf{R}\,\mathrm{Hom}_X(p^*M, \cdot) \tag{3.5}$$

$$\mathbf{H}(k, \cdot) \circ \mathbf{R}\,p_* = \mathbf{H}(X, \cdot). \tag{3.6}$$

We now review the definition of the hypercohomology functor as given in [Mil80, Appendix C]. Let $f : \mathcal{A} \to \mathcal{B}$ be a left-exact functor between abelian categories and assume that $\mathcal{A}$ has enough injectives. Denote by $C^+(\mathcal{A})$ the category of complexes bounded below. Let $A^\bullet \in C^+(\mathcal{A})$. Then there exists a complex $I^\bullet \in C^+(\mathcal{A})$ whose objects are injectives, that is quasi-isomorphic to $\mathcal{A}$. The right-hyperderived functor $\mathbb{R}^i f$ of f assigns to $A^\bullet$ the object $H^i(fI^\bullet)$ in $\mathcal{B}$. Denote by $\mathbb{H}^i(k, \cdot)$ the hyperderived functor of $\mathbf{H}(k, \cdot)$.

For a G_k-module M that is finitely generated as an abelian group with torsion coprime to the characteristic of k, fix a sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow \mathbb{Z} \longrightarrow 0$$

of G_k-modules, where G_k acts trivially on $\mathbb{Z}$. The commutative diagram 3.3 gives the

following after setting $F = \mathbf{R}\, p_* \mathbb{G}_m$ and taking cohomology.

$$\begin{array}{ccc} \mathbb{R}^1 \operatorname{Hom}_k \left(M, \tau_{\leq 1} \left(\mathbf{R}\, p_* \mathbb{G}_m\right)\right) & \longrightarrow & \mathbb{R}^1 \operatorname{Hom}_k \left(M, \tau_{[1]} \left(\mathbf{R}\, p_* \mathbb{G}_m\right)\right). \\ \downarrow d & & \downarrow d \\ \mathbb{H}^1 \left(k, \tau_{\leq 1} \left(\mathbf{R}\, p_* \mathbb{G}_m\right)[1]\right) & \longrightarrow & \mathbb{H}^1 \left(k, \tau_{[1]} \left(\mathbf{R}\, p_* \mathbb{G}_m\right)[1]\right) \end{array} \tag{3.7}$$

It remains to show that the diagrams 3.2 and 3.7 are isomorphic, i.e. there exist isomorphisms between their objects so that the following diagram commutes.

$$\begin{array}{ccccc} \mathbb{R}^1 \operatorname{Hom}_k \left(M, \tau_{\leq 1} \left(\mathbf{R}\, p_* \mathbb{G}_m\right)\right) & & \longrightarrow & & \mathbb{R}^1 \operatorname{Hom}_k \left(M, \tau_{[1]} \left(\mathbf{R}\, p_* \mathbb{G}_m\right)\right) \\ \downarrow & \searrow^{\sim} & & & \downarrow \quad \searrow^{\sim} \\ & & \operatorname{Ext}^1_X (p^* M, \mathbb{G}_m) & \longrightarrow & \operatorname{Hom}_k (M, \operatorname{Pic}(\overline{X})) \\ & & \downarrow & & \downarrow \quad \downarrow d \\ \mathbb{H}^1 \left(k, \tau_{\leq 1} \left(\mathbf{R}\, p_* \mathbb{G}_m\right)[1]\right) & & \longrightarrow & & \mathbb{H}^1 \left(k, \tau_{[1]} \left(\mathbf{R}\, p_* \mathbb{G}_m\right)[1]\right) \\ & \searrow^{\sim} & & & \searrow^{\sim} \\ & & \operatorname{Br}_1(X) & \xrightarrow{\quad r \quad} & H^1(k, \operatorname{Pic}(\overline{X})) \end{array} \tag{3.8}$$

For the proofs we refer the reader to [Mil80, Appendix C], [Sko01, p. 67 ff.], or [Wei94, Corollary 10.8.3].

3.3.2 Application to our case

Let E be an elliptic curve over a field k of characteristic prime to d. Denote by M the d-torsion of $E(\overline{k})$. Consider the torsor $\mathcal{T}$ given by multiplication by d as in example 2.2.14. It's type is the composition

$$\lambda : M \to E(\overline{k}) = \operatorname{Pic}^0(\overline{E}) \to \operatorname{Pic}(\overline{E}).$$

Furthermore, recall that $\mathrm{Pic}(\overline{E}) = \mathrm{Pic}^0\left(\overline{E}\right) \oplus \mathbb{Z}$ and $H^1(k, \mathbb{Z}) = 0$. Then the first cohomology becomes

$$H^1\left(k, \mathrm{Pic}(\overline{E})\right) = H^1\left(k, \mathrm{Pic}^0(\overline{E})\right) = H^1(k, E(\overline{k})).$$

The diagram 3.1 becomes

$$\begin{array}{ccccccccc} & & & & & & H^1(k,M) & & \\ & & & & & \overset{\epsilon}{\swarrow} & \downarrow{\scriptstyle \lambda} & & \\ 0 & \longrightarrow & \mathrm{Br}(k) & \longrightarrow & \mathrm{Br}(E) & \xrightarrow{r} & H^1(k, E(\overline{k})) & \longrightarrow & 0 \end{array} .$$

Note that both λ and r are surjective and therefore by definition

$$\mathrm{Br}_\lambda(E) = {}_d\mathrm{Br}(E).$$

By theorem 3.3.1, every element in ${}_d\mathrm{Br}(E)$ can be represented as a cup product

$$p^*(\alpha) \cup [\mathcal{T}] + p^*(A_0)$$

for some $\alpha \in H^1(k, M)$ and $A_0 \in \mathrm{Br}(k)$. Furthermore, the algebra $p^*(\alpha) \cup [\mathcal{T}]$ is trivial if and only if α is in the image of the Kummer map $\delta : E(\overline{k})/[d]E(\overline{k}) \to H^1(k, M)$.

Chapter 4

Generators of $\mathrm{Br}(E)$

Let k be a field of characteristic different from 2 or 3. Let $d \geq 2$ be an integer coprime to the characteristic of k and assume additionally that k contains a primitive d-th root of unity ρ. Let E be an elliptic curve over k. Recall that our method of computing generators of ${}_d\mathrm{Br}(E)$ is via an explicit split to the exact sequence

$$0 \longrightarrow {}_d\mathrm{Br}(k) \xrightarrow{i} {}_d\mathrm{Br}(E) \xrightarrow{r} {}_dH^1\left(k, E\left(\overline{k}\right)\right) \longrightarrow 0$$

described in section 2.3. Consider the Kummer sequence

$$0 \longrightarrow M \longrightarrow E(\overline{k}) \xrightarrow{[d]} E(\overline{k}) \longrightarrow 0\,.$$

The sequence induced on cohomology is

$$0 \longrightarrow E(k)/[d]E(k) \xrightarrow{\delta} H^1(k, M) \xrightarrow{\lambda} {}_dH^1\left(k, E(\overline{k})\right) \longrightarrow 0\,.$$

We will describe a map $\epsilon : H^1(k, M) \to {}_d\mathrm{Br}(E)$, that induces a split of the sequence in section 2.3. Denote by $\mathcal{T}$ the torsor given by multiplication by d on E as in chapter 3.

Define $\epsilon : H^1(k, M) \to {}_d\mathrm{Br}(E)$ as the following composition

$$\begin{aligned} \epsilon : \quad & H^1(k, M) \xrightarrow{\sim} H^1_{\text{ét}}(\mathrm{Spec}(k), M) \xrightarrow{p^*} H^1_{\text{ét}}(E, M) \\ & \xrightarrow{-\cup[\mathcal{T}]} H^2_{\text{ét}}(E, M \otimes M) \xrightarrow{\mathrm{e}} H^2_{\text{ét}}(E, \mu_d) \longrightarrow {}_d\mathrm{Br}(E) \, . \end{aligned} \tag{4.1}$$

In [Sko01, Theorem 4.1.1], the author proves abstractly that ϵ induces such a split using general properties of torsors and the cup-product. In this chapter, we will determine ϵ explicitly and prove directly that the map induces the desired split.

Proposition 4.0.1. *On the level of cocycles ϵ coincides with the map that assigns to a 1-cocycle $f : G_k \to M$ the 2-cocycle*

$$\begin{aligned} \epsilon(f) : G_{k(E)} \times G_{k(E)} &\to \overline{k(E)}^\times \\ (\gamma, \tau) &\mapsto \mathrm{e}\left(f(\gamma), \gamma \left(\left[\frac{\tau'(\alpha_Q)}{\alpha_Q} \right]_\rho P - \left[\frac{\tau'(\alpha_P)}{\alpha_P} \right]_\rho Q \right) \right), \end{aligned} \tag{4.2}$$

for $\gamma, \tau \in G_{k(E)}, \tau = \tau'\tilde{\sigma}$ for some $\tilde{\sigma} \in \tilde{G}_{L/k}$ and $\tau' \in G_{\overline{k}(E)}$. (For a description of $\tilde{G}_{L/k}$ see section 3.2).

Proof. Consider the following diagram

$$\begin{array}{ccccccc} H^1(k, M) & \xrightarrow{p^*} & H^1_{\text{ét}}(E, M) & \xrightarrow{-\cup[\mathcal{T}]} & H^2_{\text{ét}}(E, M \otimes M) & \xrightarrow[\sim]{\mathrm{e}} & H^2_{\text{ét}}(E, \mu_d) \\ & & \downarrow \eta^* & & \downarrow \eta^* & & \downarrow \\ & & H^1_{\text{ét}}(k(E), M) & \xrightarrow{-\cup[\eta^*\mathcal{T}]} & H^2_{\text{ét}}(k(E), M \otimes M) & \xrightarrow[\sim]{\mathrm{e}} & {}_d\mathrm{Br}\, k(E) \end{array}$$

It has commutative squares as the cup-product commutes with η^* [Bre97, Chapter 2, 8.2]. For every cocycle $f : G_k \to M$, the Brauer class $\mathrm{e} \circ (\eta^* p^*([f]) \cup [\eta^* \mathcal{T}])$ can be described by the cocycle in eq. (4.2) by proposition 3.2.1 and by the definition of the cup-product in

group cohomology (see definition 2.2.9). Recall that by [CTS07, Theorem 5.11] the map on the right is given by the injection that identifies $\mathrm{Br}(E)$ with the unramified Brauer group of $k(E)$ (for the unramified Brauer group see also section 2.2.6). □

4.1 M is k-rational

Assume throughout this section that $M \subset E(k)$ with generators P and Q so that $\mathrm{e}(P,Q) = \rho$. We are now ready to calculate a set of generators of ${}_d\mathrm{Br}(E)$. By Kummer-theory there is an isomorphism

$$\begin{aligned} \phi : \left(k^\times/(k^\times)^d\right) \times \left(k^\times/(k^\times)^d\right) &\to H^1(k, M) \\ (a,b) &\mapsto c_{a,b}, \end{aligned} \tag{4.3}$$

where $c_{a,b}$ can be represented by the cocycle

$$\begin{aligned} G_k &\to M \\ \gamma &\mapsto \left[\frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}\right]_\rho P \oplus \left[\frac{\gamma\left(\sqrt[d]{b}\right)}{\sqrt[d]{b}}\right]_\rho Q. \end{aligned}$$

Proposition 4.1.1. *The composition $\epsilon \circ \phi(a,b)$ corresponds to the Brauer class of the tensor product of symbol algebras*

$$(a, t_P)_{d,k(E)} \otimes \left(b, t_Q\right)_{d,k(E)}$$

for any $(a,b) \in k^\times/(k^\times)^d \times k^\times/(k^\times)^d$.

Proof. Observe that the class of $\epsilon_k \circ \phi(a,b)$ can be represented by the cocycle that takes the

pair $(\gamma, \tau) \in G_{k(E)} \times G_{k(E)}$ to

$$\begin{aligned} &\mathrm{e}\left(\left[\frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}\right]_\rho P \oplus \left[\frac{\gamma\left(\sqrt[d]{b}\right)}{\sqrt[d]{b}}\right]_\rho Q, \left[\frac{\tau(\alpha_Q)}{\alpha_Q}\right]_\rho P - \left[\frac{\tau(\alpha_P)}{\alpha_P}\right]_\rho Q\right) \\ =&\,\mathrm{e}\left(\left[\frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}\right]_\rho P, \left[\frac{\tau(\alpha_P)}{\alpha_P}\right]_\rho Q\right)^{-1} \mathrm{e}\left(\left[\frac{\gamma\left(\sqrt[d]{b}\right)}{\sqrt[d]{b}}\right]_\rho Q, \left[\frac{\tau(\alpha_Q)}{\alpha_Q}\right]_\rho P\right). \end{aligned}$$

The statement follows from proposition 2.2.18. □

Recall that we need to prove that ϵ induces a split to the sequence in section 2.3 on the right, i.e. we need to show that $r \circ \epsilon = \lambda$ and $\epsilon(\ker(\lambda)) = 0$. For the definitions of r and λ see section 2.3. We first prove that $r \circ \epsilon = \lambda$.

Proposition 4.1.2. *$r \circ \epsilon = \lambda$.*

Proof. We will only prove that $r \circ \epsilon \circ \phi(a, 1) = \lambda \circ \phi(a, 1)$. The other cases are similar. We showed previously that $\epsilon \circ \phi(a, 1) = (a, t_P)_{d,k(E)}$, which corresponds to the cocycle

$$(\gamma, \tau) \mapsto \begin{cases} 1 & \left[\frac{\gamma(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} + \left[\frac{\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} < d \\ t_P & \text{else} \end{cases} \qquad (*)$$

in $H^2(G_k, \overline{k}(E)^\times)$. This gives an element in $H^2(G_k, \mathrm{Prin}(E))$ via

$$(\gamma, \tau) \mapsto \begin{cases} 1 & \left[\frac{\gamma(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} + \left[\frac{\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} < d \\ d(P) - d(0) & \text{else} \end{cases}.$$

On the other hand for any $\gamma \in G_k$,

$$\lambda(\phi(a,1))(\gamma) = \phi(a,1)(\gamma) = \left[\frac{\gamma(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} P.$$

Now we follow the proof of the snake lemma to calculate the image of $\lambda(f)$ under the connecting homomorphism

$$H^1(k, E(\overline{k})) \to H^2(k, \mathrm{Prin}(E))$$

induced by the sequence

$$0 \to \overline{k}(E)^\times \to \mathrm{Prin}(\overline{E}) \to \mathrm{Div}(\overline{E}) \to 0.$$

First lift it to

$$\gamma \mapsto \left[\frac{\gamma(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} ((P) - (0)) \in \mathrm{Div}^0(\overline{E}).$$

Now use the boundary map to get

$$\begin{aligned}
(\gamma,\tau) \mapsto \gamma &\left(\left[\frac{\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} ((P) - (0))\right) - \left[\frac{\gamma\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} ((P) - (0)) + \left[\frac{\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} ((P) - (0)) \\
&= \left[\frac{\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} ((P) - (0)) - \left[\frac{\gamma\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} ((P) - (0)) + \left[\frac{\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} ((P) - (0)) \\
&= \begin{cases} d(P) - d(0) & \text{if } \left[\frac{\gamma(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} + \left[\frac{\tau(\sqrt[d]{a})}{\sqrt[d]{a}}\right]_\rho^{\mathbb{Z}} \geq d \\ 1 & \text{else} \end{cases},
\end{aligned}$$

which coincides with what we calculated in $(*)$. The statement follows. □

Proposition 4.1.3. $\epsilon\left(\ker(\lambda)\right) = 0$.

Proof. Recall that $\ker(\lambda) = \mathrm{Im}(\delta)$ and let $R \in E(k)$. By the previous proposition $r \circ \epsilon \circ \delta(R) = \lambda \circ \delta(R)$ is trivial. Thus the algebra $\epsilon \circ \delta(R)$ is in the image of the $\mathrm{Br}(k) \to \mathrm{Br}(E)$. It remains to show that the specialization of $\epsilon \circ \delta(R)$ at 0 is trivial. The cup-product commutes with specialization at a closed point [Bre97, Chapter 2, 8.2], i.e. $\left([\mathcal{T}'] \cup [\mathcal{T}]\right)_S = \left([\mathcal{T}']\right)_S \cup ([\mathcal{T}])_S$ for every $S \in E(k)$ and every $[\mathcal{T}'] \in H^1_{\text{ét}}(E, M)$. By definition of ϵ,

$$(\epsilon \circ \delta(R))_S = \delta(R) \cup \mathcal{T}_S \in \mathrm{Br}(k)$$

for any $S \in E(k)$. In particular, $(\epsilon \circ \delta(R))_0 = \delta(R) \cup \mathcal{T}_0$. The specialization of $\mathcal{T}$ at 0 admits a point (the point 0) and is therefore the trivial torsor. We deduce that $(\epsilon \circ \delta(R))_0$ is trivial and thus so is $\epsilon \circ \delta(R)$. □

Theorem 4.1.4. *Suppose that the d-torsion M of E is k-rational. Fix two generators P and Q of M. Let $t_P, t_Q \in k(E)$ with divisors $\mathrm{div}(t_P) = d(Q) - (0)$ and $\mathrm{div}(t_Q) = d(Q) - q(0)$. Then the d-torsion of $\mathrm{Br}(E)$ decomposes as*

$${}_d\mathrm{Br}(E) = {}_d\mathrm{Br}(k) \oplus I$$

and every element in I can be represented as a tensor product

$$(a, t_P)_{d,k(E)} \otimes \left(b, t_Q\right)_{d,k(E)}$$

with $a, b \in k^\times$.

This result was previously known and was proved using different methods for instance in

[CRR16, Remark 6.3].

Proof. Proposition 4.1.2 and proposition 4.1.3 imply that ϵ induces the desired split. Therefore ${}_d\mathrm{Br}(E) = {}_d\mathrm{Br}(k) \oplus \mathrm{Im}(\epsilon)$. The theorem follows from proposition 4.1.1. □

4.2 $[L : k]$ is coprime to q

From now on let $q = d$ be an odd prime and drop the assumption that M is k-rational. Consider the natural Galois representation

$$\Psi : G_k \to \mathrm{Aut}(M) = GL_2(\mathbb{F}_q).$$

Denote by L the fixed field of the kernel of Ψ. The degree of the Galois extension L over k divides the order of $GL_2(\mathbb{F}_q)$, which is $(q+1)q(q-1)^2$.

Let $\mathcal{T}$ be the torsor given by multiplication by d on E. Denote the generic points of E and $E \times \mathrm{Spec}\, L$ by $\eta : \mathrm{Spec}\, k(E) \to E$ and $\eta_L : \mathrm{Spec}\, L(E) \to E \times \mathrm{Spec}_L$, respectively. Consider the pull-back $\eta_L^*(\mathcal{T})$ of $\mathcal{T}$ to $L(E)$ and the pull-back $\eta_k^*(\mathcal{T})$ of $\mathcal{T}$ to $k(E)$. By proposition 3.1.1 and proposition 3.2.1 we see immediately that $\mathrm{res}\left(\eta_k^*(\mathcal{T})\right) = \eta_L^*(\mathcal{T})$. By [NSW08, Ch. 1, Proposition 1.5.3 (iii) and (iv)] and the construction of ϵ, the following diagram commutes

$$\begin{array}{ccccc} H^1(k,M) & \xrightarrow{\mathrm{res}} & H^1(L,M) & \xrightarrow{\mathrm{cor}} & H^1(k,M)\,. \\ \downarrow{\scriptstyle \epsilon_k} & & \downarrow{\scriptstyle \epsilon_L} & & \downarrow{\scriptstyle \epsilon_k} \\ {}_q\mathrm{Br}(E) & \xrightarrow{\mathrm{res}} & {}_q\mathrm{Br}(E \otimes L) & \xrightarrow{\mathrm{cor}} & {}_q\mathrm{Br}(E) \end{array}$$

Throughout this section, we assume that q does not divide the order $[L : k]$. The

corestriction map

$$\mathrm{cor} : {}_q\mathrm{Br}(E \otimes L) \to {}_q\mathrm{Br}(E)$$

is surjective and every element in I can be written as $\mathrm{cor}(A)$ with $A \in {}_q\mathrm{Br}(E)$. We summarize this observation in the following theorem.

Theorem 4.2.1. *Let $t_P, t_Q \in L(E)$ with divisors $\mathrm{div}(t_P) = q(Q) - q(0)$ and $\mathrm{div}(t_Q) = q(Q) - q(0)$. Then the q-torsion of $\mathrm{Br}(E)$ decomposes as*

$$ {}_q\mathrm{Br}(E) = {}_q\mathrm{Br}(k) \oplus I$$

and every element in I can be represented as a tensor product

$$\mathrm{cor}\,(a, t_P)_{q,L(E)} \otimes \mathrm{cor}\left(b, t_Q\right)_{q,L(E)}$$

with $a, b \in L^\times$.

Remark 4.2.2. *Note that corestriction is in general not injective. To get a smaller set of generators, observe that by [NSW08, Ch, 1, Corollary 1.5.7] the image of the restriction map $H^1(k, M) \to H^1(L, M)$ coincides with the image of the Norm map*

$$N_{L/k} : H^1(L, M) \to H^1(L, M).$$

Now by Kummer theory $H^1(L, M) \cong L^\times/(L^\times)^q \times L^\times/(L^\times)^q$ via the isomorphism ϕ. Let $g \in G_k$ and $(a, b) \in L^\times/(L^\times)^q \times L^\times/(L^\times)^q$. Suppose that $g^{-1}(P) = c_1P \oplus c_2Q$ and

$g^{-1}(Q) = c_3P \oplus c_4Q$. *The action of* g *compatible with* ϕ *is*

$$\begin{aligned} g.(a,b) =& \phi^{-1} g.\phi(a,b) \\ =& \phi^{-1}\left(g.\left(\gamma \mapsto \left[\frac{\gamma\left(\sqrt[q]{a}\right)}{\sqrt[q]{a}}\right]_\rho P \oplus \left[\frac{\gamma\left(\sqrt[q]{b}\right)}{\sqrt[q]{b}}\right]_\rho Q\right)\right) \\ =& \left(\left(g^{-1}(a)\right)^{c_1}\left(g^{-1}(b)\right)^{c_3}, \left(g^{-1}(a)\right)^{c_2}\left(g^{-1}(b)\right)^{c_4}\right). \end{aligned}$$

Now the image of the restriction followed by ϕ *coincides with the image of the norm on* $L^\times/(L^\times)^q \times L^\times/(L^\times)^q$ *under the above action.*

4.3 $[L:k]$ equals q

In this section, we assume that L is of degree q over k. After renaming P and Q we may assume without loss of generality that there is some $\sigma \in G_k$ such that $\sigma(Q) = P \oplus Q$ and $\overline{\sigma}$ generates G_k/G_L. Fix a coset representative $\tilde{\sigma}$ of σ in $G_{k(E)}$ (compare section 3.2). To avoid confusion, we will add subscripts to the maps ϵ, δ, r, and λ to denote their field of definition. Additionally denote a primitive element for the extension L/k by l.

Consider the diagram

$$\begin{array}{ccccc} 0 \longrightarrow H^1\left(G_k/G_L, M\right) & \xrightarrow{\inf} & H^1(G_k, M) & \xrightarrow{\text{res}} & H^1(G_L, M)^{G_k/G_L}, \\ & & \downarrow \epsilon_k & & \downarrow \epsilon_L \\ & & {}_q\mathrm{Br}(E) & \xrightarrow{\text{res}} & {}_q\mathrm{Br}(E \times_k \operatorname{Spec} L) \end{array}$$

where the first row is the inflation restriction exact sequence. The diagram commutes by

construction of ϵ and since the restriction map and the cup-product commute [NSW08, Ch. 1 Proposition 1.5.3 (iii)]. We will first describe the image of the inflation map, and then explore the restriction afterwards. We will apply the following technical lemma throughout.

Lemma 4.3.1. $\sum_{i=0}^{q-1} \sigma^i(R) = 0$ *for every* $R \in M$.

Proof. Let $R = mP \oplus nQ \in M$. We calculate directly that

$$\sum_{i=0}^{q-1} \sigma^i(mP \oplus nQ) = \sum_{i=0}^{q-1} (mP \oplus inP \oplus nQ) = mqP \oplus \frac{q(q-1)}{2} nP \oplus nqQ = 0.$$

□

4.3.1 The Image of the Inflation Map

Lemma 4.3.2. *The group* $H^1(G_k/G_L, M)$ *is cyclic of rank* q *with generator* f_L *defined by* $f_L(\overline{\sigma}) = Q$.

Proof. Lemma 4.3.1 implies that $f_L(\overline{\sigma}^q) = \sum_{i=0}^{q-1} \sigma^i f_L(\overline{\sigma}) = 0$ and thus f_L defines a cocycle. Since G_k/G_L is cyclic with generator $\overline{\sigma}$, every element f in $H^1(G_k, G_L, M)$ is determined by $f(\overline{\sigma})$. Furthermore, if $f(\overline{\sigma}) = mP \oplus nQ$, then

$$f(\overline{\sigma}) - \overline{\sigma}(mP) = mP \oplus nQ \ominus mP = nQ = f_L^b(\overline{\sigma}).$$

The statement follows. □

Let $\alpha_Q \in \overline{k(E)}$ with $\alpha_Q^q = t_Q$. Consider $n_Q = \prod_{i=0}^{q-1} \tilde{\sigma}^i \left(\alpha_Q\right)$. Note that n_Q is defined to be the element in $k(E)$ with $n_Q^q = N_{L(E)/k(E)}(t_Q)$. Furthermore, note that $\operatorname{div} n_Q = \sum_{i=0}^{q-1} \left(\sigma^i(Q) - (0)\right)$.

Proposition 4.3.3. *$\epsilon_k(\inf(f_L))$ is the inverse of the Brauer class of the symbol algebra $\left(l^q, n_Q\right)_{q,k(E)}$, where $\alpha_Q \in \overline{k(E)}$ with $\alpha_Q^q = t_Q$.*

Proof. We first show that $\prod_{i=0}^{q-1} \tilde{\sigma}^i\left(\alpha_Q\right) \in k(E)$. Let $\gamma \in G_{L(E)}$. By our previous calculations and with x_0 and g_Q as in the proof of proposition 3.2.1, we deduce that there is some $R \in M$ such that $\gamma(\alpha_Q) = R.x_0(g_Q)$. Then

$$\gamma\left(\prod_{i=0}^{q-1} \tilde{\sigma}^i\left(\alpha_Q\right)\right) = \left(\sum_{i=0}^{p-1} \sigma^i(R)\right).x_0(g_Q) = \alpha_Q \tag{4.4}$$

by lemma 4.3.1. Now $\prod_{i=0}^{q-1} \tilde{\sigma}^i\left(\alpha_Q\right)$ is obviously fixed by $\tilde{\sigma}$ and therefore $\prod_{i=0}^{q-1} \tilde{\sigma}^i\left(\alpha_Q\right) \in k(E)$. Let $\gamma, \tau \in G_{k(E)}$ and denote $\gamma = \gamma'\tilde{\sigma}^i, \tau = \tau'\tilde{\sigma}^j$ with $\gamma', \tau' \in G_{L(E)}$. Then by definition of ϵ we see that

$$\begin{aligned}
\epsilon_k(\inf(f_L))(\gamma,\tau) &= \mathrm{e}\left(\frac{(i-1)i}{2}P \oplus iQ, \sigma^i\left(\left[\frac{\tau'\left(\alpha_Q\right)}{\alpha_Q}\right]_\rho P - \left[\frac{\tau'\left(\alpha_P\right)}{\alpha_P}\right]_\rho Q\right)\right) \\
&= \mathrm{e}\left(\frac{(i-1)i}{2}P \oplus iQ, \left[\frac{\tau'\left(\alpha_Q\right)}{\alpha_Q}\left(\frac{\tau'\left(\alpha_P\right)}{\alpha_P}\right)^{-i}\right]_\rho P - \left[\frac{\tau'\left(\alpha_P\right)}{\alpha_P}\right]_\rho Q\right) \\
&= \mathrm{e}\left(\frac{(i-1)i}{2}P, -\left[\frac{\tau'\left(\alpha_P\right)}{\alpha_P}\right]_\rho Q\right)\mathrm{e}\left(iQ, \left[\frac{\tau'\left(\alpha_Q\right)}{\alpha_Q}\left(\frac{\tau'\left(\alpha_P\right)}{\alpha_P}\right)^{-i}\right]_\rho P\right) \\
&= \left(\frac{\tau'\left(\alpha_P\right)}{\alpha_P}\right)^{-\frac{(i-1)i}{2}}\left(\frac{\tau'(\alpha_Q)}{\alpha_Q}\right)^{-i}\left(\frac{\tau'\left(\alpha_P\right)}{\alpha_P}\right)^{i^2} \\
&= \left(\frac{\tau'\left(\alpha_P\right)}{\alpha_P}\right)^{\frac{(i+1)i}{2}}\left(\frac{\tau'(\alpha_Q)}{\alpha_Q}\right)^{-i}
\end{aligned}$$

Now consider the map

$$\begin{aligned} g : G_{k(E)} &\to \overline{k(E)}^{\times} \\ \gamma &\mapsto \gamma' \left(\prod_{n=0}^{i-1} \tilde{\sigma}^n(\alpha_Q) \right), \end{aligned} \tag{4.5}$$

where $\gamma = \gamma' \tilde{\sigma}^i$ for some $\gamma' \in G_{L(E)}$. The differential of g can be calculated as follows: If $i + j < q$, then

$$\begin{aligned} dg(\gamma, \tau) &= \frac{\gamma' \left(\prod_{n=0}^{i-1} \tilde{\sigma}^n(\alpha_Q) \right) \gamma \left(\tau' \left(\prod_{n=0}^{j-1} \tilde{\sigma}^n(\alpha_Q) \right) \right)}{(\gamma\tau)' \left(\prod_{n=0}^{i+j-1} \tilde{\sigma}^n(\alpha_Q) \right)} \\ &= \frac{\gamma' \left(\prod_{n=0}^{i-1} \tilde{\sigma}^n(\alpha_Q) \right) \left(\gamma' \tilde{\sigma}^i \tau' \right) \left(\prod_{n=0}^{j-1} \tilde{\sigma}^n(\alpha_Q) \right)}{\left(\gamma' \tilde{\sigma}^i \tau' \tilde{\sigma}^{-i} \right) \left(\prod_{n=0}^{i+j-1} \tilde{\sigma}^n(\alpha_Q) \right)} \\ &= \frac{\gamma' \left(\prod_{n=0}^{i-1} \tilde{\sigma}^n(\alpha_Q) \right)}{\left(\gamma' \tilde{\sigma}^i \tau' \tilde{\sigma}^{-i} \right) \left(\prod_{n=0}^{i-1} \tilde{\sigma}^n(\alpha_Q) \right)} \\ &= \frac{\prod_{n=0}^{i-1} \tilde{\sigma}^n(\alpha_Q)}{\left(\tilde{\sigma}^i \tau' \tilde{\sigma}^{-i} \right) \left(\prod_{n=0}^{i-1} \tilde{\sigma}^n(\alpha_Q) \right)} \\ &= \prod_{n=0}^{i-1} \frac{\tilde{\sigma}^n(\alpha_Q)}{\left(\tilde{\sigma}^i \tau' \tilde{\sigma}^{-i+n} \right)(\alpha_Q)} \\ &= \prod_{n=0}^{i-1} \frac{\tilde{\sigma}^{-i+n}(\alpha_Q)}{\left(\tilde{\sigma}^i \tau' \tilde{\sigma}^{-i+n} \right) \alpha_Q)} \\ &= \prod_{n=0}^{i-1} \left(\frac{\alpha_P}{\tau'(\alpha_P)} \right)^{-i+n} \frac{\alpha_Q}{\tau'(\alpha_Q)} \\ &= \left(\frac{\alpha_P}{\tau'(\alpha_P)} \right)^{-i^2 + \frac{(i-1)i}{2}} \left(\frac{\alpha_Q}{\tau'(\alpha_Q)} \right)^i \\ &= \left(\frac{\alpha_P}{\tau'(\alpha_P)} \right)^{-\frac{(i+1)i}{2}} \left(\frac{\alpha_Q}{\tau'(\alpha_Q)} \right)^i \end{aligned}$$

A similar calculation shows that if $i + j \geq q$, then

$$dg(\gamma, \tau) = \left(\prod_{n=0}^{q-1} \tilde{\sigma}^n(\alpha_Q) \right) \left(\frac{\alpha_P}{\tau'(\alpha_P)} \right)^{-\frac{(i+1)i}{2}} \left(\frac{\alpha_Q}{\tau'(\alpha_Q)} \right)^i$$

The statement follows by subtracting this trivial cocycle and applying proposition 2.2.18. □

Proposition 4.3.4. $r \circ \epsilon \circ \inf(f_L) = \lambda \circ \inf(f_L)$.

Proof. By the previous lemma, we get from $\epsilon(\inf(f_L))$ the element

$$(\gamma'\sigma^i, \tau'\sigma^j) \mapsto \begin{cases} 1 & i + j < q \\ \sum_{i=0}^{q-1} (\sigma(Q) - (0)) & i + j \geq q \end{cases}$$

in $H^2(G_k, \mathrm{Prin}(E))$, where $\gamma', \tau' \in G_k$. On the other hand, $r(\inf(f_L))$ can be presented by the cocycle

$$\gamma'\sigma^i \mapsto \sum_{m=0}^{i} \sigma^m(Q) - 0.$$

This lifts to the map

$$\gamma'\sigma^i \mapsto \sum_{m=0}^{i} (\sigma^m(Q)) - (0) \in \mathrm{Div}^0(\overline{E}),$$

and a direct computation of the boundary map gives

$$(\gamma'\sigma^i, \tau'\sigma^j) \mapsto \begin{cases} \sigma^i \left(\sum_{m=0}^{j} (\sigma^m(Q)) - (0)\right) - \left(\sum_{m=0}^{i+j} (\sigma^m(Q)) - (0)\right) & \\ + \left(\sum_{m=0}^{i} (\sigma^m(Q)) - (0)\right) & i+j < q \\ \sigma^i \left(\sum_{m=0}^{j} (\sigma^m(Q)) - (0)\right) - \left(\sum_{m=0}^{i+j-q} (\sigma^m(Q)) - (0)\right) & \\ + \left(\sum_{m=0}^{i} (\sigma^m(Q)) - (0)\right) & i+j \geq q \end{cases}$$

$$= \begin{cases} 1 & i+j < q \\ \left(\sum_{m=0}^{q-1} (\sigma^m(Q)) - (0)\right) & i+j \geq q \end{cases},$$

which coincides with the previous calculation. □

Corollary 4.3.5. *ϵ induces a split to the sequence*

$$0 \longrightarrow {}_q\mathrm{Br}(k) \xrightarrow{i} {}_q\mathrm{Br}(E) \xrightarrow{r} {}_qH^1\left(k, E\left(\overline{k}\right)\right) \longrightarrow 0\,.$$

Proof. We deduce from the previous proposition and proposition 4.1.2 that $r \circ \epsilon = \lambda$. Furthermore, $\epsilon(\ker(\lambda)) = 0$ follows as in the proof of proposition 4.1.3. □

4.3.2 The Image of the Restriction Map

We now calculate the image of the composition $\phi^{-1} \circ \mathrm{res}$ with ϕ as in eq. (4.3). By [Ser79, Chapter VII, Section 5] the action of G_k on $L^\times/(L^\times)^q \times L^\times/(L^\times)^q$ compatible with ϕ is given by

$$\sigma.(a,b) = \phi^{-1}\left(\sigma.\phi(a,b)\right) = \left(\frac{\sigma^{-1}(a)}{\sigma^{-1}(b)}, \sigma^{-1}(b)\right).$$

Lemma 4.3.6. *Under the isomorphism ϕ^{-1}, the fixed set $H^1(L,M)^{G_k/G_L}$ corresponds to*

$$\left\{\left(a, \frac{a}{\sigma(a)}\right) : \sigma(a)^2 \equiv \sigma^2(a)a \mod (L^\times)^q\right\}.$$

Proof. Let $(a,b) \in L^\times/(L^\times)^q \times L^\times/(L^\times)^q$ be fixed by the above action. Then $a \equiv \frac{\sigma^{-1}(a)}{\sigma^{-1}(b)}$, which implies that $b \equiv \frac{a}{\sigma(a)}$. Now $b \equiv \sigma^{-1}(b)$ and thus $\frac{a}{\sigma(a)} \equiv \frac{\sigma^{-1}(a)}{a}$ which implies that $a^2 \equiv \sigma(a)\sigma^{-1}(a)$ or equivalently $\sigma(a)^2 \equiv \sigma^2(a)a$. □

Lemma 4.3.7. *$f \in H^1(L,M)^{G_k/G_L}$ is in the image of the restriction map if and only if $f(\gamma^q) = 0$ for any $\gamma \in G_k$.*

Proof. Let $\gamma \in G_k$ and suppose that f is in the image of the restriction map with preimage g. Then we can write $\gamma = \gamma'\sigma^i$ for some $\gamma' \in G_L$. We calculate directly using lemma 4.3.1 that

$$f(\gamma^q) = g(\gamma^q) = \sum_{i=0}^{q-1} \gamma^q g(\gamma) = \sum_{i=0}^{q-1} \sigma^{iq} g(\gamma) = \sum_{i=0}^{q-1} \sigma^i g(\gamma) = 0.$$

For the converse, assume that f satisfies the condition that $f(\gamma^q) = 0$ for any $\gamma \in G_k$. In particular $f(\sigma^q) = 0$. Define $g \in H^1(k,M)$ by setting $g(\gamma) = f(\gamma')$, where $\gamma = \gamma'\sigma^i$ for $\gamma' \in G_L$. This is well-defined as for any $\gamma, \tau \in G_k$ with $\gamma = \gamma'\sigma^i, \tau = \tau'\sigma^j$ and $\gamma', \tau' \in G_L$ we have that $g(\gamma\tau) = g\left(\gamma'\left(\sigma^i\tau'\sigma^{-i}\right)\sigma^{i+j}\right) = g\left(\gamma'\right) g\left(\sigma^i\tau'\sigma^{-i}\right) = g\left(\gamma'\right)\sigma^i g(\tau') = g(\gamma)\,\gamma g(\tau)$. □

We will now prove a technical lemma that will be useful to determine the image of the restriction.

Lemma 4.3.8. *Let k be a field of characteristic prime to q containing a primitive q-th root of unity. Let $k \subset L \subset F$ be a tower of field extensions so that each extension is Galois of degree q. Let $a \in L^\times$ such that $F = L(\sqrt[q]{a})$. Fix a representative $\sigma \in G_k$ that generates $\mathrm{Gal}(L/k)$.*

Suppose that for every $\gamma \in G_k$ we have that $\gamma^q \left(\sqrt[q]{\sigma^i(a)} \right) = \sqrt[q]{\sigma^i(a)}$ for $0 \leq i < q$. Then there exists some $b \in k^\times$ such that $a \equiv b \mod (L^\times)^q$.

Proof. Assume that $a \notin k^\times$. Fix $\sigma \in G_k$ such that $\overline{\sigma}$ generates $\mathrm{Gal}(L/k)$. Denote the Galois closure of the extension F over k by $\tilde{L}$. By Galois theory $\tilde{L} = L\left(\sqrt[q]{a}, \sqrt[q]{\sigma(a)}, \ldots, \sqrt[q]{\sigma^{q-1}(a)} \right)$ and $\mathrm{Gal}(\tilde{L}/L)$ is isomorphic to $(\mathbb{Z}/q\mathbb{Z})^r$ for $r = 1$, or $r = q$. We prove the lemma by contradiction. So assume that $r = q$. Let $\tau \in \mathrm{Gal}(\tilde{L}/L)$ be the element with $\tau\left(\sqrt[q]{a}\right) = \rho \sqrt[q]{a}$ and $\tau\left(\sigma^i \sqrt[q]{a}\right) = \sigma^i \sqrt[q]{a}$ for $1 \leq i < q$. Now $(\sigma\tau)\left(\sqrt[q]{a}\right) = (\rho\sigma^q)\left(\sqrt[q]{a}\right) = \rho\left(\sqrt[q]{a}\right)$, which is a contradiction to our assumptions. We conclude that F/k is Galois of degree q^2. We want to show that $\mathrm{Gal}(F/k) = \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$.

Next suppose that $\mathrm{Gal}(F/k) = \mathbb{Z}/q^2\mathbb{Z}$ and denote the generator by τ. Then τ^q fixes L, as $\tau^q(\sqrt[q]{a}) = \sqrt[q]{a}$ implies that $\tau^q(a) = a$ and $L = k(a)$. Hence $\tau \in \mathrm{Gal}(F/L)$, which implies that τ is of order q, a contradiction. We conclude that $\mathrm{Gal}(F/k) \cong \mathbb{Z}/q\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Consider the fixed field $F^{\langle\sigma\rangle}$, which is a degree q extension of k. By Kummer theory, there exists an element $b \in k^\times$ so that $F^{\langle\sigma\rangle} = k\left(\sqrt[q]{b}\right)$. Finally, $F = L\left(\sqrt[q]{b}\right) = L\left(\sqrt[q]{a}\right)$ and thus by Kummer theory $a \equiv b \mod (L^\times)^q$. □

Proposition 4.3.9. *The image of the restriction map corresponds to the set*

$$\left(k^\times / \left((L^\times)^q \cap k^\times\right)\right) \times \{1\} \subset L^\times/(L^\times)^q \times L^\times/(L^\times)^q$$

under the isomorphism ϕ^{-1}.

Proof. Let $(a, b) \in L^\times/(L^\times)^q \times L^\times/(L^\times)^q$ be in the image of the restriction map. There exists some $f \in H^1(k, M)$ so that $\phi^{-1} \circ \mathrm{res}(f) = (a, b)$. Then (a, b) is necessarily in the preimage $\phi^{-1}\left(H^1(L, M)^{G_k/G_L}\right)$ and by lemma 4.3.6 we see that $(a, b) \equiv \left(a, \frac{a}{\sigma(a)}\right)$ so that

$\sigma(a)^2 \equiv \sigma^2(a)a \mod (L^\times)^q$. It remains to show that we can choose $a \in k^\times$.

By definition of ϕ and by lemma 4.3.7, we get that $\gamma^q\left(\sqrt[q]{a}\right) = \sqrt[q]{a}$ and $\gamma^q\left(\sqrt[q]{\frac{a}{\sigma(a)}}\right) = \sqrt[q]{\frac{a}{\sigma(a)}}$ for any $\gamma \in G_k$ and for any choice of q^{th} root of $\frac{a}{\sigma(a)}$. Using the condition that $\sigma(a)^2 \equiv \sigma^2(a)a$, we deduce that $\gamma^p\left(\sqrt[q]{\sigma^i(a)}\right) = \sqrt[q]{\sigma^i(a)}$ for any i. The statement follows from lemma 4.3.8. □

The following theorem summarizes the results of this section.

Theorem 4.3.10. *Suppose that $[G_k : G_L]$ is of order q and assume that there is some $\sigma \in G_k$ with $\sigma(Q) = P \oplus Q$ such that $\overline{\sigma}$ generates G_k/G_L. Additionally denote a primitive element for the extension L/k by l.*

$$ {}_q\mathrm{Br}(E) = {}_q\mathrm{Br}(k) \oplus I $$

and I has generators $\left\{\left(l^q, n_Q\right)_{k(E)}, (a, t_P)_{k(E)} : a \in k^\times\right\}$, where $n_Q \in k(E)$ with $n_Q^q = N_{L(E)/k(E)}(t_Q)$.

4.4 q divides the degree $[L : k]$

Suppose for this section that q divides $[L : k]$. Let $k \subset L' \subset L$ be an intermediate field so that L/L' is a Galois extension of degree q and q does not divide the degree L'/k. After renaming P and Q, we may assume that there is some element $\sigma \in G_k$ so that $\overline{\sigma}$ generates $\mathrm{Gal}(L/L')$ and $\sigma(P) = P$ and $\sigma(Q) = P \oplus Q$. Furthermore, let $l \in L$ with $l^q \in L'$ and $L = L'(l)$. Fix $t_P, t_Q \in L(E)$ with $\mathrm{div}(t_P) = q(P) - q(0)$ and $\mathrm{div}(t_Q) = q(Q) - q(0)$. Assume additionally that $t_P \circ [q], t_Q \circ [q] \in \left(L(E)^\times\right)^d$. Furthermore, let $\alpha_Q \in \overline{k(E)}$ so that

$\alpha_Q^q = t_Q$.

Although the field extension L'/k might not be Galois, restriction followed by corestriction coincides with multiplication by $[L' : k]$, which is an isomorphism. Using the previous section we deduce the following result.

Proposition 4.4.1. *Under the above assumptions, the Brauer group decomposes as*

$$ {}_q\mathrm{Br}(E) = {}_q\mathrm{Br}(k) \oplus I $$

and every element in I can be expressed using the generators

$$ \left\{ \mathrm{cor}\left(l^q, n_Q\right)_{L'(E)}, \mathrm{cor}(a, t_P)_{L'(E)} : a \in L'^{\times} \right\}. $$

This completes the description of the generators of ${}_q\mathrm{Br}(E)$.

Chapter 5

Relations

In this chapter we describe the relations in the Brauer group. Recall that that an element in I as before is trivial if and only if it is in the image of the composition

$$E(k)/[d]E(k) \xrightarrow{\delta} H^1(k, M) \xrightarrow{\epsilon} {}_d\mathrm{Br}(k) \ .$$

As in the section before, we will consider various cases depending on the rationality of the d-torsion M.

5.1 M is k-rational

Assume for this section that M is k-rational. Recall the isomorphism

$$\begin{aligned} \phi : \left(k^\times / \left(k^\times\right)^d\right) \times \left(k^\times / \left(k^\times\right)^d\right) &\to H^1(k, M) \\ (a, b) &\mapsto \left[c_{a,b}\right] \end{aligned}$$

from eq. (4.3). We first describe the composition $\phi^{-1} \circ \delta$.

Proposition 5.1.1. *Let $R \in E(k)/[d]E(k)$ and let $t_P, t_Q \in k(E)$ with $\operatorname{div}(t_P) = d(P) - d(0)$, $\operatorname{div}(t_Q) = d(Q) - d(0)$. Assume that $t_P \circ [d], t_Q \circ [d] \in (k(E)^\times)^d$. Then*

$$\phi^{-1} \circ \delta(R) = \begin{cases} (1,1) & R = 0 \\ \left(t_Q(P), \frac{t_P(P \oplus Q)}{t_P(Q)}\right) & R = P \\ \left(\frac{t_Q(P \oplus Q)}{t_Q(P)}, t_P(Q)\right) & R = Q \\ \big(t_Q(R), t_P(R)\big) & \textit{else} \end{cases}$$

The proof of this proposition is inspired by a computation of the Kummer pairing in [Sil09, Ch. X, Theorem 1.1].

Proof. Let $R \in E(k)/dE(k) \setminus \{0, P, Q\}$ and fix some $S \in E(\overline{k})$ with $[d]S = R$. Let t_P, t_Q as above and fix $g_P, g_Q \in \overline{k}(E)$ with $g_P^d = t_P \circ [d]$ and $g_Q^d = t_Q \circ [d]$. Since the divisors of g_P and g_Q are G_k-invariant, we may choose $g_P, g_Q \in k(E)$. By the definition of ϕ we see that for $\phi(f) = (a, b)$ for some cocycle $H^1(k, M)$ means that

$$\mathrm{e}\left(f(\gamma), P\right) = \frac{\gamma\left(\sqrt[d]{b}\right)}{\sqrt[d]{b}} \text{ and } \mathrm{e}\left(f(\gamma), Q\right) = \frac{\gamma\left(\sqrt[d]{a}\right)}{\sqrt[d]{a}}.$$

The Weil pairing satisfies

$$\mathrm{e}(\gamma(S) \ominus S, P) = \frac{g_P(\gamma(S) \ominus S \oplus S)}{g_P(S)} = \frac{g_P(\gamma(S))}{g_P(S)} = \frac{\gamma(g_P(S))}{g_P(S)}.$$

Additionally by definition of g_P, we see that $g_P(S)^d = t_P \circ [d](S) = t_P(R)$. A similar result holds for Q as well. Therefore $\phi^{-1} \circ \delta(R) = \big(t_Q(R), t_P(R)\big)$. The other results follow by bilinearity of the Weil pairing. □

Summarizing these results, we conclude theorem 1.0.5.

From now on assume that $d = q$ is an odd prime and L is the smallest Galois extension of k so that M is L-rational.

5.2 $[L : k]$ is coprime to q

Suppose throughout this section that q does not divide the order $[L : k]$. Consider the following commutative diagram

$$\begin{array}{ccccc} E(k)/[q]E(k) & \xrightarrow{\text{res}} & E(L)/[q]E(L) & \xrightarrow{\text{cor}} & E(k)/[q]E(k) \\ \downarrow{\scriptstyle \delta_k} & & \downarrow{\scriptstyle \delta_L} & & \downarrow{\scriptstyle \delta_k} \\ H^1(k, M) & \xrightarrow{\text{res}} & H^1(L, M) & \xrightarrow{\text{cor}} & H^1(k, M) \end{array},$$

where the horizontal compositions coincide with multiplication by $[L : k]$ and are therefore isomorphisms. Thus, the image of δ_k is also given by the image of the composition $\delta_k \circ \text{cor} = \text{cor} \circ \delta_L$. Using the description of the image of δ_L in the previous section, we deduce the following result.

Proposition 5.2.1. *Suppose that $[L : k]$ is not divisible by q. Fix two generators P and Q of M and and let $t_P, t_Q \in L(E)$ with $\text{div}(t_P) = q(P) - q(0)$ and $\text{div}(t_Q) = q(Q) - q(0)$. Assume additionally that $t_P \circ [q], t_Q \circ [q] \in \left(L(E)^\times\right)^d$. An element*

$$\text{cor}(a, t_P)_{L(E)} \otimes \text{cor}(b, t_Q)_{L(E)}$$

in I is trivial if and only if it is similar to one of the following

- $\operatorname{cor}\left(t_Q(P), t_P\right)_{k(E)} \otimes \operatorname{cor}\left(\frac{t_P(P\oplus Q)}{t_P(Q)}, t_Q\right)_{k(E)}$,
- $\operatorname{cor}\left(\frac{t_Q(P\oplus Q)}{t_Q(P)}, t_P\right)_{k(E)} \otimes \operatorname{cor}\left(t_P(Q), t_Q\right)_{k(E)}$, *or*
- $\operatorname{cor}\left(t_Q(R), t_P\right)_{k(E)} \otimes \operatorname{cor}\left(t_P(R), t_Q\right)_{k(E)}$ *for some* $R \in E(k) \setminus \{0, P, Q\}$.

The following observation will be useful to calculate these corestrictions explicitly. Consider the following commutative diagram

$$\begin{array}{ccccccccc}
E(k) & \longrightarrow & E(L) & \longrightarrow & E(k) & \longrightarrow & E(L) & \longrightarrow & E(k) \\
\downarrow{\scriptstyle \delta_k} & & \downarrow{\scriptstyle \delta_L} & & \downarrow{\scriptstyle \delta_k} & & \downarrow{\scriptstyle \delta_L} & & \downarrow{\scriptstyle \delta_k} \\
H^1(k,M) & \xrightarrow{\text{res}} & H^1(L,M) & \xrightarrow{\text{cor}} & H^1(k,M) & \xrightarrow{\text{res}} & H^1(L,M) & \xrightarrow{\text{cor}} & H^1(k,M) \\
\downarrow{\scriptstyle \epsilon_k} & & \downarrow{\scriptstyle \epsilon_L} & & \downarrow{\scriptstyle \epsilon_k} & & \downarrow{\scriptstyle \epsilon_L} & & \downarrow{\scriptstyle \epsilon_k} \\
{}_q\mathrm{Br}\, E & \longrightarrow & {}_q\mathrm{Br}\, E_L & \longrightarrow & {}_q\mathrm{Br}\, E & \longrightarrow & {}_q\mathrm{Br}\, E_L & \longrightarrow & {}_q\mathrm{Br}\, E
\end{array},$$

where the composition of morphisms along a row give multiplication by $[L:k]^2$, which is an isomorphism. Furthermore, the composition $\operatorname{res} \circ \operatorname{cor}$ coincides with the Norm map [NSW08, Ch. 1, Corollary 1.5.7]. Therefore, an element in I is trivial if it lies in the image of the composition $\operatorname{cor} \circ \epsilon_L \circ N_{L/k} \circ \delta_L \circ \operatorname{res}$. In section 7.2, we see how this observation can be applied to the calculation of the relations in I.

5.3 $[L:k] = q$

Throughout this section suppose that $[L:k] = q$ and fix some generator $\overline{\sigma}$ of $\operatorname{Gal}(L/k)$. Let $P, Q \in M$ so that $\sigma(P) = P$ and $\sigma(Q) = P \oplus Q$. Furthermore, let $l \in L$ with $l^q \in k$ and $L = k(l)$. Fix $t_P, t_Q \in L(E)$ with $\operatorname{div}(t_P) = q(P) - q(0)$ and $\operatorname{div}(t_Q) = q(Q) - q(0)$. Assume additionally that $t_P \circ [q], t_Q \circ [q] \in \left(L(E)^\times\right)^d$. Fix $\tilde{\sigma} \in \tilde{G}_{L/k}$ as in section 4.3. Furthermore,

let $\alpha_Q \in \overline{k(E)}$ so that $\alpha_Q^q = t_Q$ and denote $n_Q = \prod_{i=0}^{n-1} \tilde{\sigma}^i(\alpha_Q)$.

Consider the commutative diagram with exact rows and columns

$$\begin{array}{ccccccc} & & & & 0 & & 0 \\ & & & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \frac{E(k)\cap[q]E(L)}{[q]E(k)} & \xrightarrow{\inf} & E(k)/[q]E(k) & \xrightarrow{\text{res}} & E(L)/[q]E(L) \\ & & \downarrow{\scriptstyle \delta_{L/k}} & & \downarrow{\scriptstyle \delta_k} & & \downarrow{\scriptstyle \delta_L} \\ 0 & \longrightarrow & H^1(\mathrm{Gal}(L/k), M) & \xrightarrow{\inf} & H^1(k, M) & \xrightarrow{\text{res}} & H^1(L, M) \end{array},$$

where $\delta_{L/k}$ is the map induced by δ_k. It is immediate that $\delta_{L/k}$ is injective. Recall that $H^1(\mathrm{Gal}(L/k), M)$ is cyclic of order q with generator f_L. Furthermore, we saw that $\epsilon_L(\inf(f_L)) = \left(l^q, n_Q\right)_{k(E)}$ (proposition 4.3.3). We deduce the following result.

Proposition 5.3.1. *The Brauer class of $\left(l^q, n_Q\right)_{k(E)}$ is trivial, that is, it is in the image of the map $\mathrm{Br}(k) \to \mathrm{Br}(E)$, if and only if the quotient $\frac{E(k)\cap[q]E(L)}{[q]E(k)}$ is non-trivial.*

Recall that by proposition 4.3.9 any element in the image of $\left(\phi^{-1} \circ \text{res}\right)$ can be written as $(a, 1)$ for some $a \in k^\times$.

Proposition 5.3.2. *The Brauer class of $(a, t_P)_{k(E)}$ is trivial if and only if there is some $R \in E(k)/[q]E(k)$ so that $\phi^{-1}(a, 1) = \delta_L(R)$.*

5.4 q divides $[L : k]$

Suppose that q divides $[L : k]$ and use the notation used in section 4.4. Recall that every element in I can be written as $\mathrm{cor}(A)$ for some $A \in {}_q\mathrm{Br}(E \times \mathrm{Spec}(L'))$. Such an element is trivial if and only if it is similar to $\epsilon_{L'} \circ \delta_{L'}$. Remark that some corestrictions of elements in

${}_q\mathrm{Br}(E_L)$ may coincide and we do not account for this in our description.

Chapter 6

Conclusions – The Algorithm

In this chapter, we summarize the results from the previous chapters and assemble the algorithm to calculate generators and relations of the Brauer group. Let k be a field of characteristic different from 2 or 3 and let q be an odd prime. Assume that q is coprime to the characteristic of k and that k contains a primitive q-th root of unity. Let E be an elliptic curve over k. Denote by M the q torsion of $E(\overline{k})$.

The Brauer group of E decomposes as

$$ {}_q\mathrm{Br}(E) = {}_q\mathrm{Br}(k) \oplus I $$

and generators $\mathcal{G}$ and relations $\mathcal{R}$ of I can be calculated using the following algorithm.

1. Determine the kernel of the natural Galois representation

$$ \Psi : G_k \to \mathrm{End}(M) = GL_2\left(\mathbb{F}_q\right). $$

Denote by L the fixed field of this kernel.

2. (a) If q divides the order of L/k, fix some intermediate field L' so that L/L' is a Galois extension of degree q. Let P and Q be elements in M so that $\mathrm{Gal}(L/L')$

is generated by $\overline{\sigma}$ with $\sigma(P) = P$ and $\sigma(Q) = P \oplus Q$. Set

$$\mathcal{G}_{L'} = \left\{ \left(l^q, n_Q\right)_{L'(E)}, (a, t_P)_{L'(E)} : a \in L'^{\times} \right\},$$

where $t_P \in L'(E)$ with $\operatorname{div}(t_P) = q(P) - q(0)$ and $n_Q \in L'(E)$ with $\operatorname{div}(n_Q) = \sum_{i=0}^{q-1} \sigma^i(Q) = \sum_{i=0}^{q-1}(iP + Q)$. Furthermore, let $t_Q \in L(E)$ with $\operatorname{div}(t_Q) = q(Q) - q(0)$ and $n_Q^q = N_{L(E)/k(E)}(t_Q)$.

(b) If q does not divide the order of L/k, fix some generators P and Q of M. Set

$$\mathcal{G}_{L'} = \left\{ (a, t_P)_{L(E)}, \left(b, t_Q\right)_{L(E)} : a, b \in L^{\times} \right\},$$

where $t_P, t_Q \in L(E)$ with $\operatorname{div}(t_P) = q(P) - q(0)$ and $\operatorname{div}(t_Q) = q(Q) - q(0)$.

3. Set

$$\mathcal{R}_L = \left\{ \begin{array}{l} \left(t_Q(P), t_P\right)_{L(E)} \otimes \left(\dfrac{t_P(P \oplus Q)}{t_P(Q)}, t_Q\right)_{L(E)}, \\ \left(\dfrac{t_Q(P \oplus Q)}{t_Q(P)}, t_P\right)_{L(E)} \otimes \left(t_P(Q), t_Q\right)_{L(E)} \end{array} \right\}$$
$$\cup \left\{ \left(t_Q(R), t_P\right)_{L(E)} \otimes \left(t_P(R), t_Q\right)_{L(E)} : R \in E(L) \setminus \{P, Q\} \right\}.$$

(a) If q divides the order of L/k, let

$$\mathcal{R}_{L', \mathrm{res}} = \left\{ (a, t_P)_{L'(E)} : \mathrm{res}(a, t_P)_{L'(E)} \in \mathcal{R}_L \right\}.$$

Further, if the quotient $\frac{E(k)\cap[q]E(L)}{[q]E(k)}$ is not trivial let

$$\mathcal{R}_{L',\,\mathrm{inf}} = \left\{ \left(l^q, n_Q\right)_{L'(E)} \right\}.$$

If the quotient is trivial, let $\mathcal{R}_{L',\,\mathrm{inf}} = \emptyset$. Set $\mathcal{R}_{L'} = \mathcal{R}_{L',\,\mathrm{res}} \cup \mathcal{R}_{L',\,\mathrm{inf}}$.

(b) If q does not divide the order of L/k, let $L = L'$ and $\mathcal{R}_{L'} = \mathcal{R}_L$.

4. Set

$$\mathcal{G} = \left\{ \mathrm{cor}(A) : A \in \mathcal{G}_{L'} \right\}$$

and

$$\mathcal{R} = \left\{ \mathrm{cor}(A) : A \in \mathcal{R}_{L'} \right\}.$$

Note that there are additional relations that come from the fact that the corestriction map is not injective. These relations need a more careful treatment. See for example section 7.2. A direct consequence of algorithm 7.2.2 is the following.

Corollary 6.0.1. *Every element in I as above can be written as a tensor product of at most $2(q-1)^2(q+1)$ symbol algebras.*

Remark 6.0.2. *Note that we assume that the characteristic of k is different form 2 or 3 for simplicity of the presentation of the elliptic curves and its torsion subgroups. The general results still hold in characteristic equal to two and three.*

Chapter 7

Examples

In this chapter, we calculate the q-torsion of the Brauer group for some elliptic curves E, where q is an odd prime. For computational reasons, we only consider the case $q = 3$. The algorithm described in chapter 6 can be used to determine ${}_q\mathrm{Br}(E)$ for any odd prime q. As before, we will consider various cases depending on the extension L, that is the smallest Galois extension of k, so that M is L-rational.

7.1 M is k-rational over a number field

Let $k = \mathbb{Q}(\omega) \subset \mathbb{C}$, where ω is a primitive third root of unity. In [Pal10] the author describes a family of elliptic curves such that M is $\mathbb{Q}(\omega)$-rational, for example E given by the affine equation $y^2 = x^3 + 16$. In this case, the three torsion of E is generated by $P = (0, 4)$ and $Q = (-4, 8\omega + 4) = (-4, 4\sqrt{3}i)$. Furthermore, the tangent lines at P and Q, respectively are given by $t_P = y - 4$ and

$$t_Q = y - \frac{6}{2\omega + 1}(x + 4) - 8\omega - 4 = y - 4\sqrt{3}ix - 20\sqrt{3}i.$$

By the previous discussion ${}_3\mathrm{Br}(E) = {}_3\mathrm{Br}(k) \oplus I$ and every element in I can be written as a tensor product

$$(a, y - 4)_{3,k(E)} \otimes \left(b, y - 4\sqrt{3}ix - 20\sqrt{3}i\right)_{3,k(E)} \tag{7.1}$$

for some $a, b \in k^\times$. We calculate with the magma code in the appendix , that $E(k) = M$ and therefore also $E(k)/3E(k) = M$. By our previous calculations on the relations, a tensor product as in eq. (7.1) is trivial if and only if it is similar to an element in the subgroup generated by

$$\left(4 - 20\sqrt{3}i, t_P\right)_{k(E)}$$

and

$$\left(\frac{6}{19} - \frac{8}{19}\sqrt{3}i, t_P\right)_{k(E)} \otimes \left(4\sqrt{3}i - 4, t_Q\right)_{k(E)}.$$

7.2 Degree L/k coprime to q for k a number field

We first need to discuss computational results for the corestriction of symbol algebras.

Lemma 7.2.1. *Let $K \subset F$ be a finite extension of fields over k. Then*

$$\mathrm{cor}_{F/K}(a, b) = \left(a, N_{F/K}(b)\right)$$

for all $a \in K^\times, b \in F^\times$.

Proof. See for instance [Ser79, page 209]. □

The following algorithm from [RT83, Section 3] may also be used to calculate the corestriction explicitly. For a polynomial $p(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_m t^m$ with $a_m a_n \neq 0$ define $p^*(t) = \frac{p(t)}{a_m t^m}$ and $c(p) = (-1)^n a_n$.

Algorithm 7.2.2. *Let $K \subset F$ be a finite extension of fields over k and let $a, b \in F^\times$. Let $g(t) \in K[t]$ be the minimal polynomial of a over K and $f(t) \in K[t]$ is the polynomial of smallest degree such that $N_{F/K(a)}(b) = f(a)$. Define a sequence $g_0, \ldots, g_m$ of nonzero*

polynomials by setting $g_0 = g, g_1 = f$, *and for* $i \geq 1$ *let* g_{i+1} *be the remainder of the division of* g_{i-1}^* *by* g_i *as long as* $g_i \neq 0$. *Then*

$$\mathrm{cor}_{F/K}(a,b)_F = -\sum_{i=q}^{m} \left(c(g_{i-1}^*), c(g_i)\right)_K .$$

Let $k = \mathbb{Q}(\omega)$ and E the elliptic curve given by the affine equation

$$y^2 = x^3 + B,$$

where $B \equiv 2 \mod (\mathbb{Q}^\times)^3$ and $B \not\equiv 1, -3 \mod (\mathbb{Q}^\times)^2$. By [BP12, Theorem 3.2 and Corollary 3.3] we get that $L = k(\sqrt{B})$. Let σ be given by $\sigma(\sqrt{B}) = -\sqrt{B}$. The three torsion of E has generators P and Q with $P = (0, \sqrt{B})$ and $Q = \left(\sqrt[3]{-4B}, \sqrt{-3B}\right)$. Then $\sigma(P) = 2P$ and $\sigma(Q) = 2Q$. We need to calculate

$$\mathrm{cor}_{L(E)/k(E)} \left((a, t_P)_{L(E)} \otimes (b, t_Q)_{L(E)}\right).$$

Recall that by remark 4.2.2, it will be enough to consider (a, b) a Norm in $L^\times/(L^\times)^3 \times L^\times/(L^\times)^3$. For $(a,b) \in L^\times/(L^\times)^3 \times L^\times/(L^\times)^3$ we have $N_{L/k}(a,b) = \left(\frac{a}{\sigma(a)}, \frac{b}{\sigma(b)}\right)$, or equivalently we may assume that $N_{L/k}(a) = 1$ and $N_{L/k}(b) = 1$ and $a, b \in L^\times \setminus k^\times$. Note that

$$t_P = y - \sqrt{B}$$

and

$$t_Q = y - \frac{3\sqrt[3]{-4B}}{2\sqrt{-3B}}x - 3\sqrt{-3B}.$$

Furthermore, $\sqrt{-3} \in k$ as $\omega \in k$ and $\sqrt[3]{16B^2} \in k^\times$ since $B \equiv 2 \mod (\mathbb{Q}^\times)^3$.

Let $a = a_1\sqrt{B} + a_2$ with $a_1 \neq 0$ and $N_{L/k}(a) = 1$. We now employ algorithm 7.2.2 to calculate $\mathrm{cor}(a, t_P)_{L(E)}$. In the notation of algorithm 7.2.2, we calculate

$$\begin{aligned}
g_0 &= \text{Minimal Polynomial of } a \text{ over } k \\
&= (t - a_1\sqrt{B} - a_2)(t + a_1\sqrt{B} - a_2) \\
&= t^2 - 2a_2t + a_2^2 - Ba_1^2 \\
&= t^2 - 2a_2t + N_{L/k}(a) \\
&= t^2 - 2a_2t + 1, \\
g_0^* &= t^2 - 2a_2t + 1, \\
g_1 &= y - \frac{a_2 - t}{a_1} \\
&= \frac{1}{a_1}t + y - \frac{a_2}{a_1} \\
g_1^* &= \frac{1}{a_1y - a_2}t + 1.
\end{aligned}$$

The element g_2 is the remainder of the division of g_0^* by g_1. Note that

$$\begin{aligned}
\left(a_1t - a_1a_2 - a_1^2y\right) g_1 &= t^2 - 2a_2t + a_2^2 - a_1^2y^2 \\
&= g_0^* - 1 + a_2^2 - a_1^2y^2
\end{aligned}$$

and therefore

$$g_2 = 1 - a_2^2 + a_1^2y^2 = 1 - a_2^2 + a_1^2x^3 + a_1^2B = 1 - N_{L/k}(a) + a_1^2x^3 = a_1^2x^3.$$

Overall, the corestriction is

$$\begin{aligned}\operatorname{cor}(a, t_P) &= \left(1, -\frac{1}{a_1}\right)_{k(E)}^{-1} \otimes \left(\frac{1}{a_2 - a_1 y}, a_1^2 x^3\right)_{k(E)}^{-1} \\ &= \left(a_2 - a_1 y, a_1^2 x^3\right)_{k(E)} \\ &= \left(a_2 - a_1 y, a_1^2\right)_{k(E)}.\end{aligned}$$

Finally, let $b = b_1\sqrt{B} + b_2$ with $b_1 \neq 0$ and $N_{L/k}(b) = 1$. Use the notation of algorithm 7.2.2 to calculate $\operatorname{cor}(b, t_Q)_{L(E)}$. Then

$$\begin{aligned}g_0 &= t^2 - 2b_2 t + 1, \\ g_0^* &= t^2 - 2b_2 t + 1, \\ g_1 &= -\frac{\sqrt{3}i}{b_1}(x+1)\,t + y + \frac{\sqrt{3}ib_2}{b_1}(x+1).\end{aligned}$$

Furthermore, note that

$$\begin{aligned}\left(-\frac{b_1}{\sqrt{3}i(x+1)}t + \frac{b_1 b_2}{\sqrt{3}i(x+1)} + \frac{y b_1^2}{3(x+1)^2}\right) g_1 &= t^2 - 2b_2 t + b_2^2 + \frac{b_1^2}{3(x+1)^2}y^2 \\ &= g_0^* - 1 + b_2^2 + \frac{b_1^2}{3(x+1)^2}y^2\end{aligned}$$

and therefore

$$g_2 = 1 - b_2^2 - \frac{b_1^2}{3(x+1)^2}y^2 = 1 - b_2^2 - \frac{b_1^2(x^3 + B)}{3(x+1)^2}.$$

We deduce that

$$\begin{aligned}\operatorname{cor}(b, t_Q)_{L(E)} &= \left(1, \frac{\sqrt{3}i}{b_1}(x+1)\right)_{k(E)}^{-1} \otimes \left(\frac{\frac{\sqrt{3}i}{b_1}(x+1)}{y + \frac{\sqrt{3}ib_2}{b_1}(x+1)}, 1 - b_2^2 - \frac{b_1^2(x^3+B)}{3(x+1)^2}\right)_{k(E)}^{-1} \\ &= \left(\frac{yb_1}{\sqrt{3}i\,(x+1)} + b_2, 1 - b_2^2 - \frac{b_1^2(x^3+B)}{3(x+1)^2}\right)_{k(E)}.\end{aligned}$$

Overall, the 3-torsion of the Brauer group decomposes as follows.

Proposition 7.2.3. *Let $k = \mathbb{Q}(\omega)$ and let E be an elliptic curve given by $y^2 = x^3 + B$, where $B \equiv 2 \mod (\mathbb{Q}^\times)^3$ and $B \not\equiv 1, -3 \mod (\mathbb{Q}^\times)^2$. Then the 3-torsion of the Brauer group decomposes as*

$$ {}_3\mathrm{Br}(E) = {}_3\mathrm{Br}(k) \oplus I$$

and every element in I can be written as a tensor product

$$\left(a_2 - a_1 y, a_1^2\right)_{k(E)} \otimes \left(\frac{yb_1}{\sqrt{3}i\,(x+1)} + b_2, 1 - b_2^2 - \frac{b_1^2(x^3+B)}{3(x+1)^2}\right)_{k(E)}$$

for some $a_1, a_2, b_1, b_2 \in k^\times$ with $a_1, b_1 \neq 0$, and $a_2^2 - Ba_1^2 = b_2^2 - Bb_1^2 = 1$.

To calculate the relations we need to specify B. We first consider the case $B = -1024$. Using the code in the appendix , we calculate that $E(k) = 0$. Thus there are no additional relations. Note that some elements might still become trivial due to the fact that the corestriction map is not surjective.

Consider the case $B = 2$. We use the code in the appendix to see that $E(k) \cong \mathbb{Z}^2$ with generators $R = (-\omega, 1) = \left(\frac{1}{2} - \frac{\sqrt{-3}}{2}, 1\right)$ and $S = (-1, -1)$. In this case $P = (0, \sqrt{2}), Q = (-2, \sqrt{-3}\sqrt{2}), t_P = y - \sqrt{2}$, and $t_Q = y + \sqrt{-3}\sqrt{2}x + \sqrt{-3}\sqrt{2}$. Therefore by a direct

computation

$$
\begin{aligned}
t_P(R) &= 1-\sqrt{2}, & \frac{t_P(R)}{\sigma(t_P(R))} &= 2\sqrt{2}-3,\\
t_Q(R) &= 1+\frac{3}{2}\sqrt{-3}\sqrt{2}+\frac{3}{2}\sqrt{2}, & \frac{t_Q(R)}{\sigma(t_Q(R))} &\equiv \left(-51+57i\sqrt{3}\right)\sqrt{2}-323+18i\sqrt{3},\\
t_P(S) &= -1-\sqrt{2}, & \frac{t_P(S)}{\sigma(t_P(S))} &= -2\sqrt{2}-3,\\
t_Q(S) &= -1, & \frac{t_Q(S)}{\sigma(t_Q(S))} &= 1.
\end{aligned}
$$

Consider the following commutative diagram

$$
\begin{array}{ccccccccc}
E(k) & \longrightarrow & E(L) & \longrightarrow & E(k) & \longrightarrow & E(L) & \longrightarrow & E(k)\\
\downarrow{\scriptstyle \delta_k} & & \downarrow{\scriptstyle \delta_L} & & \downarrow{\scriptstyle \delta_k} & & \downarrow{\scriptstyle \delta_L} & & \downarrow{\scriptstyle \delta_k}\\
H^1(k,M) & \xrightarrow{\text{res}} & H^1(L,M) & \xrightarrow{\text{cor}} & H^1(k,M) & \xrightarrow{\text{res}} & H^1(L,M) & \xrightarrow{\text{cor}} & H^1(k,M)\\
\downarrow{\scriptstyle \epsilon_k} & & \downarrow{\scriptstyle \epsilon_L} & & \downarrow{\scriptstyle \epsilon_k} & & \downarrow{\scriptstyle \epsilon_L} & & \downarrow{\scriptstyle \epsilon_k}\\
{}_3\mathrm{Br}\, E & \longrightarrow & {}_3\mathrm{Br}\, E_L & \longrightarrow & {}_3\mathrm{Br}\, E & \longrightarrow & {}_3\mathrm{Br}\, E_L & \longrightarrow & {}_3\mathrm{Br}\, E
\end{array}
\quad ,
$$

where the rows compose to multiplication by 4, which is the identity on three torsion. An element in I is trivial if it is similar to an element in the subgroup generated by $\epsilon_k \circ \delta_k(R)$ and $\epsilon_k \circ \delta_k(S)$. Finally,

$$\epsilon_k \circ \delta_k(R) = \mathrm{cor} \circ \epsilon_L \circ N_{L(E)/k(E)} \circ \delta_L \circ \mathrm{res}(R)$$

and therefore by our previous calculations of the Norm map and corestriction, we get that

$$\begin{aligned}\epsilon_k \circ \delta_k(R) =& \operatorname{cor}\left(\frac{t_Q(R)}{\sigma(t_Q(R))}, t_P\right)_{L(E)} \otimes \operatorname{cor}\left(\frac{t_P(R)}{\sigma(t_P(R))}, t_Q\right)_{L(E)} \\ =& \left(-323 + 18i\sqrt{3} - \left(-51 + 57i\sqrt{3}\right) y, \left(-51 + 57i\sqrt{3}\right)^2\right)_{k(E)} \\ & \otimes \left(\frac{2y}{\sqrt{3}i\,(x+1)} - 3, -8 - \frac{4(x^3+2)}{3(x+1)^2}\right)_{k(E)}\end{aligned}$$

and similarly

$$\begin{aligned}\epsilon_k \circ \delta_k(S) =& \operatorname{cor}\left(\frac{t_P(S)}{\sigma(t_P(S))}, t_Q\right)_{L(E)} \\ =& \left(\frac{-2y}{\sqrt{3}i\,(x+1)} - 3, -8 - \frac{4(x^3+2)}{3(x+1)^2}\right)_{k(E)}.\end{aligned}$$

7.3 Degree $L/k = q$ for k a number field

Let $k = \mathbb{Q}(\omega)$, $\omega = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ and let E be the elliptic curve given by the affine equation

$$y^2 = x^3 + 4.$$

Then the third division polynomial is $\psi_3(x) = 3x^4 + 48$. We use this to calculate that generators of the three torsion are given by $P = (0, 2)$ and $Q = (-2\sqrt[3]{2}, 2i\sqrt{3})$. Let $l = \sqrt[3]{2}$. In our previous notation $L = k\left(\sqrt[3]{2}\right)$ and the Galois group $\operatorname{Gal}(L/k)$ is generated by $\overline{\sigma}$ with

$\sigma(Q) = P + Q = (-\omega 2\sqrt[3]{2}, 2i\sqrt{3})$. It can be seen that

$$t_P = y - 2$$
$$t_Q = y + i\sqrt{3}\sqrt[3]{4}x + 2i\sqrt{3}$$

Using chapter 6 or theorem 4.3.10 we deduce that the Brauer group ${}_3\mathrm{Br}(E) = {}_3\mathrm{Br}(k) \oplus I$ and I is generated by

$$\left\{ \left(l^3, n_Q\right)_{k(E)}, (a, t_P)_{k(E)} : a \in k^{\times}. \right\}$$

We will now determine n_Q explicitly. Note that the line through Q and $P + Q$ has divisor $Q + (P \oplus Q) + (2P \oplus Q)$. Furthermore, a straightforward calculation shows that

$$\begin{aligned}
(y - 2\sqrt{3}i)^3 &= y^3 - 6\sqrt{3}iy^2 - 36y + 24\sqrt{3}i \\
&= y^3 + 6\sqrt{3}iy^2 - 36y - 24\sqrt{3}i - 12\sqrt{3}i\left(y^2 - 4\right) \\
&= y^3 + 6\sqrt{3}iy^2 - 36y - 24\sqrt{3}i - 12\sqrt{3}ix^3 \\
&= \left(y + 2\sqrt{3}i\right)^3 + 4\left(i\sqrt{3}x\right)^3 \\
&= N_{L(E)/k(E)}(t_Q)
\end{aligned}$$

We summarize our calculations in the following proposition.

Proposition 7.3.1. *Let $k = \mathbb{Q}(\omega)$, $\omega = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$ and let E be the elliptic curve given by the affine equation $y^2 = x^3 + 4$. Then the Brauer group decomposes as*

$${}_3\mathrm{Br}(E) = {}_3\mathrm{Br}(k) \oplus I$$

and every element in I can be written as a tensor product of the symbol algebras

$$\left(2, y - 2\sqrt{3}i\right)_{3,k(E)} \text{ and } (a, y-2)_{3,k(E)}$$

for some $a \in k^{\times}$.

We calculate with magma, that $E(k) = \langle P \rangle$ and $E(L) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Therefore $E(k)/3E(k) = \langle P \rangle$ and $E(L)/3E(L) = M$ and the quotient $\frac{E(k) \cap [3]E(L)}{[3]E(k)}$ is trivial. Therefore the symbol algebra $\left(2, y - 2\sqrt{3}i\right)_{k(E)}$ is not trivial.

Finally, $\epsilon \circ \delta \circ \mathrm{res}(P) = \left(2 + i\sqrt{3}, y - 2\right)_{L(E)}$ and therefore a symbol algebra $(a, y-2)_{k(E)}$ is trivial if and only if it is similar to one of the following

$$\left\{(1,1)_{k(E)}, \left(2 + i\sqrt{3}, y - 2\right)_{k(E)}, \left(-8 + 8i\sqrt{3}, y - 2\right)_{k(E)}\right\}$$

7.4 Positive rank over a number field

Let ω be a primitive third root of unity in $\mathbb{C}$, i.e. $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Set $k = \mathbb{Q}(\omega)$ and let E be the elliptic curve defined by the affine equation

$$y^2 = x^3 - 48.$$

The third division polynomial associated to E is

$$\psi_3(x) = 3x^3 - 576x = 3x^3 - 2^6 3^2 x.$$

We calculate directly that the three torsion M of $E(\overline{k})$ is generated by $P = (0, 8\omega + 4) = \left(0, 4i\sqrt{3}\right)$ and $Q = \left(4\sqrt[3]{3}, 12\right)$. Furthermore, we see by direct computation that $P \oplus Q = \left(\omega^2 4\sqrt[3]{3}, 12\right)$. Now using the code in the appendix we calculate that $E(k) \cong \mathbb{Z}^2 \oplus \mathbb{Z}/3\mathbb{Z}$ and $E(L) \cong \mathbb{Z}^2 \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Furthermore, generators of $E(L)$ are

$$\left\{ \begin{array}{c} P, Q, R = (-4\omega - 4, -4) = \left(-2i\sqrt{3}, -4\right), \\ S = \left((\omega + 1)\left(\sqrt[3]{3}\right)^2 + \omega\sqrt[3]{3} + 3, (\omega - 1)\left(\sqrt[3]{3}\right)^2 + (3\omega + 6)\sqrt[3]{3} + 6\omega + 3\right) \end{array} \right\}$$

We conclude that the quotient $\frac{E(k) \cap [3]E(L)}{[3]E(L)}$ is nontrivial. Finally, the polynomials t_P and t_Q are

$$t_P = y - 8\omega - 4 = y - 4i\sqrt{3}$$
$$t_Q = y - \frac{1}{6}\left(\sqrt[3]{3}\right)^2 x - 12 - \frac{2}{3}$$

By our algorithm the three torsion of the Brauer group decomposes as

$${}_3\mathrm{Br}(E) = {}_3\mathrm{Br}\, k \oplus I$$

and every element in I can be written as a $(a, t_P)_{k(E)}$ with $a \in k^\times$. Furthermore, an element in I is trivial if and only if its restriction to L is similar to an element in the

subgroup generated by

$$\left\{\begin{array}{c}\left(4i\sqrt{3}-12-\frac{2}{3},t_P\right)_{L(E)},\left(\frac{1}{134}\left(5-9i\sqrt{3}\right),t_P\right)_{L(E)}\otimes\left(12-4i\sqrt{3},t_Q\right)_{L(E)},\\ \left(\frac{\sqrt{3}i}{3}\left(\sqrt[3]{3}\right)^2-16-\frac{2}{3},t_P\right)_{L(E)}\otimes\left(-4-4i\sqrt{3},t_Q\right)_{L(E)},\\ \left((\omega-3)\left(\sqrt[3]{3}\right)^2+(\omega+4)\sqrt[3]{3}+\frac{11}{2}\omega-\frac{20}{3},t_P\right)_{L(E)}\\ \otimes\left((\omega-1)\left(\sqrt[3]{3}\right)^2+(3\omega+6)\sqrt[3]{3}-2\omega-1,t_Q\right)_{L(E)}\end{array}\right\}$$

7.5 Over a local field

Denote by $\mathbb{Q}_7$ the 7-adic field. It is easy to see that the field $\mathbb{Q}_7$ contains a primitive third root of unity ω. Let E be the elliptic curve

$$E: y^2 = x^3 + 16$$

over k. Consider the reduction $\tilde{E}$ of E modulo 7. Then $\tilde{E}$ is a non-singular curve and using the code in the appendix we see that

$$\tilde{E}\left(\mathbb{F}_7\right) = \mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z} = \{0,(0,3),(0,4),(3,1),(3,6),(5,1),(5,6),(6,1),(6,6)\}.$$

Denote by $\hat{E}$ the formal group associated to E and consider the group $\hat{E}\left(7\mathbb{Z}_7\right)$. By [Sil09, IV Theorem 6.4], there is an isomorphism $\hat{E}\left(7\mathbb{Z}_7\right)\to\hat{\mathbb{G}}_a\left(7\mathbb{Z}_7\right)$, where $\mathbb{G}_a$ denotes the additive group. By [Sil09, IV.3 and VII.2] there is an exact sequence

$$0\longrightarrow\hat{\mathbb{G}}_a\left(7\mathbb{Z}_7\right)\longrightarrow E(\mathbb{Q}_7)\longrightarrow\tilde{E}\left(\mathbb{F}_7\right)\longrightarrow 0\,.$$

Furthermore, by [Sil09, VII.3 Proposition 3.1] the reduction map ${}_3E(\mathbb{Q}_7) \to \tilde{E}(\mathbb{F}_7)$ is injective. Thus E has k-rational 3-torsion. Since 3 is a unit in $\mathbb{Z}_7$ we further deduce that $E(\mathbb{Q}_7)/[3]E(\mathbb{Q}_7) = \tilde{E}(\mathbb{F})/[3]\tilde{E}(\mathbb{F}) = M$. Finally,

$$\mathbb{Q}_7^\times / \left(\mathbb{Q}_7^\times\right)^3 \cong \left(\mathbb{Z}_7^\times \times (7\mathbb{Z}_7)\right) / \left(\mathbb{Z}_7^\times \times (7\mathbb{Z}_7)\right)^3 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Therefore, $H^1(k, M) \cong \left(\mathbb{Q}_7^\times / \left(\mathbb{Q}_7^\times\right)^3\right)^2 \cong (\mathbb{Z}/3\mathbb{Z})^4$. By the algorithm and using [Gro68b, Corollaire 2.3], the 3-torsion of the Brauer group decomposes as follows

$${}_3\mathrm{Br}(E) \cong {}_3\mathrm{Br}\left(\mathbb{Q}_7\right) \oplus (\mathbb{Z}/3\mathbb{Z})^2 = {}_3(\mathbb{Q}/\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})^2 = (\mathbb{Z}/3\mathbb{Z})^3.$$

Remark 7.5.1. *The above computations also show that* ${}_3\mathrm{Br}\left(\tilde{E}\right) = {}_3\mathrm{Br}\left(\mathbb{F}_7\right) = 0$.

7.6 Over a finite field

Let $k = \mathbb{F}_5(\omega)$ be the extension of the field with five elements given by attaching a third root of unity ω. Let E be the elliptic curve given by the affine equation

$$y^2 = x^3 + 1.$$

The three torsion of $E(\overline{k})$ is also k-rational with generators $P = (0, 4)$ and $Q = (1, 3\omega + 4)$. Furthermore, we use the code in the appendix to calculate that $E(k) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. A direct calculation gives that $(k^\times)^3 = \mathbb{F}_5^\times \cup (1 + 2\omega)\mathbb{F}_5^\times$ Therefore, the quotient $k^\times/(k^\times)^3$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$ with distinct representatives $\{1, \omega, \omega + 1\}$. We conclude that δ is surjective, and therefore ${}_3\mathrm{Br}(E) = {}_3\mathrm{Br}(k)$. Since $\mathbb{F}_5$ is a C_1-field and finite extensions of

C_1-fields are C_1 as well [GS17, Lemma 6.2.4, page 161], we deduce that $\mathrm{Br}(k) = 1$ and ${}_3\mathrm{Br}(E)$ is trivial.

7.7 Degree $[L : k]$ divisible by q

Let $k = \mathbb{Q}(\omega)$, where ω is a primitive third root of unity. Consider the elliptic curve E given by the affine equation

$$y^2 = x^3 + x + 1.$$

The three torsion M of $E(\overline{k})$ is generated by $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ with

$$\begin{aligned}
x_1 =& -\frac{1}{2}\sqrt{\frac{\sqrt[3]{\Delta}-8}{3} - \frac{8\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta}-4}}} + \frac{\sqrt{-\sqrt[3]{\Delta}-4}}{2\sqrt{3}},\\
x_2 =& \frac{1}{2}\sqrt{\frac{\sqrt[3]{\Delta}-8}{3} - \frac{8\sqrt{3}}{\sqrt{-\sqrt[3]{\Delta}-4}}} + \frac{\sqrt{-\sqrt[3]{\Delta}-4}}{2\sqrt{3}},\\
y_1 =& \sqrt{x_1^3 + x_1 + 1},\\
y_2 =& \sqrt{x_2^3 + x_2 + 1}
\end{aligned}$$

where $\Delta = -496$ is the discriminant of E (see [Pal10, Section 3]). Denote $P + Q = (x_3, y_3)$ and $2P + Q = (x_4, y_4)$. By [Pal10, Theorem 4.1 (1)], the field L is $k(x_1, x_2, y_1) = k(x_2 - x_1, y_1)$ and the Galois group of L over k is isomorphic to $SL_2(\mathbb{F}_3)$. Consider the subgroup P generated by $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and denote its fixed field by L'. By the proof of the primitive element theorem, an element $l \in L$ with $l^3 \in L'$ and $L = L'(l)$ is

$$l = x_2 + \omega x_3 + \omega^2 x_4.$$

As we have seen before, n_Q is given by the equation of the line through Q and $P+Q$, that is

$$n_Q = y - y_2 - \frac{y_3 - y_2}{x_3 - x_2}(x - x_2).$$

By the main algorithm we deduce that

$$ {}_3\mathrm{Br}(E) = {}_3\mathrm{Br}(k) \oplus I$$

and every element in I can be written as a tensor product

$$\begin{aligned}\mathrm{cor}_{L'(E)/k(E)} \left(\left(x_2 + \omega x_3 + \omega^2 x_4 \right)^{3j}, y - y_2 - \frac{y_3 - y_2}{x_3 - x_2}(x - x_2) \right)_{L'(E)} \\ \otimes \mathrm{cor}_{L'(E)/k(E)} \left(a, y - y_1 - \frac{3x_1^2 + 1}{2y_1}(x - x_1) \right)_{L'(E)}\end{aligned}$$

for some $a \in L'$ and some $j \in \{0, 1, 2\}$. It remains to calculate $\mathrm{cor}_{L'(E),k(E)}$ of these algebras, which can be computed for specific values of a and j using algorithm 7.2.2. We can therefore write every element in I as a tensor product of at most 16 symbol algebras over $k(E)$.

APPENDIX

Appendix

Magma Code

This appendix contains the magma-code used in chapter 7.

Code for section 7.1

```
K<w> := CyclotomicField(3);

E := EllipticCurve([L|0,16]);

AbelianGroup(E);

Generators(E);
```

Code for section 7.2

This is the code for $B = -1024$:

```
K<w> := CyclotomicField(3);

E := EllipticCurve([L|0,-1024]);

AbelianGroup(E);
```

This is the code for $B = 2$:

```
K<w> := CyclotomicField(3);

E := EllipticCurve([L|0,2]);
```

```
AbelianGroup(E);

Generators(E);
```

Code for section 7.3

We first calculate the k-rational points of E by using:

```
K<w> := CyclotomicField(3);

E := EllipticCurve([L|0,4]);

AbelianGroup(E);

Generators(E);
```

Now we calculate the L-rational points of E with:

```
K<w> := CyclotomicField(3);

R<y> := PolynomialRing(K);

f := y^2-2;

L := ext<K|f>;

E := EllipticCurve([L|0,4]);

Generators(E);
```

Code for section 7.4

```
K<w> := CyclotomicField(3);

E := EllipticCurve([K|0,-48]);

AbelianGroup(E);

Generators(E);
```

```
R<y> := PolynomialRing(K);

f := y^3 - 3;

L := ext<K|f>;

E := EllipticCurve([L|0,-48]);

AbelianGroup(E);

Generators(E);
```

Code for section 7.5

```
F := FiniteField(7);

E := EllipticCurve([F|0,16]);

AbelianGroup(E);

Points(E);
```

Code for section 7.6

```
F := FiniteField(5);

R<w> := PolynomialRing(F);

f := w^2 + w + 1;

L := ext<F|f>;

E := EllipticCurve([L|0,1]);

AbelianGroup(E);

Points(E);
```

BIBLIOGRAPHY

BIBLIOGRAPHY

[AG60] Maurice Auslander and Oscar Goldman. The Brauer group of a commutative ring. *Trans. Amer. Math. Soc.*, 97:367–409, 1960.

[AM72] M. Artin and D. Mumford. Some elementary examples of unirational varieties which are not rational. *Proc. London Math. Soc. (3)*, 25:75–95, 1972.

[BNH32] R. Brauer, E. Noether, and H. Hasse. Beweis eines Hauptsatzes in der Theorie der Algebren. *J. Reine Angew. Math.*, 167:399–404, 1932.

[BP12] Andrea Bandini and Laura Paladino. Number fields generated by the 3-torsion points of an elliptic curve. *Monatsh. Math.*, 168(2):157–181, 2012.

[Bre97] Glen E. Bredon. *Sheaf theory*, volume 170 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.

[CG01] V. Chernousov and V. Guletskiĭ. 2-torsion of the Brauer group of an elliptic curve: generators and relations. In *Proceedings of the Conference on Quadratic Forms and Related Topics (Baton Rouge, LA, 2001)*, pages 85–120, 2001.

[CRR16] Vladimir I. Chernousov, Andrei S. Rapinchuk, and Igor A. Rapinchuk. On the size of the genus of a division algebra. *Tr. Mat. Inst. Steklova*, 292(Algebra, Geometriya i Teoriya Chisel):69–99, 2016. Reprinted in Proc. Steklov Inst. Math. **2**92 (2016), no. 1, 63–93.

[CTS87] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. La descente sur les variétés rationnelles. II. *Duke Math. J.*, 54(2):375–492, 1987.

[CTS07] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. The rationality problem for fields of invariants under linear algebraic groups (with special regards to the Brauer group). In *Algebraic groups and homogeneous spaces*, volume 19 of *Tata Inst. Fund. Res. Stud. Math.*, pages 113–186. Tata Inst. Fund. Res., Mumbai, 2007.

[CV15] Brendan Creutz and Bianca Viray. Two torsion in the Brauer group of a hyperelliptic curve. *Manuscripta Math.*, 147(1-2):139–167, 2015.

[dJ] A.J. de Jong. A result of Gabber. http://www.math.columbia.edu/ dejong/papers/2-gabber.pdf.

[Fad56] D. K. Faddeev. Simple algebras over a field of algebraic functions of one variable. *Amer. Math. Soc. Transl. (2)*, 3:15–38, 1956.

[FSS79] Burton Fein, Murray Schacher, and Jack Sonn. Brauer groups of rational function fields. *Bull. Amer. Math. Soc. (N.S.)*, 1(5):766–768, 1979.

[Gro68a] Alexander Grothendieck. Le groupe de Brauer. II. Théorie cohomologique. In *Dix exposés sur la cohomologie des schémas*, volume 3 of *Adv. Stud. Pure Math.*, pages 67–87. North-Holland, Amsterdam, 1968.

[Gro68b] Alexander Grothendieck. Le groupe de Brauer. III. Exemples et compléments. In *Dix exposés sur la cohomologie des schémas*, volume 3 of *Adv. Stud. Pure Math.*, pages 88–188. North-Holland, Amsterdam, 1968.

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2017. Second edition of [MR2266528].

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[Lan78] Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin-New York, 1978.

[Lic69] Stephen Lichtenbaum. Duality theorems for curves over p-adic fields. *Invent. Math.*, 7:120–136, 1969.

[Man71] Y. I. Manin. Le groupe de Brauer-Grothendieck en géométrie diophantienne. In *Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1*, pages 401–411. Gauthier-Villars, Paris, 1971.

[Mer86] A. S. Merkurjev. K_2 of fields and the Brauer group. In *Applications of algebraic K-theory to algebraic geometry and number theory, Part I, II (Boulder, Colo., 1983)*, volume 55 of *Contemp. Math.*, pages 529–546. Amer. Math. Soc., Providence, RI, 1986.

[Mil80] James S. Milne. *Étale cohomology*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, Princeton, N.J., 1980.

[Mil04] Victor S. Miller. The Weil pairing, and its efficient calculation. *J. Cryptology*, 17(4):235–261, 2004.

[MS82] A. S. Merkurjev and A. A. Suslin. K-cohomology of Severi-Brauer varieties and the norm residue homomorphism. *Izv. Akad. Nauk SSSR Ser. Mat.*, 46(5):1011–1046, 1135–1136, 1982.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*, volume 323 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2008.

[Pal10] Laura Paladino. Elliptic curves with $\mathbb{Q}(\mathcal{E}[3]) = \mathbb{Q}(\zeta_3)$ and counterexamples to local-global divisibility by 9. *J. Théor. Nombres Bordeaux*, 22(1):139–160, 2010.

[Rei03] I. Reiner. *Maximal orders*, volume 28 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, Oxford, 2003. Corrected reprint of the 1975 original, With a foreword by M. J. Taylor.

[RT83] Shmuel Rosset and John Tate. A reciprocity law for K_2-traces. *Comment. Math. Helv.*, 58(1):38–47, 1983.

[Sal99] David J. Saltman. *Lectures on division algebras*, volume 94 of *CBMS Regional Conference Series in Mathematics*. Published by American Mathematical Society, Providence, RI; on behalf of Conference Board of the Mathematical Sciences, Washington, DC, 1999.

[Ser79] Jean-Pierre Serre. *Local fields*, volume 67 of *Graduate Texts in Mathematics*. Springer-Verlag, New York-Berlin, 1979. Translated from the French by Marvin Jay Greenberg.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sko99] Alexei N. Skorobogatov. Beyond the Manin obstruction. *Invent. Math.*, 135(2):399–424, 1999.

[Sko01] Alexei Skorobogatov. *Torsors and rational points*, volume 144 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 2001.

[Sta19] The Stacks Project Authors. *Stacks Project*. https://stacks.math.columbia.edu, 2019.

[Wei94] Charles A. Weibel. *An introduction to homological algebra*, volume 38 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1994.