2-Torsion of the Brauer Group of an Elliptic Curve: Generators and Relations

V. Chernousov, V. Guletskiĭ

Received: May 1, 2001

Communicated by Ulf Rehmann

Abstract. In this paper we describe the 2-torsion part of the Brauer group $\operatorname{Br} E$ of an elliptic curve E defined over an arbitrary field of characteristic $\neq 2$ in terms of generators and relations.

2000 Mathematics Subject Classification: 14H52, 16H05, 16K20
Keywords and Phrases: Elliptic curves, Brauer groups.

1 *Introduction*

Let E be an elliptic curve defined over a field K of characteristic different from 2 and given by an affine equation

$$y^2 = f(x),$$

where $f(x)$ is a unitary cubic polynomial over K without multiple roots. We will say that E is *split*, *semisplit* or *non-split* if $f(x)$ has 3, 1 or no roots in K respectively.

Let $\operatorname{Br} E$ be the Brauer group of the curve E. The group $\operatorname{Br} E$ plays an important role in arithmetic and algebraic geometry. For example, it can be used to study arithmetical properties of elliptic surfaces and some other algebraic varieties (cf. [AM72], [CEP71], [CSS98], [S99]). Another important application is the construction of unirational varieties which are not rational. Let us describe the last point in some more details. We follow the famous paper of Artin and Mumford [AM72] slightly modifying their examples.

Let S be a smooth projective surface defined over an algebraically closed field of characteristic $\neq 2$, say $\mathbb{C}$ for simplicity. Assume that S is a rational elliptic

surface defined by a regular map $\pi : S \to \mathbb{P}^1$ such that the generic fiber $E_\xi = \pi^{-1}(\xi)$ is an elliptic curve.
Given a quaternion algebra $D = (d_1, d_2)$ over the function field $L = \mathbb{C}(S)$ of the surface S, whose ramification curve has nonsingular components, one can associate a smooth S-scheme $\phi : V_D \to S$ in a natural way, all of whose geometric fibres are isomorphic to $\mathbb{P}^1$ or to $\mathbb{P}^1 \vee \mathbb{P}^1$ (the so-called Brauer-Severi scheme). Let C be the ramification curve of D and let $C = C_1 \cup \ldots \cup C_n$ be its decomposition into irreducible components. The remarkable thing about V_D is that V_D viewed as a variety over $\mathbb{C}$ is not rational if all components $C_1, \ldots, C_n$ are disjoint. Namely, Artin and Mumford [AM72] proved that under these conditions V_D has 2-torsion in $H^3(V_D, \mathbb{Z})$. Since the torsion in H^3 is a birational invariant for complete smooth 3-dimensional varieties, V_D is not rational.
On the other hand, it turns out that for many quaternion algebras D the variety V_D is unirational. To prove it we first remark that if we want to have the ramification curve C of D with disjoint irreducible components it is natural to take D such that C has vertical components (with respect to π) only. It easily follows that all candidates for such D are among quaternion algebras in the Brauer group of the generic fiber E_ξ. As we show in this paper, there are lots of non-trivial quaternion algebras in $\operatorname{Br} E_\xi$. Taking the appropriate D we may assume that C has ≥ 2 irreducible components. As it was said, this implies that the corresponding V_D is not rational.
Now let η be a generic point of S. Then $V_\eta = \phi^{-1}(\eta)$ is a conic over $\mathbb{C}(\eta) = \mathbb{C}(S) = L$. Consider the extension F/L of degree 4 corresponding to the Kummer map $E_\xi \overset{2}{\to} E_\xi$. It kills D, hence the conic V_η has an F-point. In particular V_η is rational over F, i.e. the function field $F(V_\eta)$ is isomorphic to $F(z)$ over F, where z is a transcendental variable over F. Furthermore, since F/L corresponds to the Kummer map, we have $F \overset{\mathbb{C}(t)}{\simeq} \mathbb{C}(t)(E_\xi)$, hence

$$F(V_\eta) \overset{F}{\simeq} F(z) \overset{\mathbb{C}(t)}{\simeq} \mathbb{C}(t)(E_\xi)(z) = \mathbb{C}(S)(z)$$

is a purely transcendental extension of $\mathbb{C}$. Here we used the fact that S is a rational surface. Finally, since $\mathbb{C}(V_D) = L(V_\eta)$ is a subfield of $F(V_\eta)$, V_D viewed as a 3-fold variety over $\mathbb{C}$ is unirational.

Our construction shows that if we want to produce an explicit example of an unirational variety which is not rational, one needs to know the structure of 2-torsion of $\operatorname{Br} E_\xi$. So it makes sense to get an explicit description of 2-torsion ${}_2\operatorname{Br} E$ of the Brauer group of an elliptic curve E defined over an arbitrary field K. One of the main goals of this paper is to accomplish (to some extent) a description of ${}_2\operatorname{Br} E$ in terms of generators and relations. The initial results in this direction were obtained in [Pu98] where a description of quaternion algebras over E is presented and in [GMY97] where an explicit description of generators of ${}_2\operatorname{Br} E$ for a split elliptic curve is given. The second-named author [G99] generalized the results of [GMY97] for semisplit elliptic curves. Our paper, in fact, grew out of his preprint [G99] and here we go further and

obtain more complete results that concern generators as well as relations for arbitrary elliptic curves. Our arguments are elementary and based only on using standard properties of restriction and corestriction maps for H^1 with coefficients in certain finite modules.
After this paper was released as a preprint [CG00] we learnt of the nice paper [S99] of Skorobogatov where he gave, among other things, a description of generators of the Brauer groups of algebraic varieties X defined over a field K of characteristic 0 satisfying the condition $H^0(\overline{K}, G_m) = \overline{K}[X]^\times = \overline{K}^\times$ where $\overline{K}$ is an algebraical closure of K. In that paper the generators of $\mathrm{Br}\, X$ are given in the form of the cup product of certain torsors over X and cocycles in H^1 with coefficients in finitely generated submodules of $\mathrm{Pic}\,(\overline{X})$. The proofs in [S99] are based on the heavy machinery of homological algebra. However, it seems worth while to have elementary constructions and proofs for elliptic curves as well.

We proceed to describe our results. Let $\overline{K}$ be a separable closure of K and $\overline{E} = E(\overline{K})$. The starting point of our consideration is the following exact sequence:

$$0 \to \mathrm{Br}\, K \longrightarrow \mathrm{Br}\, E \xrightarrow{\kappa} H^1(K, \overline{E}) \to 0 \,. \tag{1}$$

Since $E(K) \neq \emptyset$, the homomorphism κ has a section, so that (1) induces the exact sequence

$$0 \to {}_2\mathrm{Br}\, K \longrightarrow {}_2\mathrm{Br}\, E \xrightarrow{\kappa} {}_2H^1(K, \overline{E}) \to 0 \,,$$

where the subscript 2 means the 2-torsion part.
The main result of the paper is formulated in Theorems 3.6, 4.12, 5.2 and 5.3. After some preliminaries given in Section 2 we construct a section for κ in an explicit form. This eventually enables us to give an explicit description of ${}_2\mathrm{Br}\, E$ in terms of generators and relations.
More exactly, let M be the 2-torsion part of $\overline{E}$ and let $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$. The Kummer sequence

$$0 \to M \longrightarrow \overline{E} \xrightarrow{2} \overline{E} \to 0,$$

where the symbol 2 over the arrow means multiplication by 2, yields the exact sequence

$$0 \to E(K)/2 \xrightarrow{\delta} H^1(\Gamma, M) \xrightarrow{\zeta} {}_2H^1(\Gamma, \overline{E}) \to 0 \,.$$

Here $\delta : E(K)/2 \hookrightarrow H^1(\Gamma, M)$ is a connecting homomorphism. In Sections 3 through 5 we show that there exists a homomorphism $\epsilon : H^1(\Gamma, M) \to {}_2\mathrm{Br}\, E$ with the properties

$$\kappa \circ \epsilon = \zeta, \qquad \epsilon\,(\ker(\zeta)) = 0. \tag{2}$$

The second property implies that ϵ factors through ${}_2H^1(\Gamma, \overline{E})$, i.e. there is a unique homomorphism $\varepsilon : {}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\, E$ such that $\varepsilon \circ \zeta = \epsilon$, and the first one shows that ε is a required section.

If $f(x) = (x-a)(x-b)(x-c)$ with a, b, $c \in K$, then $M \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$; hence

$$H^1(\Gamma, M) \simeq K^*/(K^*)^2 \times K^*/(K^*)^2.$$

It turns out that the map

$$\epsilon : \; K^*/(K^*)^2 \times K^*/(K^*)^2 \to {}_2\mathrm{Br}\, E$$

which takes a pair $(r, s) \in K^* \times K^*$ into the product $(r, x-b) \otimes (s, x-c)$ of quaternion algebras over $K(E)$ satisfies (2). Thus letting $I = \mathrm{Im}\, \epsilon$, we obtain the natural isomorphism ${}_2\mathrm{Br}\, E \simeq {}_2\mathrm{Br}\, K \oplus I$ where, by construction, the second summand I is generated by quaternion algebras over $K(E)$ of the form $(r, x-b)$ and $(s, x-c)$ with $r, s \in K^*$.
Assume that $f(x)$ does not split over K. We denote the minimal extension of K over which a section ϵ is already constructed by L. Then using standard properties of restriction and corestriction maps we show that for a special map $\tau : H^1(K, M) \to H^1(L, M)$ the composition $\epsilon = \mathrm{cor} \circ \epsilon_L \circ \tau$ satisfies (2). As a corollary of our construction, we again obtain the decomposition

$$ {}_2\mathrm{Br}\, E \simeq {}_2\mathrm{Br}\, K \oplus \mathrm{cor}\ (\mathrm{Im}\, \epsilon_L)\,. \tag{3}$$

Note that in all cases the degree of L/K is either two or three. This fact enables us to present generators of the second summand in (3) in an explicit form. It turns out that all of them are tensor products of quaternion algebras over $K(E)$ of a very specific form.
It follows from the construction that all relations between our generators are given by algebras from $(\epsilon \circ \delta)(E(K)/2)$. These algebras are also presented in an explicit form in Theorems 3.6, 4.12, 5.2 and 5.3 and all of them are parametrized by K-points of the elliptic curve E. This result shows that the two problems of an explicit description of the 2-torsion part of $\mathrm{Br}\, E$ (of course, modulo *numerical algebras*, i.e. algebras from ${}_2\mathrm{Br}\, K$) and the group $E(K)/2$ are, in fact, equivalent. So, every time information about $E(K)/2$ is available we can effectively describe ${}_2\mathrm{Br}\, E$ and vice versa.
In the second part of the paper we apply our results to the computation of ${}_2\mathrm{Br}\, E$ for an elliptic curve E over a local non-dyadic field K. In this case the structure of the group $E(K)$ is well understood. Applying known results we easily construct generators of $E(K)/2$ in Sections 7 and 8. This, in turn, yields an explicit description of ${}_2\mathrm{Br}\, E$ in the concluding Sections 8 and 9 very quickly. Thus, we reopen a result of Margolin and Yanchevskii [YM96]. It seems that in this part our argument is more natural and shorter (cp. loc. cit.).
Finally, we remark that by repeating almost verbatim our argument one can describe in a similar way the 2-torsion part of $\mathrm{Br}\, X$ for a hyperelliptic curve X defined over a field K such that $X(K) \neq \emptyset$. However, in order to keep the volume reasonable we do not consider hyperelliptic curves in the present paper.

If A is an abelian group, $A \xrightarrow{2} A$ denotes the homomorphism of multiplication by 2 and ${}_2A$, $A/2$ are its kernel and cokernel respectively.

$|S|$ denotes the number of elements in a finite set S.
Throughout this paper all fields under consideration are of characteristic $\neq 2$. For a field K denote by $\overline{K}$ a separable closure of K, K^* its multiplicative group and K^{*2} the subgroup of squares. By abuse of language, we will write s for a coset sK^{*2}, whenever there is no danger of confusion.
A variety is always a smooth projective and geometrically integral scheme over a field K. For a variety X over K, we write $K(X)$ for the function field of X and $X(K)$ for the set of its K-points. If L/K is a field extension, we put $X_L = X \times_{Spec\,K} Spec\,L$. We also write $\overline{X} = X \times_{Spec\,K} Spec\,\overline{K}$ and for brevity $\overline{K}$-points of $\overline{X}$ will be denoted by the same symbol $\overline{X}$.
In the paper we will consider quaternion algebras and their tensor products only. If A is a central simple algebra over a field K then $[A]$ means its class in the Brauer group $\operatorname{Br} K$. If $a, b \in K^*$ and (a, b) is a quaternion algebra, then, for short, we write $[a, b]$ instead of $[(a, b)]$. The group law in a Brauer group we always write additively: if $a, b, c, d \in F^*$, then $[(a, b) \otimes (c, d)] = [a, b] + [c, d]$.
If Γ is a profinite group, then $H^*(\Gamma, -)$ is a Galois cohomology functor. Let Λ be a subgroup of finite index in Γ. Then $\operatorname{res} : H^*(\Gamma, -) \to H^*(\Lambda, -)$ and $\operatorname{cor} : H^*(\Lambda, -) \to H^*(\Gamma, -)$ are the restriction and corestriction homomorphisms respectively. In particular, if $\Gamma = \operatorname{Gal}(\overline{K}/K)$ and Λ corresponds to a finite exension F/K then (using the cohomological description of Brauer groups) we have the homomorphism of a scalar extension $\operatorname{Br} K \to \operatorname{Br} F$ and the corestriction homomorphism $\operatorname{cor}_{F/K} : \operatorname{Br} F \to \operatorname{Br} K$. Thus, $\operatorname{cor}_{F/K}[A]$ means the value of the homomorphism $\operatorname{cor}_{F/K}$ on the class $[A] \in \operatorname{Br} F$.
If E is an elliptic curve over K, then its Brauer group is naturally isomorphic to the unramified Brauer group $\operatorname{Br}_{nr}(K(E)/K)$ (see [Lich69], [Co88]). So we will always identify $\operatorname{Br} E$ with $\operatorname{Br}_{nr}(K(E)/K)$.

Acknowledgements. The authors gratefully acknowledge the support of SFB 343 "Diskrete Strukturen in der Mathematik", TMR ERB FMRX CT-97-0107 and the hospitality of the University of Bielefeld. We would like also to express our thanks to H. Abels and U. Rehmann for support and encouragement during the preparation of this paper and O. Izhboldin for useful discussions.

2 *Preliminaries*

Let E be an elliptic curve over a field K defined by an affine equation

$$y^2 = f(x),$$

where $f(x)$ is a unitary cubic polynomial over K without multiple roots. Let O be the infinite point on E. On the set of K-points $E(K)$ there is a natural structure of an abelian group, such that O is a zero element. Throughout the paper we denote the 2-torsion subgroup in $\overline{E}$ by M. Let $\Gamma = \operatorname{Gal}(\overline{K}/K)$ be the absolute Galois group of the ground field K. If

$$f(x) = (x - a)(x - b)(x - c)$$

is the decomposition of $f(x)$ over $\overline{K}$, then

$$M = \{\, O,\ (a,0),\ (b,0)\,(c,0)\,\}.$$

We say that E is *split* if $a,b,c \in K$. In this case $M \subset E(K)$; hence M is a trivial Γ-module. We say that E is *semisplit* if $f(x)$ has one root in K only. If $f(x)$ is irreducible over K, then we say that E is *non-split*.

A starting point of our explicit description of ${}_2\mathrm{Br}\,E$ is the following exact sequence:

$$0 \to \mathrm{Br}\,K \xrightarrow{\iota} \mathrm{Br}\,E \xrightarrow{\kappa} H^1(\Gamma,\overline{E}) \to 0\,. \tag{4}$$

Here the maps ι and κ are defined as follows (see details in [Fadd51], [Lich69], [Mi81] or [Sch69]). Recall that we identify $\mathrm{Br}\,E$ with the unramified Brauer group $\mathrm{Br}_{nr}(K(E)/K)$. Then ι is induced by the scalar extension functor: if A is a central simple algebra over K, then $\iota([A]) = [A \otimes_K K(E)]$.

Next let $h \in \mathrm{Br}\,E$. By Tsen's theorem (see [P82]), we have $\mathrm{Br}\,K(E) \cong H^2(\Gamma,\overline{K}(E)^*)$. Hence h can be viewed as an element in $H^2(\Gamma,\overline{K}(E)^*)$. Let $\mathrm{Div}\,\overline{E}$ be the group of divisors on $\overline{E}$ and let $\mathrm{P}\,(\overline{E})$ be the group of principal divisors on $\overline{E}$. Let h' be the image of h under the homomorphism

$$H^2(\Gamma,\overline{K}(E)^*) \longrightarrow H^2(\Gamma,\mathrm{P}\,(\overline{E}))$$

induced by the map $\overline{K}(E)^* \to \mathrm{P}\,(\overline{E})$ that takes a rational function f to its divisor $\mathrm{div}(f)$. Since h belongs to the unramified subgroup of $\mathrm{Br}\,K(E) \cong H^2(\Gamma,\overline{K}(E)^*)$, it follows that h' lies in the kernel of the homomorphism

$$H^2(\Gamma,\mathrm{P}\,(\overline{E})) \longrightarrow H^2(\Gamma,\mathrm{Div}(\overline{E})) \tag{5}$$

induced by the embedding $\mathrm{P}\,(\overline{E}) \to \mathrm{Div}(\overline{E})$.

Let $\mathrm{Div}^0(\overline{E})$ be the group of degree zero divisors on $\overline{E}$. Clearly, $H^1(\Gamma,\mathbb{Z}) = 0$, so that a natural homomorphism $H^2(\Gamma,\mathrm{Div}^0(\overline{E})) \to H^2(\Gamma,\mathrm{Div}(\overline{E}))$ is injective. Therefore, the kernel of (5) coincides with the kernel of

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

and the last one coincides with the image of the connecting homomorphism

$$\partial : H^1(\Gamma,\overline{E}) \longrightarrow H^2(\Gamma,\mathrm{P}\,(\overline{E}))$$

induced by the exact sequence

$$0 \to \mathrm{P}\,(\overline{E}) \longrightarrow \mathrm{Div}^0(\overline{E}) \longrightarrow \overline{E} \to 0\,.$$

Since $E(K) \neq \emptyset$ and $H^1(\Gamma,\mathbb{Z}) = 0$, we easily get

$$H^1(\Gamma,\mathrm{Div}^0(\overline{E})) = H^1(\Gamma,\mathrm{Div}(\overline{E})) = 1,$$

so that ∂ is injective. It follows that there exists a unique element $h'' \in H^1(\Gamma,\overline{E})$ such that $\partial(h'') = h'$. Then, by definition, $\kappa(h) = h''$.

We claim that sequence (4) splits. Indeed, if $x \in E(K)$ and $K(E)_x$ is the completion of $K(E)$ at x, then $\mathrm{Br}\,K(E)_x \cong \mathrm{Br}\,K \oplus \mathrm{Hom}_{cont}(\Gamma, \mathbb{Q}/\mathbb{Z})$. Let

$$\varsigma : \mathrm{Br}\,E \longrightarrow \mathrm{Br}\,K$$

be the composition

$$\mathrm{Br}\,E \hookrightarrow \mathrm{Br}\,K(E) \to \mathrm{Br}\,K(E)_x \cong \mathrm{Br}\,K \oplus \mathrm{Hom}_{cont}(\Gamma, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Br}\,K$$

where the last homomorphism is the projection on the first summand. It is easy to check that the composition $\varsigma \circ \iota$ is an identical map and the claim follows. In view of splitness, (4) induces the exact sequence

$$0 \to {}_2\mathrm{Br}\,K \xrightarrow{\iota} {}_2\mathrm{Br}\,E \xrightarrow{\kappa} {}_2H^1(\Gamma, \overline{E}) \to 0, \tag{6}$$

which also splits. Since ${}_2H^1(\Gamma, \overline{E})$ can be easily computed, we obtain that for an explicit description of ${}_2\mathrm{Br}\,E$ it suffices to construct a section for κ. To do it, we first consider the Kummer sequence

$$0 \to M \longrightarrow \overline{E} \xrightarrow{2} \overline{E} \to 0. \tag{7}$$

It yields the exact sequence

$$0 \to E(K)/2 \xrightarrow{\delta} H^1(\Gamma, M) \xrightarrow{\zeta} {}_2H^1(\Gamma, \overline{E}) \to 0 \tag{8}$$

where $\delta : E(K)/2 \hookrightarrow H^1(\Gamma, M)$ is a connecting homomorphism. In the next three sections we will construct a homomorphism $\epsilon : H^1(\Gamma, M) \to {}_2\mathrm{Br}\,E$ with the properties

$$\kappa \circ \epsilon = \zeta, \qquad \epsilon\,(\ker(\zeta)) = 0.$$

The second property implies that ϵ induces a unique homomorphism ε : ${}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\,E$ such that $\varepsilon \circ \zeta = \epsilon$. Then it follows that $\kappa \circ \varepsilon \circ \zeta = \kappa \circ \epsilon = \zeta$. Since ζ is surjective, we conclude that $\kappa \circ \varepsilon = 1$, i.e. ε is a required section for κ.

Letting $I = \mathrm{Im}\,\varepsilon$, we have ${}_2\mathrm{Br}\,E \cong I \oplus \mathrm{Im}\,\iota \cong I \oplus {}_2\mathrm{Br}\,K$. As we see in Sections 3, 4 and 5, elements in I are tensor product of quaternion algebras over $K(E)$ of a very specific form. So our construction eventually gives a simple system of generators of ${}_2\mathrm{Br}\,E$ modulo *numerical algebras* (i.e. algebras from $\mathrm{Im}\,\iota$) and according to the construction of the maps ϵ and ε all relations between the generators are given by algebras from $\epsilon(\ker(\zeta))$. Thus, to find all relations explicitly, we first have to describe the subset $\mathrm{Im}\,\delta \subset H^1(\Gamma, M)$ and then apply ϵ to its elements.

Since the structure of the group $H^1(\Gamma, M)$ (and hence the construction of ϵ) depends on splitting properties of the polynomial $f(x)$, to realize our program we consider split, semisplit and non-split cases in the next three sections separately.

3 *Split elliptic case*

Let E be a split elliptic curve. Then M is a trivial Γ-module; hence we have

$$H^1(\Gamma, M) = \mathrm{Hom}\,(\Gamma, M)\ .$$

Fix two non-zero points in M, say $(b,0)$ and $(c,0)$. Considering them as generators of M we have an isomorphism

$$M \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2\ .$$

It induces the isomorphism

$$H^1(\Gamma, M) = \mathrm{Hom}(G, M) \cong K^*/K^{*2} \oplus K^*/K^{*2}\ .$$

Consider a map

$$\epsilon_b : K^*/K^{*2} \longrightarrow {}_2\mathrm{Br}\,E$$

which takes $s \in K^*$ into the class $[s, x-b]$. Here and below, for an element $r \in K$ the polynomial $x - r$ is considered as a rational function on E. Clearly, the quaternion algebra $(s, x-b)$ is unramified and ϵ_b is a homomorphism. Analogously, consider a homomorphism

$$\epsilon_c : K^*/K^{*2} \longrightarrow {}_2\mathrm{Br}\,E$$

which takes $s \in K^*$ into the class $[s, x-c]$. Let now

$$\epsilon = \epsilon_b \oplus \epsilon_c : K^*/K^{*2} \oplus K^*/K^{*2} = \mathrm{Hom}(\Gamma, M) \longrightarrow {}_2\mathrm{Br}\,E\ . \tag{9}$$

Using the description of κ given in Section 2 it is easy to show that $\kappa \circ \epsilon = \zeta$.

Lemma 3.1 $\kappa \circ \epsilon = \zeta$.

Proof. Let P be a non zero point in M. For any $s \in K^* \backslash K^{*2}$ let $\phi_{P,s}$ be a homomorphism from Γ into M, such that $\phi_{P,s}(g) = P$ if $g \notin U_s = \mathrm{Gal}(\overline{K}/K(\sqrt{s}))$ and $\phi_{s,b}(g) = O$ otherwise. The group $H^1(\Gamma, M) = Hom(\Gamma, M)$ is generated by the homomorphisms of type $\phi_{P,s}$. Therefore it is sufficient to show that $(\kappa \circ \epsilon)(\phi_{P,s}) = \zeta(\phi_{P,s})$ for any P and s.

Let $\Phi_{P,s}$ be a homomorphism from Γ into $\mathrm{Div}^0(\overline{E})$, such that $\Phi_{P,s}(g) = (P) - (O)$ if $g \notin U_s$ and $\Phi_{s,b}(g) = 0$ otherwise. Let $d\Phi_{P,s} : \Gamma \times \Gamma \to \mathrm{Div}^0(\overline{E})$ be a codifferential of $\Phi_{P,s}$, that is

$$(d\Phi_{P,s})(g_1, g_2) = g_1\Phi_{P,s}(q_2) - \Phi_{P,s}(g_1 g_2) + \Phi_{P,s}(g_2)$$

for any $g_1, g_2 \in \Gamma$. Then $d\Phi_{P,s}$ takes its values in $\mathrm{P}(E)$ and $\partial(\mathrm{cls}(\phi_{P,s})) = \mathrm{cls}(d\Phi_{P,s})$ where cls denotes a cohomology class of a cocycle. Using the above formula for $d\Phi_{P,s}$ it is easy to compute that $d\Phi_{P,s}(g_1, g_2) = 2(P) - 2(O)$ if g_1 and g_2 lie in $\Gamma \backslash U_s$ and $d\Phi_{P,s}(g_1, g_2) = 0$ otherwise. Let $x(P)$ be the x-coordinate of P and let $\psi_{P,s} : \Gamma \times \Gamma \to \overline{K}(E)^*$ be a map, such that

$\Psi_{P,s}(g_1, g_2) = x - x(P)$ if g_1 and g_2 lie in $\Gamma \backslash U_s$ and $d\Phi_{P,s}(g_1, g_2) = 1$ otherwise. Then we see that the composition of $\Psi_{P,s}$ with the natural homomorphism div : $\overline{K}(E)^* \to \mathrm{P}(\overline{E})$ coincides with the homomorphism $d\Phi_{P,s}$. Therefore $\partial(\mathrm{cls}(\phi_{P,s})) = \eta(\mathrm{cls}(\Psi_{P,s}))$. Since $\Psi_{P,s}$ is a cocycle of the unramified quaternion algebra $(s, x - x(P))$, we see that $\kappa([s, x - x(P)]) = \mathrm{cls}(\phi_{P,s})$. But $[s, x - x(P)]$ is equal to $\epsilon(\phi_{P,s})$. So we have $\kappa(\epsilon(\phi_{P,s})) = \mathrm{cls}(\phi_{P,s}) = \zeta(\phi_{P,s})$. □

According to our plan we also need to make sure that $\epsilon(\mathrm{Im}\, \delta) = 0$. The description of $\mathrm{Im}(\delta)$ in the split case is well known. However for the reader's convenience we describe this image in details.

To ease notation, for a point $(u, v) \in E(K)$ the coset $(u, v) + 2E(K)$ will be denoted by the same symbol (u, v). We start with a simple lemma which gives a formula for dividing a point $(u, v) \in E(K)$ in the group $\overline{E}$ by 2. Let

$$r = \sqrt{u-a}\ , \quad s = \sqrt{u-b}\ , \quad t = \sqrt{u-c} \quad \text{and} \quad w = r + s - t\ .$$

Let also

$$p = \frac{1}{2}(w^2 - (r^2 + s^2 + t^2)) + u = rs - rt - st + u \quad \text{and} \quad q = w(p - u) + v\ .$$

LEMMA 3.2 *We have $(p, q) \in \overline{E}$ and $2(p, q) = (u, v)$.*

Proof. This is a straightforward calculation (see also the proof of Theorem 4.1 on page 38 in [Hu87]) and we omit the details to the reader. □

PROPOSITION 3.3 *Let $(u, v) \in E(K)$. Then*

$$\delta(u, v) = \begin{cases} (u - c, u - b) & \text{if } u \neq b \text{ and } u \neq c, \\ (b - c, (b - c)(b - a)) & \text{if } u = b, \\ ((c - a)(c - b), c - b) & \text{if } u = c, \\ (1, 1) & \text{if } u = \infty. \end{cases}$$

Proof. If $u = b$, then $u \neq a$ and $u \neq c$ and, analogously, if $u = c$, then $u \neq a$ and $u \neq b$. Therefore, by the symmetry argument, it suffices to prove the statement in the case $u \neq b$ and $u \neq c$. Moreover, we consider only "a generic case" where $u - b$ and $u - c$ generate a subgroup in K^*/K^{*2} of order 4, i.e. $u - b$ and $u - c$ are nontrivial and different modulo squares. The other cases can be handled in a similar way.

We keep the notation of Lemma 3.2. Since $2(p, q) = (u, v)$, the cocycle $\delta(u, v)$ corresponds to the homomorphism $\phi_{(u,v)} : \Gamma \to M$ that takes γ to the point $(p, q)^\gamma - (p, q)$. Let $U = \mathrm{Gal}(\overline{K}/K(s))$ and $V = \mathrm{Gal}(\overline{K}/K(t))$. We fix arbitrary automorphisms

$$\sigma \in U \backslash V \quad \text{and} \quad \tau \in V \backslash U\ .$$

Let $\psi_{(u,v)} \in \mathrm{Hom}\,(\Gamma, M)$ be the homomorphism corresponding to the pair $(u - c, u - b)$. Clearly, $\phi_{(u,v)}(\gamma) = \psi_{(u,v)}(\gamma) = 0$ for all $\gamma \in \mathrm{Gal}(\overline{K}/K(s, t))$

and $\psi_{(u,v)}(\sigma) = b$, $\psi_{(u,v)}(\tau) = c$. So it suffices to show that the abscissas of the points $(p,q)^\sigma - (p,q)$ and $(p,q)^\tau - (p,q)$ are b and c respectively.
Note that, by construction, we have

$$\sigma(r) = -r\ , \quad \sigma(s) = s \quad \text{and} \quad \sigma(t) = -t\ .$$

Then it easily follows that $(p,q)^\sigma \neq \pm(p,q)$. Denoting by m the abscissa of the point $(p,q)^\sigma - (p,q)$ and taking into account the group law algorithm given on p. 58 in [Sil85], we have

$$\begin{aligned} m &= \left(\tfrac{q+\sigma(q)}{\sigma(p)-p}\right)^2 + a + b + c - \sigma(p) - p \\ &= \left(\tfrac{q+\sigma(q)}{\sigma(p)-p}\right)^2 + 3u - r^2 - s^2 - t^2 - \sigma(p) - p\ . \end{aligned}$$

Since $q = w(p-u) + v$ and $p = rs - rt - st + u$, we can write

$$\begin{aligned} q + \sigma(q) &= w(p-u) + v + \sigma(w)\sigma(p-u) + v \\ &= w(p-u) + \sigma(w)\sigma(p-u) + 2v \\ &= (r+s-t)(rs-rt-st) + (-r+s+t)(-rs-rt+st) + 2rst \\ &= 2r^2s - 4rst + 2st^2 \\ &= 2s(r-t)^2\ , \end{aligned}$$

and

$$\sigma(p) - p = -rs - rt + st - rs + rt + st = 2s(t-r)\ .$$

Thus, we obtain

$$\begin{aligned} m &= \left(\tfrac{(2s(r-t)^2}{2s(t-r)}\right)^2 + 3u - r^2 - s^2 - t^2 + 2rt - 2u \\ &= -s^2 + u \\ &= b\ . \end{aligned}$$

The equality $(p,q)^\tau - (p,q) = (c,0)$ is proved in exactly the same fashion. □

Proposition 3.4 *$\epsilon(\operatorname{Im}\delta) = 0$.*

Proof. Let $(u,v) \in E(K)$. Since $\kappa \circ \epsilon = \zeta$, we have $(\kappa \circ \epsilon)(\delta(u,v)) = 0$, i.e. the algebra $\epsilon(\delta(u,v))$ is numerical. We claim that this algebra is trivial. Indeed, we may assume that (u,v) is a point in $E(K)$ such that $u-b \neq 0$ and $u-c \neq 0$. Then the evaluation of the algebra

$$\epsilon(\delta(u,v)) = [u-c, x-b] + [u-b, x-c]$$

at the point (u,v) yields

$$[u-c, u-b] + [u-b, u-c] = 2[u-c, u-b] = 0\ .$$

This implies that the algebra $\epsilon(\delta(u,v))$ is itself trivial, as required. □

Summarizing the above results, we obtain the following

Proposition 3.5 *Let E/K be a split elliptic curve over K, char $K \neq 2$. Let $\kappa : {}_2\mathrm{Br}\, E \to {}_2H^1(\Gamma, \overline{E})$ be the homomorphism described in Section 2 and let $\zeta : H^1(\Gamma, M) \to {}_2H^1(\Gamma, \overline{E})$ be the homomorphism induced by the embedding $M \subset \overline{E}$. Let also*

$$\epsilon : H^1(\Gamma, M) \longrightarrow {}_2\mathrm{Br}\, E$$

be the homomorphism defined by (9). Then

(i) $\kappa \circ \epsilon = \zeta$.

(ii) *There exists a unique homomorphism*

$$\varepsilon : {}_2H^1(\Gamma, \overline{E}) \longrightarrow {}_2\mathrm{Br}\, E$$

such that $\varepsilon \circ \zeta = \epsilon$ and $\kappa \circ \varepsilon = 1_{{}_2H^1(\Gamma, \overline{E})}$ is an identical map.

Proof. The equality $\kappa \circ \epsilon = \zeta$ is proved in Lemma 3.1. Since ζ is the cokernel of the homomorphism δ and, by Proposition 3.4, $\epsilon(\mathrm{Im}\, \delta) = 0$, there exists a unique homomorphism $\varepsilon : {}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\, E$, such that $\varepsilon \circ \zeta = \epsilon$. Since $\kappa \circ \varepsilon \circ \zeta = \kappa \circ \epsilon = \zeta$, we obtain that $\kappa \circ \varepsilon = 1_{{}_2H^1(\Gamma, \overline{E})}$ because ζ is an epimorphism. □

Reformulating the results of Proposition 3.5 in terms of central simple algebras and using Proposition 3.3, we obtain

Theorem 3.6 *Let E/K be a split elliptic curve defined by an affine equation*

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

where $a, b, c \in K$ and char $K \neq 2$. Let $\epsilon : {}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\, E$ be the section for the homomorphism $\kappa : {}_2\mathrm{Br}\, E \to {}_2H^1(\Gamma, \overline{E})$ constructed in Proposition 3.5 and let $I = \mathrm{Im}\, \varepsilon$. Then

$${}_2\mathrm{Br}\, E = {}_2\mathrm{Br}\, K \oplus I$$

and every element in I is represented by a biquaternion algebra

$$(r, x-b) \otimes (s, x-c)$$

with $r, s \in K^*$. Conversely, every algebra of such a type is unramified over E. An algebra $A = (r, x-b) \otimes (s, x-c)$ is trivial in $I = \mathrm{Im}\,(\varepsilon)$ if and only if A is similar to an algebra of one of the three following types:

(i) *an algebra*

$$(u-c, x-b) \otimes (u-b, x-c),$$

where u is the abscissa of a point in $E(K)$ such that $u - b \neq 0$ and $u - c \neq 0$;

(ii) *an algebra*

$$(b-c, x-b) \otimes ((b-c)(b-a), x-c) \ ;$$

(iii) *an algebra*

$$((c-a)(c-b), x-b) \otimes (c-b, x-c) \ .$$

4 *Semisplit elliptic case*

Let E be a semisplit elliptic curve given by an affine equation

$$y^2 = (x - w)(x^2 - d),$$

where $w, d \in K$, $char\, K \neq 2$ and d is not a square in K^*. Let $L = K(\sqrt{d})$, $\Gamma = \mathrm{Gal}\,(\overline{K}/K)$ and $\Lambda = \mathrm{Gal}\,(\overline{K}/L)$. Clearly, Λ is a subgroup of index two in Γ and

$$M \cong M_{\Gamma}^{\Lambda}(\mathbb{Z}/2),$$

where $M_{\Gamma}^{\Lambda}(\mathbb{Z}/2)$ is an induced Γ-module. Therefore, by Shapiro's lemma (see, for example, [Serre64]), we have

$$H^1(\Gamma, M) = H^1(\Gamma, M_{\Gamma}^{\Lambda}(\mathbb{Z}/2)) \cong H^1(\Lambda, \mathbb{Z}/2) \cong L^*/L^{*2} .$$

Let us consider the split elliptic curve $E_L = E \times_K L$ over L. Fixing its points $(b, 0)$, $(c, 0)$, where $b = \sqrt{d}$, $c = -\sqrt{d}$, we get the isomorphisms over L

$$M \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2, \qquad H^1(\Lambda, M) \cong L^*/L^{*2} \oplus L^*/L^{*2} .$$

Under these identifications the restriction map is given by the formula

$$\mathrm{res} : H^1(\Gamma, M) \to H^1(\Lambda, M), \quad l \in L^*/L^{*2} \to (l^{\sigma}, l) \in L^*/L^{*2} \oplus L^*/L^{*2} \quad (10)$$

where σ is the nontrivial automorphism L/K.
We denote the homomorphisms constructed in the previous section for the split curve E_L by the same symbols but equipped with the subscript L. Thus, we have the homomorphisms

$$\epsilon_L : H^1(\Lambda, M) \longrightarrow {}_2\mathrm{Br}\,(E_L) ,$$

$$\zeta_L : H^1(\Lambda, M) \longrightarrow {}_2H^1(\Lambda, \overline{E})$$

and

$$\varepsilon_L : {}_2H^1(\Lambda, \overline{E}) \longrightarrow {}_2\mathrm{Br}\,(E_L) .$$

Let

$$H^1(\Gamma, M) \cong L^*/L^{*2} \xrightarrow{\tau} L^*/L^{*2} \oplus L^*/L^{*2} \cong H^1(\Lambda, M)$$

be the homomorphism which takes l into the pair $(1, l)$. We define the homomorphism

$$\epsilon : H^1(\Gamma, M) \longrightarrow {}_2\mathrm{Br}\, E$$

by means of the following commutative diagram

$$\begin{array}{ccc} H^1(\Lambda, M) & \xrightarrow{\epsilon_L} & {}_2\mathrm{Br}\,(E_L) \\ \uparrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \mathrm{cor}} \\ H^1(\Gamma, M) & \xrightarrow{\epsilon} & {}_2\mathrm{Br}\, E \end{array}$$

Proposition 4.1 *Let E/K be a semisplit elliptic curve. Let $\zeta : H^1(\Gamma, M) \to {}_2H^1(\Gamma, \overline{E})$ be the homomorphism induced by the embedding $M \subset \overline{E}$ and let ϵ be the above homomorphism. Then there exists a homomorphism*

$$\varepsilon : {}_2H^1(\Gamma, \overline{E}) \longrightarrow {}_2\mathrm{Br}\, E$$

such that $\kappa \circ \varepsilon = 1_{{}_2H^1(\Gamma,\overline{E})}$ (i.e. ε is a section for the homomorphism κ) and $\varepsilon \circ \zeta = \epsilon$.

Proof. The proof is based on a diagram chase. We divide it into a sequence of simple observations.

Lemma 4.2 *The restriction homomorphism*

$$H^1(\Gamma, M) \xrightarrow{\mathrm{res}} H^1(\Lambda, M)$$

is injective.

Proof. This easily follows from (10). □

Lemma 4.3 *The composition*

$$H^1(\Gamma, M) \xrightarrow{\tau} H^1(\Lambda, M) \xrightarrow{\mathrm{cor}} H^1(\Gamma, M)$$

coincides with the identical map $1_{H^1(\Gamma,M)}$.

Proof. By Lemma 4.2, the homomorphism res : $H^1(\Gamma, M) \to H^1(\Lambda, M)$ is injective. Therefore, it is sufficient to prove that $\mathrm{res} \circ \mathrm{cor} \circ \tau = \mathrm{res}$. Let $l \in L^*$. Using (10) we have

$$(\mathrm{res} \circ \mathrm{cor} \circ \tau)(l) = (\mathrm{res} \circ \mathrm{cor})(1, l) = (1, l) + (1, l)^\sigma =$$
$$(1, l) + (l^\sigma, 1) = (l^\sigma, l) = \mathrm{res}(l) \ .$$

□

Lemma 4.4 $\kappa \circ \epsilon = \zeta$.

Proof. The commutative diagram

$$\begin{array}{ccccc}
H^1(\Lambda, M) & \xrightarrow{\zeta_L} & {}_2H^1(\Lambda, \overline{E}) & \xleftarrow{\kappa_L} & {}_2\mathrm{Br}\,(E_L) \\
\downarrow{\scriptstyle \mathrm{cor}} & & \downarrow{\scriptstyle \mathrm{cor}} & & \downarrow{\scriptstyle \mathrm{cor}} \\
H^1(\Gamma, M) & \xrightarrow{\zeta} & {}_2H^1(\Gamma, \overline{E}) & \xleftarrow{\kappa} & {}_2\mathrm{Br}\, E
\end{array}$$

and Lemma 4.3 imply

$$\kappa \circ \epsilon = \kappa \circ \mathrm{cor} \circ \epsilon_L \circ \tau = \mathrm{cor} \circ \kappa_L \circ \varepsilon_L \circ \zeta_L \circ \tau = \mathrm{cor} \circ \zeta_L \circ \tau = \zeta \circ \mathrm{cor} \circ \tau = \zeta \ .$$

□

Lemma 4.5 $\mathrm{cor} \circ \zeta_L \circ \tau = \zeta$.

Proof. Clearly, we have $\mathrm{cor} \circ \zeta_L = \zeta \circ \mathrm{cor}$. Multiplying from the right hand by τ we obtain that $\mathrm{cor} \circ \zeta_L \circ \tau = \zeta \circ \mathrm{cor} \circ \tau = \zeta$ (the last equality holds by Lemma 4.3). □

Lemma 4.6 $\epsilon\,(\mathrm{Im}\,\delta) \subset \mathrm{Im}\,\iota$.

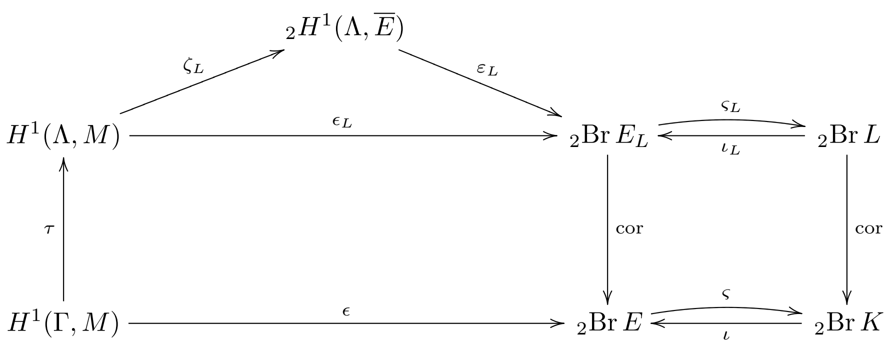
Proof. By Lemma 4.4, we have $\kappa \circ \epsilon = \zeta$, hence

$$\epsilon\,(\mathrm{Im}\,\delta) = \epsilon\,(\ker\,\zeta) \subset \ker\,\kappa = \mathrm{Im}\,\iota\,.$$

□

Lemma 4.7 $\mathrm{Im}\,\epsilon \cap \mathrm{Im}\,\iota = 0$.

Proof. Our computations are illustrated by the following commutative diagram



Let $b \in {}_2\mathrm{Br}\,E$ be such that $b = \epsilon(h) = \iota(a)$ for some $h \in H^1(\Gamma, M)$ and some $a \in {}_2\mathrm{Br}\,K$. Let $c = \zeta_L(\tau(h))$. Then

$$a = (\varsigma \circ \iota)(a) = \varsigma(b) = (\varsigma \circ \mathrm{cor} \circ \varepsilon_L)(c) = (\mathrm{cor} \circ \varsigma_L \circ \varepsilon_L)(c) = 0,$$

because $\varsigma_L \circ \varepsilon_L = 0$. □

Lemma 4.8 $\epsilon\,(\mathrm{Im}\,\delta) = 0$.

Proof. By Lemmas 4.6 and 4.7, we have $\epsilon\,(\mathrm{Im}\,\delta) \subset \mathrm{Im}\,\epsilon \cap \mathrm{Im}\,\iota = 0$. □

We are now in the position to finish the proof of Proposition 4.1. Since $\epsilon\,(\mathrm{Im}\,\delta) = \epsilon\,(\ker\,\zeta) = 0$, it follows that there exists a unique homomorphism $\varepsilon :\, {}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\,E$ such that $\epsilon = \varepsilon \circ \zeta$. Furthermore,

$$\kappa \circ \varepsilon \circ \zeta = \kappa \circ \epsilon = \kappa \circ \mathrm{cor} \circ \epsilon_L \circ \tau = \kappa \circ \mathrm{cor} \circ \varepsilon_L \circ \zeta_L \circ \tau =$$

$$\mathrm{cor} \circ \kappa_L \circ\, \varepsilon_L \circ \zeta_L \circ \tau = \mathrm{cor} \circ \zeta_L \circ \tau = \zeta \circ \mathrm{cor} \circ \tau = \zeta\,.$$

Since ζ is an epimorphism, it follows that $\kappa \circ \varepsilon = 1_{{}_2H^1(\Gamma,\overline{E})}$. Proposition 4.1 is proved. □

To reformulate the results of Proposition 4.1 in terms of central simple algebras we need three well-known lemmas which describe images of quaternion algebras under corestriction homomorphisms.

LEMMA 4.9 *Let F be a field and let P be a finite separable extension of F. Then for elements $a \in F$ and $b \in P$ we have*

$$\operatorname{cor}_{P/F}[a,b] = [a, N_{P/F}(b)]$$

in the Brauer group $\operatorname{Br} F$.

Proof. This is a well-known fact (see, for instance, [Serre79], p. 209). □

LEMMA 4.10 *Let F be a field and let P be a quadratic extension of F. Suppose that $P = F(\sqrt{s})$, where $s \in F$. Then for elements $a, b \in F$ with the property $a + b \neq 0$ we have*

$$\operatorname{cor}_{P/F}[a+\sqrt{s}, b-\sqrt{s}] = [a+b, (a^2-s)(b^2-s)]\ .$$

Proof. Let

$$t = \frac{a+\sqrt{s}}{a+b} \quad \text{and} \quad l = \frac{b-\sqrt{s}}{a+b}\ .$$

Then $t + l = 1$, whence $[t,l] = [t, 1-t] = 0$ in $\operatorname{Br} P$. Substituting t and l, we have

$$0 = [t,l] = \left[\frac{a+\sqrt{s}}{a+b}, \frac{b-\sqrt{s}}{a+b}\right] =$$

$$= [a+\sqrt{s}, b-\sqrt{s}] + [a+b, b-\sqrt{s}] + [a+\sqrt{s}, a+b] + [a+b, a+b].$$

Taking $\operatorname{cor}_{P/F}$ and using Lemma 4.9 we obtain that

$$0 = \operatorname{cor}_{P/F}[a+\sqrt{s}, b-\sqrt{s}] + [a+b, b^2-s] + [a^2-s, a+b] + [a+b, (a+b)^2]\ .$$

Therefore,

$$\operatorname{cor}_{P/F}[a+\sqrt{s}, b-\sqrt{s}] = [a+b, b^2-s] + [a^2-s, a+b]\ .$$

□

LEMMA 4.11 *Let F be a field and let $P = F(\sqrt{s})$ be a quadratic extension of F. Let $u_1, v_1, u_2, v_2 \in F$ be such that $v_1 \neq 0$, $v_2 \neq 0$ and $v_1u_2 \neq u_1v_2$. Then*

$$\operatorname{cor}_{P/F}[u_1 + v_1\sqrt{s}, u_2 + v_2\sqrt{s}] =$$

$$[v_1, u_1^2 - v_1^2 s] + [-v_2, u_2^2 - v_2^2 s] + [v_1u_2 - u_1v_2, (u_1^2 - v_1^2 s)(u_2^2 - v_2^2 s)]\ .$$

Proof. Let
$$a = \frac{u_1}{v_1} \quad \text{and} \quad b = -\frac{u_2}{v_2}\ .$$
Then
$$[u_1 + v_1\sqrt{s}, u_2 + v_2\sqrt{s}] = [v_1(a + \sqrt{s}), -v_2(b - \sqrt{s})] =$$
$$= [v_1, -v_2] + [a + \sqrt{s}, b - \sqrt{s}] + [v_1, b - \sqrt{s}] + [a + \sqrt{s}, -v_2]\ .$$
Lemmas 4.10 and 4.9 give
$$\mathrm{cor}_{D/F}[u_1 + v_1\sqrt{s}, u_2 + v_2\sqrt{s}] =$$
$$[a + b, (a^2 - s)(b^2 - s)] + [v_1, b^2 - s] + [-v_2, a^2 - s]$$
and it remains to substitute $a = u_1/v_1$, $b = -u_2/v_2$. □

Theorem 4.12 *Let E be a semisplit elliptic curve over K, char $K \neq 2$, given by an affine equation $y^2 = (x - w)(x^2 - d)$, where $w, d \in K$ and d is not a square in K. Let $\varepsilon : {}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\, E$ be the section for the homomorphism $\kappa : {}_2\mathrm{Br}\, E \to {}_2H^1(\Gamma, \overline{E})$ constructed in Proposition 4.1 and let $I = \mathrm{Im}\, \varepsilon$. Then*
$${}_2\mathrm{Br}\, E \cong {}_2\mathrm{Br}\, K \oplus I$$
and every element in I is represented by either a quaternion algebra
$$(r, x - w),$$
where $r \in K^*$, or a biquaternion algebra
$$(t, r^2 - t^2 d) \otimes (tx + r, (r^2 - t^2 d)(x^2 - d))$$
where $r, t \in K$ and $t \neq 0$. Conversely, every algebra of the above types is unramified over E. It is trivial in I if and only if it is similar to a quaternion algebra
$$(x + u, (u - w)(x - w)),$$
where u is the abscissa of a point in $E(K)$.

Proof. The first statement is trivial because ε is a section for the homomorphism κ. To prove the second one we have to compute $\epsilon(h)$ in terms of quaternion algebras for all $h \in H^1(\Gamma, M)$.
By definition, $\epsilon = \mathrm{cor} \circ \epsilon_L \circ \tau$, where $L = K(\sqrt{d})$. Recall that we identify $L^*/L^{*2} \cong H^1(\Gamma, M)$ and $L^*/L^{*2} \oplus L^*/L^{*2} \cong H^1(\Lambda, M)$ and that $\tau : L^*/L^{*2} \to L^*/L^{*2} \oplus L^*/L^{*2}$ takes $l \in L^*/L^{*2}$ into $(1, l)$. Let $l \in L^*$. Then we have
$$(\mathrm{cor} \circ \epsilon_L \circ \tau)\,(l) = (\mathrm{cor} \circ \epsilon_L)\,(1, l) = \mathrm{cor}_{L(E)/K(E)}\,[l, x - \sqrt{d}]\ .$$
Let $l = r + t\sqrt{d}$. If $t = 0$, then, by Lemma 4.9, we have
$$\mathrm{cor}_{L(E)/K(E)}\,[r, x - \sqrt{d}] = [r, x^2 - d] = [r, x - w]\ .$$

If $t \neq 0$, then, by Lemma 4.11, we have

$$\mathrm{cor}_{L(E)/K(E)}[r + t\sqrt{d}, x - \sqrt{d}] =$$
$$[t, r^2 - t^2 d] + [1, x^2 - d] + [tx + r, (r^2 - t^2 d)(x^2 - d)] =$$
$$[t, r^2 - t^2 d] + [tx + r, (r^2 - t^2 d)(x^2 - d)]\ .$$

It remains to find out when an algebra $b \in I = \mathrm{Im}\,\epsilon$ is trivial. Let $b = \epsilon\,(l)$. By Proposition 4.1, we have $\epsilon = \varepsilon \circ \zeta$ and $\ker \varepsilon = 0$. So b is trivial if and only if $l \in \ker \zeta = \mathrm{Im}\,\delta$.
Let $(u, v) \in E(K)$ and $l = \delta(u, v)$. The commutative square

$$\begin{array}{ccc} E(L)/2 & \xhookrightarrow{\ \delta_L\ } & L^*/L^{*2} \oplus L^*/L^{*2} \\ \uparrow{\scriptstyle \mathrm{res}} & & \uparrow{\scriptstyle \mathrm{res}} \\ E(K)/2 & \xhookrightarrow{\ \delta\ } & L^*/L^{*2} \end{array}$$

shows that

$$(l^\sigma, l) = \mathrm{res}\,(l) = (\mathrm{res} \circ \delta)(u, v) = (\delta_L \circ \mathrm{res})\,(u, v) = \delta_L(u, v),$$

where σ is a unique nontrivial automorphism L/K. Proposition 3.3 gives

$$\delta_L(u, v) = (u + \sqrt{d}, u - \sqrt{d}).$$

Thus, $l = u - \sqrt{d}$ and finally we get

$$\begin{array}{rcl} (\epsilon \circ \delta)\,(u, v) & = & (\mathrm{cor}_{L/K} \circ \epsilon_L \circ \tau)\,(l) \\ & = & (\mathrm{cor}_{L/K} \circ \epsilon_L)\,(1, l) \\ & = & \mathrm{cor}_{L/K}\,[u - \sqrt{d}, x + \sqrt{d}] \\ & = & [x + u, (u^2 - d)(x^2 - d)] \\ & = & [x + u, (u - w)(x - w)]\ . \end{array}$$

The theorem is proved. □

To consider the non-split case it is convenient to have a reformulation of the last theorem without conditions on the equation of E. Let E be a semisplit elliptic curve given by an affine equation

$$y^2 = (x - a)g(x),$$

where $a \in K$ and $g(x)$ is a unitary irreducible polynomial over K. Denote the roots of $g(x)$ by b and c. Let also E' be a semisplit elliptic curve given by an equation

$$y^2 = (x - w)(x^2 - d),$$

where

$$w = a - \frac{b+c}{2} \quad \text{and} \quad d = \frac{(b-c)^2}{4}\,.$$

Clearly, the map

$$E \longrightarrow E'$$

$$(u, v) \mapsto (u - \frac{b+c}{2}, v)$$

is an isomorphism of elliptic curves. It induces the commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & {}_2\mathrm{Br}\,K & \longrightarrow & {}_2\mathrm{Br}\,E & \xrightarrow{\kappa} & {}_2H^1(\Gamma, \overline{E}) & \longrightarrow & 0 \\
 & & \| & & \uparrow\cong & & \uparrow\cong & & \\
0 & \longrightarrow & {}_2\mathrm{Br}\,K & \longrightarrow & {}_2\mathrm{Br}\,E' & \xrightarrow{\kappa'} & {}_2H^1(\Gamma, \overline{E}') & \longrightarrow & 0
\end{array}$$

Let $\varepsilon' : {}_2H^1(\Gamma, \overline{E}') \to {}_2\mathrm{Br}\,E'$ be the section for the homomorphism $\kappa' : {}_2\mathrm{Br}\,E' \to {}_2H^1(\Gamma, \overline{E}')$ described in Proposition 4.1. Let $\varepsilon : {}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\,E$ be the section for the homomorphism $\kappa : {}_2\mathrm{Br}\,E \to {}_2H^1(\Gamma, \overline{E})$ defined by the following commutative square

$$\begin{array}{ccc}
{}_2\mathrm{Br}\,E & \xleftarrow{\varepsilon} & {}_2H^1(\Gamma, \overline{E}) \\
\uparrow\cong & & \uparrow\cong \\
{}_2\mathrm{Br}\,E' & \xleftarrow{\varepsilon'} & {}_2H^1(\Gamma, \overline{E}')
\end{array}$$

Theorem 4.13 *Let E be a semisplit elliptic curve defined by an equation*

$$y^2 = (x - a)g(x),$$

where $a \in K$, $g(x)$ is a unitary irreducible quadratic polynomial over K and $g(x) = (x - b)(x - c)$ over $\overline{K}$. Let $\varepsilon : {}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\,E$ be the section for the homomorphism $\kappa : {}_2\mathrm{Br}\,E \to {}_2H^1(\Gamma, \overline{E})$ defined above and let $I = \mathrm{Im}\,\varepsilon$. Then

$${}_2\mathrm{Br}\,E \cong {}_2\mathrm{Br}\,K \oplus I$$

and every element in I is represented by either a quaternion algebra of the form

$$(r, x - a),$$

where $r \in K^*$, or a biquaternion algebra of the form

$$(t, r^2 - h^2t^2) \otimes (t(x-h) + r, (r^2 - t^2h^2)g(x)),$$

where $h = (b+c)/2 \in K$, $r, t \in K$ and $t \neq 0$. Conversely, every algebra of the above types is unramified over E. It is trivial in I if and only if it is similar to a quaternion algebra

$$(x - h + u, (u + h - a)(x - a)) ,$$

where u is the abscissa of a point in $E(K)$.

Proof. All statements follow from Theorem 4.12. □

5 *Non-split elliptic case*

In this section we consider a non-split elliptic curve E given by an affine equation

$$y^2 = f(x),$$

where $f(x)$ is an irreducible unitary polynomial without multiple roots. Let a be a root of $f(x)$. We define $L = K(a)$ and $\Theta = \mathrm{Gal}(\overline{K}/L)$.
By construction, the curve $E_L = E \times_K L$ is either split or semisplit over L. Let

$$\zeta_L : H^1(\Theta, M) \longrightarrow {}_2H^1(\Theta, \overline{E})$$

be the homomorphism induced by the embedding $M \subset \overline{E}$ and let

$$\kappa_L : {}_2\mathrm{Br}\, E_L \longrightarrow {}_2H^1(\Theta, \overline{E})$$

be the homomorphism defined either in Section 3 or 4. Let also

$$\epsilon_L : H^1(\Theta, M) \longrightarrow {}_2\mathrm{Br}\, E_L$$

be the homomorphism defined either by formula (9) in the split case or by means of the homomorphism τ in the semisplit case (see Section 4).
According to Propositions 3.5 and 4.1 there exists a section

$$\varepsilon_L : {}_2H^1(\Theta, \overline{E}) \longrightarrow {}_2\mathrm{Br}\, E_L$$

for the homomorphism κ_L, such that the composition $\varepsilon_L \circ \zeta_L$ coincides with ϵ_L. We are now in the position to prove the existence of ϵ and ε with the same properties for the curve E/K in the non-split case.

Proposition 5.1 *Let E be a non-split elliptic curve over K, char $K \neq 2$. Let $\kappa : {}_2\mathrm{Br}\, E \to {}_2H^1(\Gamma, \overline{E})$ be the homomorphism defined in Section 2 and let $\zeta : H^1(\Gamma, M) \to {}_2H^1(\Gamma, \overline{E})$ be the homomorphism induced by the embedding $M \subset \overline{E}$. Let also ϵ be the composition*

$$\epsilon : H^1(\Gamma, M) \xrightarrow{\mathrm{res}} H^1(\Theta, M) \xrightarrow{\epsilon_L} {}_2\mathrm{Br}\, E_L \xrightarrow{\mathrm{cor}} {}_2\mathrm{Br}\, E$$

where ϵ_L is as above. Then there exists a homomorphism $\varepsilon : {}_2H^1(\Gamma, \overline{E}) \longrightarrow {}_2\mathrm{Br}\, E$ such that $\varepsilon \circ \zeta = \epsilon$ and $\kappa \circ \varepsilon = 1_{{}_2H^1(\Gamma, \overline{E})}$ is the identical map.

Proof. This is entirely analogous to the proof of Proposition 4.1. The only difference is that instead of τ we have to use the homomorphism $H^1(\Gamma, M) \stackrel{\text{res}}{\to} H^1(\Theta, M)$. □

Keeping the above notation we may reformulate Proposition 5.1 in terms of central simple algebras. We distinguish two cases.

Theorem 5.2 *Suppose that the curve E_L is split. Let $f(x) = (x-a)(x-b)(x-c)$, where $a, b, c \in L = K(a)$. Let $\varepsilon : {}_2H^1(\Gamma, \overline{E}) \to {}_2\mathrm{Br}\, E$ be the section for the homomorphism κ described in Proposition 5.1 and $I = \mathrm{Im}\, \varepsilon$. Then*

$$ {}_2\mathrm{Br}\, E \cong {}_2\mathrm{Br}\, K \oplus I $$

and any element in I has the form

$$ \mathrm{cor}_{L/K}\, [(r, x-b) \otimes (s, x-c)] $$

where $r, s \in L^*$. Conversely, any such a class of algebras is unramified over $K(E)$ and it is trivial in I if and only if it coincides with a class

$$ \mathrm{cor}_{L/K}\, [(u-c, x-b) \otimes (u-b, x-c)], $$

where u is the abscissa of a point in $E(K)$.

Proof. Since ϵ is the composition

$$ H^1(\Gamma, M) \stackrel{\text{res}}{\longrightarrow} H^1(\Theta, M) \stackrel{\epsilon_L}{\longrightarrow} {}_2\mathrm{Br}\, E_L \stackrel{\text{cor}}{\longrightarrow} {}_2\mathrm{Br}\, E\ , $$

it follows that ε is the composition

$$ {}_2H^1(\Gamma, \overline{E}) \stackrel{\text{res}}{\longrightarrow} {}_2H^1(\Theta, \overline{E}) \stackrel{\varepsilon_L}{\longrightarrow} {}_2\mathrm{Br}\, E_L \stackrel{\text{cor}}{\longrightarrow} {}_2\mathrm{Br}\, E $$

(an easy diagram chase). Hence

$$ I = \mathrm{Im}\, \varepsilon = \mathrm{cor}(\mathrm{Im}\, \varepsilon_L)\ . $$

According to Theorem 3.6 any element in $\mathrm{Im}\, \varepsilon_L$ is represented by an algebra of type $(r, x-b) \otimes (s, x-c)$ where $r, s \in L^*$. Hence an element in I has the form $\mathrm{cor}_{L/K}\, [(r, x-b) \otimes (s, x-c)]$ for some $r, s \in L^*$.
Let $r, s \in L^*$. Consider the algebra $(r, x-b) \otimes (s, x-c)$ over $L(E)$. It is unramified because its class lies in the image of the homomorphism ϵ_L. Therefore the class

$$ \alpha = \mathrm{cor}_{L/K}\, [(r, x-b) \otimes (s, x-c)] \in \mathrm{Br}\, K(E) $$

is also unramified. Assume that $\alpha \in I$. If

$$ \alpha = \mathrm{cor}_{L/K}\, [(u-c, x-b) \otimes (u-b, x-c)] $$

where u is the abscissa of a point in $E(K)$, then $\alpha = 0$ because

$$ [(u-c, x-b) \otimes (u-b, x-c)] = 0 $$

in $\operatorname{Im}\varepsilon_L$, by Theorem 3.6. Conversely, if $\alpha = 0$ in I then α grows up (via ζ and ε) from the image of the connecting homomorphism δ. By the construction all homomorphisms δ, ζ, ε commute with restriction homomorphisms. It follows that α is equal to a class of algebras coming from $E(K)/2$, that is of type $\operatorname{cor}_{L/K}[(u-c, x-b)\otimes(u-b, x-c)]$ where u is the abscissa of a point in $E(K)$.
□

THEOREM 5.3 *Suppose that the curve E_L is semisplit. Let $f(x) = (x-a)g(x)$, where $a \in L$, $g(x)$ is an irreducible quadratic polynomial over L and $g(x) = (x-b)(x-c)$ over $\overline{K}$. Let $\varepsilon : {}_2H^1(\Gamma, \overline{E}) \to {}_2\operatorname{Br} E$ be the section for the homomorphism κ described in Proposition 5.1 and $I = \operatorname{Im}\varepsilon$. Then*

$$ {}_2\operatorname{Br} E \cong {}_2\operatorname{Br} K \oplus I $$

and every element in I is represented either by a class

$$ \operatorname{cor}_{L/K}[r, x-a], $$

where $r \in L^*$, or a class of the form

$$ \operatorname{cor}_{L/K}\left[(t, r^2 - h^2t^2) \otimes (t(x-h) + r, (r^2 - t^2h^2)g(x))\right] $$

where $h = (b+c)/2 \in L$, $r, t \in L$ and $t \neq 0$. Conversely, every such a class is unramified over $K(E)$. It is trivial in I if and only if it coincides with a class

$$ \operatorname{cor}_{L/K}[x-h+u, (u+h-a)(x-a)] $$

where u is the abscissa of a point in $E(K)$.

Proof. The proof is similar to that of Theorem 5.2. The difference is just that we use Proposition 4.13 instead of Proposition 3.6. Indeed, we have $I = \operatorname{cor}(\operatorname{Im}\varepsilon_L)$. According to Theorem 4.13 any element in $\operatorname{Im}\varepsilon_L$ is represented by either a quaternion algebra of the form $A = (r, x-a)$, where $r \in K^*$, or a biquaternion algebra of the form

$$ B = (t, r^2 - h^2t^2) \otimes (t(x-h) + r, (r^2 - t^2h^2)g(x)), $$

where $h = (b+c)/2 \in K$, $r, t \in K$ and $t \neq 0$. Therefore an element in I is equal to either $\operatorname{cor}_{L/K}[A]$ or $\operatorname{cor}_{L/K}[B]$.
An algebra of the types A or B lies in $\operatorname{Im}\varepsilon_L$ and hence it is unramified. Therefore, classes $\operatorname{cor}_{L/K}[A]$ and $\operatorname{cor}_{L/K}[B]$ are also unramified. They are trivial in I if and only if they come from the image of the connecting homomorphism δ via the homomorphisms ζ and ε. Since δ, ζ and ε commute with the corresponding restriction homomorphisms, it follows (using the second assertion of Proposition 4.13) that the classes $\operatorname{cor}_{L/K}[A]$ and $\operatorname{cor}_{L/K}[B]$ are trivial in I if and only if they coincide with a class

$$ \operatorname{cor}_{L/K}[x-h+u, (u+h-a)(x-a)]\ , $$

where u is the abscissa of a point in $E(K)$. □

The generators of ${}_2\mathrm{Br}\, E$ given in Theorems 5.2 and 5.3 are represented as classes $\mathrm{cor}_{L/K}[A]$, where A is a quaternion or biquaternion algebra over the cubic extension $L(E)/K(E)$. We close this section by showing how one can rewrite these generators as tensor products of quaternion algebras defined over $K(E)$.
Let P/K be a cubic extension and let $P = K(s)$ for some element $s \in P$.

Lemma 5.4 *Every element $a \in P$ can be written in the form*

$$a = \frac{\theta_1 + \theta_2 s}{\theta_3 + \theta_4 s} \ ,$$

where $\theta_1, \theta_2, \theta_3, \theta_4 \in K$.

Proof. Let $V = \{\theta_1 + \theta_2 s \mid \theta_1, \theta_2 \in K\}$ be a two-dimensional vector space over F. Since aV is also a two-dimensional vector space over K, the intersection $V \cap aV$ has dimension at least one. Let $b \in V \cap aV$ be a non-zero element. Then there exists $\theta_1, \theta_2, \theta_3, \theta_4 \in K$ such that

$$b = \theta_1 + \theta_2 s = (\theta_3 + \theta_4 s)a.$$

It follows that

$$a = \frac{\theta_1 + \theta_2 s}{\theta_3 + \theta_4 s} \ ,$$

as required. □

Lemma 5.5 *Let $a, b \in K$ be such that $a + b \neq 0$. Then*

$$\mathrm{cor}_{P/K}[a+s, b-s] = \big[a+b, (a+b)\, N_{P/K}((a+s)(b-s))\big] \ .$$

Proof. Let

$$t = \frac{a+s}{a+b} \quad \text{and} \quad l = \frac{b-s}{a+b} \ .$$

Then $t + l = 1$, whence $[t, l] = [t, 1-t] = 0$ in $\mathrm{Br}\, P$. Substituting t, l, we have

$$0 = [t, l] = \left[\frac{a+s}{a+b}, \frac{b-s}{a+b}\right] =$$

$$[a+s, b-s] + [a+b, b-s] + [a+s, a+b] + [a+b, a+b] \ .$$

Taking $\mathrm{cor}_{P/F}$ and using Lemma 4.9 we obtain that

$$0 = \mathrm{cor}_{P/K}[a+s, b-s] + [a+b, N_{P/K}(b-s)] +$$

$$[N_{P/K}(a+s), a+b] + [a+b, (a+b)^3] \ .$$

Therefore,

$$\mathrm{cor}_{P/F}[a+s, b-s] = [a+b, N_{P/K}(b-s)] + [N_{P/K}(a+s), a+b] + [a+b, a+b] \ ,$$

as required. □

Lemma 5.6 *Let* $u_1, v_1, u_2, v_2 \in K$*,* $v_1 \neq 0$*,* $v_2 \neq 0$ *and* $v_1 u_2 \neq u_1 v_2$*. Then*

$$\operatorname{cor}_{P/K}[u_1 + v_1 s, u_2 + v_2 s] = \big[v_1(v_1 u_2 - u_1 v_2), N_{P/K}(u_1 + v_1 s)\big] +$$

$$\big[v_2(u_1 v_2 - v_1 u_2), v_1(v_1 u_2 - u_1 v_2)\, N_{P/K}(u_2 + v_2 s)\big] \ .$$

Proof. This is entirely analogous to the proof of Lemma 4.11 and so we omit the details to the reader. □

Using Lemmas 5.4, 4.9, 5.5 and 5.6 one can easily produce explicit formulas to compute all algebras in Theorems 5.2 and 5.3. However we do not present them because of their bulk.

6 *Elliptic curves over local fields*

In the next few sections we demonstrate the efficiency of the above cohomological methods by considering an elliptic curve E defined over a local non-dyadic field K. To get an explicit description of ${}_2\mathrm{Br}\, E$, by Theorems 3.6, 4.13, 5.2 and 5.3, we only need to explicitly describe all relations between the generators indicated in these theorems which is equivalent to the description of the image of the boundary map $\delta : E(K)/2 \to H^1(\Gamma, M)$.
For an elliptic curve over local fields there is a natural p-adic filtration on the group of K-points with finite quotients. Examining each quotient individually one can very quickly find generators for the group $E(K)/2$. This leads in turn to the required description of $\mathrm{Im}\, \delta$. All necessary facts for our further argument can be easily elicited from standard textbooks, for example from [Hu87] and [Sil85]. For the convenience of the reader we start with recalling them.

For the rest of the paper we use the following specific notation:

K – a local non-dyadic field, i.e. a finite extension of the p-adic field $\mathbb{Q}_p$, $p \neq 2$;
v – the discrete valuation on K;
$\mathcal{O} = \mathcal{O}_K$ – the ring of integers of K;
$\mathcal{O}^* = \mathcal{O}^*_K$ – the unit group of O;
$\alpha = \alpha_K \in \mathcal{O}^*$ – a non-square element;
$\pi = \pi_K$ – a uniformizer for O;
$k = \mathcal{O}/\pi\, \mathcal{O}$ – the residue field of K.

Theorem 6.1 *There is a natural isomorphism*

$$H^1(\Gamma, \overline{E}) \cong \mathrm{Hom}_{cont}(E(K), \mathbb{Q}/\mathbb{Z}) \ .$$

Proof. See [Tate57] or [Mi86]. □

Corollary 6.2 $|\, {}_2\mathrm{Br}\, E| = 2 \cdot \sqrt{|H^1(\Gamma, M)|}$.

Proof. By Theorem 6.1, we have

$$|\ {}_2H^1(\Gamma,\overline{E})| = |\ {}_2\mathrm{Hom}_{cont}(E(K),\mathbb{Q}/\mathbb{Z})| =$$

$$|\mathrm{Hom}_{cont}(E(K)/2,\mathbb{Q}/\mathbb{Z})| = |E(K)/2|\ .$$

On the other hand, sequence (8) shows that

$$|\ {}_2H^1(\Gamma,\overline{E})| = |H^1(\Gamma,M)|/|E(K)/2|\ .$$

Therefore,

$$|E(K)/2|^2 = |H^1(\Gamma,M)|$$

and the result follows. □

Proposition 6.3 *Let n be a natural number. Then*

$$|E(K)/nE(K)| = |{}_nE(K)|\cdot|\mathcal{O}/n\mathcal{O}|.$$

Proof. See, for example, [Mi86], p. 52. □

Corollary 6.4 *Let E be a non-split elliptic curve defined over a local non-dyadic field K. Then ${}_2\mathrm{Br}\,E = {}_2\mathrm{Br}\,K$.*

Proof. Clearly, we have

$$|\ {}_2\mathrm{Br}\,E\,| = |\ {}_2\mathrm{Br}\,K\,|\cdot|\ {}_2H^1(\Gamma,\overline{E})\,| = |\ {}_2\mathrm{Br}\,K\,|\cdot|E(K)/2\,|\ .$$

Since E is non-split, it follows that every nontrivial element from M is not defined over K. Therefore, ${}_2E(K)=0$ and, by Proposition 6.3, we obtain that $E(K)/2=0$. This implies that $|\ {}_2\mathrm{Br}\,E\,| = |\ {}_2\mathrm{Br}\,K\,|$, as required. □

Let E be an elliptic curve over K and let

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be a Weierstrass equation for the curve E/K with all coefficients $a_i \in \mathcal{O}$. Since its discriminant Δ is also an integer and since v is discrete we can look for an equation with $v(\Delta)$ as small as possible. A Weierstrass equation is called a *minimal* equation for E if $v(\Delta)$ is minimized subject to the condition a_1, a_2, a_3, a_4, $a_6 \in \mathcal{O}$.
It is known (see [Sil85], Proposition 1.3, p. 172) that a minimal (Weierstrass) equation is unique up to a change of coordinates

$$x = u^2x' + r\ , \qquad y = u^3y' + u^2sx' + t$$

with $u \in \mathcal{O}^*$ and r, s, $t \in \mathcal{O}$. Since, by our assumption, $2 \in \mathcal{O}^*$, a coordinate change $y \to y' = y + (a_1x + a_3)/2$ shows that we may always assume that $a_1 = a_3 = 0$, i.e. E is given by a minimal equation of the form

$$y^2 = x^3 + a_2x^2 + a_4x + a_6\ . \tag{11}$$

Later we need to know when (11) is a minimal equation for E. Let

$$b_2 = 4a_2\ , \quad b_4 = 2a_4\ , \quad b_6 = 4a_6\ , \quad b_8 = 4a_2a_6 - a_4^2\ ,$$

$$c_4 = b_2^2 - 24b_4\ , \quad c_6 = b_2^3 + 36b_2b_4 - 216b_6$$

be the usual combinations of the a_i‘s and let

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

be the discriminant of equation (11) (see [Sil85], p. 46).

Proposition 6.5 *Equation (11) with integer coefficients* a_2, a_4, a_6 *is minimal if and only if either* $v(\Delta) < 12$ *or* $v(c_4) < 4$.

Proof. See [Sil85], page 186, Exercises 7.1. □

We assume that our elliptic curve E is given by a minimal equation (11). Reducing its coefficients modulo π we obtain the curve (possibly singular) $\widetilde{E}$ over k:

$$y^2 = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6\ .$$

The curve $\widetilde{E}$ is called the *reduction* of E modulo π.
Next let $P \in E(K)$. We can find homogeneous coordinates $P = [x_0, y_0, z_0]$ with integers x_0, y_0, z_0 such that at least one of them is in $\mathcal{O}^*$. Then the reduced point $\widetilde{P} = [\tilde{x}_0, \tilde{y}_0, \tilde{z}_0]$ is in $\widetilde{E}$. This gives a reduction map

$$E(K) \longrightarrow \widetilde{E}(k), \qquad P \longrightarrow \widetilde{P}\ .$$

Since the curve $\widetilde{E}$ can be singular, we denote its set of nonsingular points by $\widetilde{E}_{ns}(k)$ and we put

$$E_0(K) = \{P \in E(K) \mid \widetilde{P} \in \widetilde{E}_{ns}(k)\}$$

$$E_1(K) = \{P \in E(K) \mid \widetilde{P} = \widetilde{O}\}\ .$$

Proposition 6.6 *The following natural sequence of abelian groups*

$$0 \to E_1(K) \longrightarrow E_0(K) \longrightarrow \widetilde{E}_{ns}(k) \to 0$$

is exact.

Proof. See [Sil85], Proposition 2.1, p. 174. □

Proposition 6.7 *The group* $E_1(K)$ *is uniquely divisible by* 2*; in particular, we have* $E_1(K) = 2E_1(K)$.

Proof. See [Hu87], Corollary 1.3, p. 264. □

Let E/K be an elliptic curve and let $\widetilde{E}/k$ be the reduced curve for a minimal Weierstrass equation. One says that

(a) E has *good* reduction over K if $\widetilde{E}$ is nonsingular;

(b) E has *multiplicative* reduction over K if $\widetilde{E}$ has a node; in this case the reduction is said to be *split* (respectively *non-split*) if the slopes of the tangent lines at the node are in k (respectively not in k);

(c) E has *additive* reduction over K if $\widetilde{E}$ has a cusp.

Proposition 6.8 *Let E/K be an elliptic curve given by a minimal Weierstrass equation* (11)*.*

(a) *E has good reduction if and only if $v(\Delta) = 0$;*
(b) *E has multiplicative reduction if and only if $v(\Delta) > 0$ and $v(c_4) = 0$;*
(c) *E has additive reduction if and only if $v(\Delta) > 0$ and $v(c_4) > 0$.*

Proof. See [Sil85], Proposition 5.1, p. 180. □

7 *Generators of $E(K)/2$ for a split elliptic curve over a local field*

Let E be a split elliptic curve given by a minimal equation (11). Since M is a trivial Γ-module, it follows that all roots of the cubic polynomial $f(x) = x^3 + a_2x^2 + a_4x + a_6$ are in K. Then these roots, clearly, belong to $\mathcal{O}$, so that we may assume that E is given by a minimal equation of the form

$$y^2 = (x - a)(x - b)(x - c) \tag{12}$$

with all a, b, c in $\mathcal{O}$. In this coordinate system M consists of the points

$$O, \quad P = (a, 0), \quad Q = (b, 0), \quad T = (c, 0)\ .$$

Recall also that, by Proposition 6.3, we have $|E(K)/2| = |M| = 4$.

7.1 *Additive reduction*

Lemma 7.1 *The group $E_0(K)$ is divisible by* 2*.*

Proof. Since E has additive reduction, we have $E_0(K)/E_1(K) \cong k^+$; in particular the finite group $E_0(K)/E_1(K)$ is divisible by 2. Then the result follows from Proposition 6.7. □

Proposition 7.2 *The elements O, P, Q, T are representatives of $E(K)/2$.*

Proof. In view of Lemma 7.1 we have $E_0(K) \subset 2E(K) \subset E(K)$ and by [Sil85], Theorem 6.1, p. 183, the group $E(K)/E_0(K)$ is finite of order at most 4. Since $|E(K)/2| = 4$, we get $E_0(K) = 2E(K)$ and it remains to note that the points P, Q, T do not belong to $E_0(K)$. □

7.2 *Multiplicative reduction*

By our assumption, among the residues $\tilde{a}$, $\tilde{b}$, $\tilde{c}$ there are exactly two coinciding elements; say $\tilde{a} = \tilde{b}$. Changing coordinates, if necessary, we may assume that E is given by a minimal equation of the form

$$y^2 = x(x + \pi^m \beta)(x + \gamma)$$

with $\beta \in \mathcal{O}^*$, $m \geq 1$ and $\gamma \in \mathcal{O}^*$. Recall that in the case of non-split reduction γ coincides modulo squares with α; otherwise γ is a square in $\mathcal{O}^*$.

LEMMA 7.3 *There exists a point $R_1 = (u, v) \in E_0(K)$ such that*

$$u = \alpha t^2 \,, \quad u + \pi^m \beta = \alpha q^2 \,, \quad u + \gamma = s^2 \,, \quad v = \alpha\, t\, q\, s$$

with t, q, s in $\mathcal{O}^*$.

Proof. The proof is easy. Namely, we have to find a solution of the system

$$\begin{cases} \alpha x^2 + \pi^m \beta & = & \alpha y^2 \\ \alpha x^2 + \gamma & = & z^2 \end{cases}$$

According to standard facts from the theory of quadratic forms over finite and local fields the quadratic form $\tilde{\alpha} x^2 - z^2$ represents $-\gamma \in k^*$, whence, by the Hensel lemma, we can pick units t, $s \in \mathcal{O}^*$ satisfying the second equation. Substitute t in the first equation. Since the residues of the elements $\alpha t^2 + \pi^m \beta$ and α coincide modulo squares, again, applying the Hensel lemma we can find $q \in \mathcal{O}^*$ satisfying the equation $\alpha t^2 + \pi^m \beta = \alpha y^2$. $\square$

REMARK 7.4 *Since the abscissa u of R_1 is not a square in K^*, Proposition 3.3 shows that $\delta(R_1) \neq (1,1)$. Then it follows that $R_1 \notin 2E(K)$.*

LEMMA 7.5 *There exists a point $R_2 = (u, v) \in E(K) \setminus E_0(K)$ with $u = \pi d$, $d \in \mathcal{O}$, and such that its image in the group $E(K)/E_0(K)$ is not divisible by 2.*

Proof. The abscissa of every point from $E(K) \setminus E_0(K)$ is of the form πd with $d \in \mathcal{O}$ because its residue is the node. Further, we have $\Delta = 16(\pi^m \beta \gamma (\pi^m \beta - \gamma))^2$ and $\pi^m \beta - \gamma \in \mathcal{O}^*$, so that $v(\Delta)$ is even. Then, by [Hu87], p. 266, the order of the finite group $E(K)/E_0(K)$ is divisible by 2, whence such a point exists. $\square$

REMARK 7.6 *If the reduction is non-split, we can take $R_2 = (0,0)$, because in this case the group $E(K)/E_0(K)$ has order 2 (loc. cit.) and, of course, $R_2 = (0,0) \notin E_0(K)$.*

PROPOSITION 7.7 *The points R_1, R_2 from the above two lemmas are generators of $E(K)/2E(K)$.*

Proof. Since $|E(K)/2| = 4$, we have $E(K)/2E(K) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. By our construction and by Remark 7.4, the images of R_1, R_2 in $E(K)/2E(K)$ are not trivial and they do not coincide. $\square$

8 *Generators of $E(K)/2$ for a semisplit elliptic curve over a local field*

We may assume that E is given by a minimal equation of the form

$$y^2 = (x-a)(x^2-d), \tag{13}$$

where $a, d \in \mathcal{O}$ and the polynomial $g(x) = x^2 - d$ is irreducible over K. Let $L = K(\sqrt{d})$ be its splitting field and let $\Lambda = \mathrm{Gal}\,(\overline{K}/L)$. As it was mentioned in Section 4, the module M is isomorphic to the induced module $M_\Gamma^\Lambda(\mathbb{Z}/2)$. This gives the isomorphisms

$$H^1(\Gamma, M) \cong L^*/L^{*2}\,, \qquad H^1(\Lambda, M) \cong L^*/L^{*2} \times L^*/L^{*2}\,.$$

Recall also that under this identification the restriction map $H^1(\Gamma, M) \to H^1(\Lambda, M)$ is given by the formula $l \to (l^\sigma, l)$, where $l \in L^*$ and σ is the nontrivial automorphism L/K; in particular, res is injective (see Section 4). It then follows from the commutative square

$$\begin{array}{ccc} E(L)/2 & \xhookrightarrow{\delta_L} & L^*/L^{*2} \oplus L^*/L^{*2} \\ \uparrow{\scriptstyle \eta} & & \uparrow{\scriptstyle \mathrm{res}} \\ E(K)/2 & \xhookrightarrow{\delta} & L^*/L^{*2} \end{array}$$

that $\eta : E(K)/2 \to E(L)/2$ is also injective. Applying Proposition 6.3 we have $|E(K)/2| = |\,{}_2E(K)| = 2$. Now we want to explicitly describe the image $\eta(E(K)/2)$. The answer depends on the type of reduction.

8.1 *Multiplicative reduction.*

For an elliptic curve given by (13) one has $\Delta = 64d(a^2-d)^2$ and $c_4 = 16(a^2 + 3d)$. Since, by Proposition 6.8, $v(\Delta) > 0$ and $v(c_4) = 0$, we obtain that $v(d) > 0$ and $a \in \mathcal{O}^*$. Then, according to Proposition 6.5, (13) is a minimal equation for E_L. Hence E_L has multiplicative reduction (again by Proposition 6.8). Note that in view of $v(d) > 0$ and $a \in \mathcal{O}^*$ we have $a^2 - d \in O^*$, whence $v(\Delta) = v(d)$. We say that we are in case:

(M1) if either $v(d)$ is odd or 4 divides $v(d)$ and E has non-split multiplicative reduction;

(M2) if $v(d)$ is even and either E has split multiplicative reduction or 4 does not divide $v(d)$.

Proposition 8.1 *Let R_1, R_2 be the points in $E(L)$ introduced in 7.2. Then in case* (M1) *the nontrivial element of $\eta(E(K)/2)$ coincides with $R_1 + 2E(L)$ and in case* (M2) *it coincides with $R_2 + 2E(L)$.*

Proof. Consider case (M1). If $v(d)$ is odd, then by, [Hu87], p. 266, the group $E(K)/E_0(K)$ has an odd order. So we may choose a representative R of a unique nontrivial element in $E(K)/2$ among elements of $E_0(K)$. Since $E_0(K) \subset E_0(L)$ and η is injective, R coincides with R_1 modulo $2E(L)$.

Next suppose that 4 divides $v(d)$ and E has non-split multiplicative reduction. Since $v(d)$ is even, the extension L/K is unramified, so that $[k_L : k] = 2$, where k_L is the residue field of the local field L. It follows that E_L has split multiplicative reduction and, by [Hu87], p. 266, the group $E(L)/E_0(L)$ is cyclic of order $v(\Delta_L) = v(\Delta_K) = v(d)$; in particular, 4 divides $|E(L)/E_0(L)|$.

Let R be a representative of the nontrivial element of $E(K)/2$. Since E has non-split multiplicative reduction, it follows that $|E(K)/E_0(K)| = 2$ (loc. cit.), hence R can be chosen among elements $E(K)\backslash E_0(K)$. To show that $\eta(R)$ coincides with R_1 modulo $2E(L)$ consider the 2-Sylow subgroup G in $E(L)/E_0(L)$. It is clear that $R + E_0(L) \in G$ and it has order 2. Then $R + E_0(L)$ is divisible by 2 in G and so in $E(L)/E_0(L)$. But, by our construction (see Lemma 7.5), the element R_2 is not divisible by 2 in $E(L)/E_0(L)$, so we obtain $R+2E(L) \neq R_2+2E(L)$ and similarly we have $R+2E(L) \neq R_1+R_2+2E(L)$. It follows that $R + 2E(L) = R_1 + 2E(L)$, as required.

Consider case (M2). We have already mentioned that (13) is a minimal equation for E_L. It follows that $E_0(K) \subset E_0(L)$ and that the natural embedding $E(K) \subset E(L)$ induces the injection $\psi : E(K)/E_0(K) \to E(L)/E_0(L)$.

Suppose that E has split multiplicative reduction and $v(d)$ is even. Then L/K is unramified and again, by [Hu87], p. 266, the groups $E(K)/E_0(K)$ and $E(L)/E_0(L)$ are cyclic of the same order $v(\Delta) = v(\Delta_L) = v(d)$ implying ψ is a bijection. Since $v(d)$ is even, we can choose a representative R of the nontrivial element of $E(K)/2$ such that $R + E_0(K)$ is not divisible by 2 in $E(K)/E_0(K)$. Then it is not divisible by 2 in $E(L)/E_0(L)$; hence $R + 2E(L) = R_2 + 2E(L)$.

Suppose that E has non-split multiplicative reduction. Then according to [Hu87], p. 266, we have $|E(K)/E_0(K)| = 2$ and $|E(L)/E_0(L)| = v(d)$. Since 4 does not divide $v(d)$, the group $\psi\,(E(K)/E_0(K))$ is a 2-Sylow subgroup in $E(L)/E_0(L)$. Hence again picking an element R with the same property as above we easily get $R + 2E(L) = R_2 + 2E(L)$. □

8.2 *Additive reduction*

Proposition 8.2 (1) *If L/K is unramified, then $E(K)/2$ is generated by $P = (a, 0)$.*

(2) *Let L/K be ramified. If $a - \sqrt{d}$ is not a square in L^*, then $E(K)/2$ is again generated by $P = (a, 0)$. If $a - \sqrt{d} = s^2$, $s \in L^*$, then $E(K)/2$ is generated by the point $U = (u, w) \in E(K)$, where $u = N_{L/K}(s) + a$ and $w = N_{L/K}(s)\; Tr_{L/K}(s)$.*

Proof. First let L/K be unramified. Then E_L has additive reduction and by Proposition 7.2, we have $P \notin 2E(L)$. It follows that $P \notin 2E(K)$, as required.

Next let L/K be ramified. Recall that, by Lemma 7.1, we have $E_0(K) \subset 2E(K)$ and that $E(K)/E_0(K)$ is a group of order at most 4 (see [Sil85], p. 183).
If $a - \sqrt{d}$ is not a square in L^*, then, by Proposition 3.3, $\delta_L(P) \neq (1,1)$, hence $P \notin 2E(L)$ and the result follows.
Let $a - \sqrt{d} = s^2$, $s \in L^*$. Then it is easy to check that $2U = P$. This implies that $P \in 2E(K) \setminus E_0(K)$ and so $|2E(K)/E_0(K)| \geq 2$. But $|E(K)/2E(K)| = 2$ and $|E(K)/E_0(K)| \leq 4$. It follows that $|2E(K)/E_0(K)| = 2$, whence $U \notin 2E(K)$, as required. □

For the description of ${}_2\mathrm{Br}\, E$ we will also need to know whether $(\delta_L \circ \eta)\,(E(K)/2)$ belongs to the unramified part of the subset $\mathrm{res}\,(L^*/L^{*2}) \subset L^*/L^{*2} \times L^*/L^{*2}$. In other words, we will need to know whether $v_L(a + \sqrt{d})$ and $v_L(u + \sqrt{d})$ are odd or even. Here u is the abscissa of the above point U. It turns out that the answer depends on the coefficients of the minimal equation (13) only.
Let $a = \pi^m a'$, $d = \pi^{2k+\lambda} d'$ with $a', d' \in \mathcal{O}^*$ and $\lambda = 0, 1$. Using Propositions 6.5 and 6.8 one can easily make sure that $m > 0$, $2k + \lambda > 0$ and that $m = 1$ or $2k + \lambda \leq 3$. We will say that we are in case:

$(A1)$ if one of the following conditions holds:
- (a) $\lambda = 0$, i.e. L/K is unramified,
- (b) $\lambda = 1$, $m = 1$, $k = 0$,
- (c) $\lambda = 1$, $m > 1$;

$(A2)$ if $\lambda = 1$, $m = 1$, $k \geq 1$ and $a - \sqrt{d} \notin L^{*2}$.

$(A3)$ if $\lambda = 1$, $m = 1$, $k \geq 1$ and $a - \sqrt{d} \in L^{*2}$,

Lemma 8.3 (i) *In case* (A1) *the group* $E(K)/2$ *is generated by* P *and* $v_L(a + \sqrt{d})$ *is odd.*
(ii) *In case* (A2) *the group* $E(K)/2$ *is generated by* P *and* $v_L(a + \sqrt{d})$ *is even.*
(iii) *In case* (A3) *the group* $E(K)/2$ *is generated by* U *and* $v_L(u + \sqrt{d})$ *is odd.*

Proof. First examine case $(A1)$.
(a) Here L/K is unramified and at least one of the numbers k and m equals 1. So, obviously, $v_L(a + \sqrt{d}) = 1$.
(b) Since L/K is ramified, we have $v_L(a) = v_L(\pi) = 2$ and $v_L(\sqrt{d}) = 1$. So $v_L(a + \sqrt{d}) = 1$.
(c) We have $v_L(a) = 2m \geq 4$ and $v_L(\sqrt{d}) = 2k+1$. Since $2k+\lambda \leq 3$, we obtain that $v_L(a + \sqrt{d}) = v_L(d) = 2k + 1$ is odd.
Case $(A2)$. Since L/K is ramified, we have $v_L(a) = v_L(\pi) = 2$ and $v_L(\sqrt{d}) = 2k + 1 \geq 3$. It follows that $v_L(a + \sqrt{d}) = 2$.
Case $(A3)$. Keeping the notation of Proposition 8.2 we have $a - \sqrt{d} = s^2$ and $u = N_{L/K}(s) + a$. It easily follows that $v_L(s) = 1$. Further, letting σ be the nontrivial automorphism L/K we have

$$u + \sqrt{d} = N_{L/K}(s) + a + \sqrt{d} = ss^\sigma + s^\sigma s^\sigma = (s + s^\sigma)s^\sigma.$$

Therefore, $v_L(u + \sqrt{d}) = v_L(s + s^\sigma) + 1$ and it remains to note that $v_L(s + s^\sigma)$ is even because $s + s^\sigma \in K$. □

9 *Computing* ${}_2\mathrm{Br}\,E$ *over non-dyadic local fields: split case*

Putting together the results of the previous sections one can easily obtain an explicit and very short description of the 2-torsion subgroup of $\mathrm{Br}\,E$ for split and semisplit elliptic curves (note that for non-split curves it was done in Corollary 6.4). Namely, let $\delta : E(K)/2 \to H^1(\Gamma, M)$ be the boundary map. The description of generators of $E(K)/2$ and their images under the map δ given in Sections 7 and 8 enables us to explicitly construct a subgroup in $H^1(\Gamma, M)$ that complements $\delta(E(K)/2)$. If we then restrict the section $\epsilon : H^1(\Gamma, M) \to {}_2\mathrm{Br}\,E$ constructed in Sections 3 and 4 at this subgroup, we immediately obtain a description of the second summand in the decomposition ${}_2\mathrm{Br}\,E = {}_2\mathrm{Br}\,K \oplus \mathrm{Im}\,\epsilon$ as, by Proposition 3.4, and Lemma 4.8, the equality $\epsilon\,(\mathrm{Im}\,\delta) = 0$ holds.
In this section we consider a split elliptic curve E given by a minimal equation of the form

$$y^2 = x(x-b)(x-c)\ , \tag{14}$$

with b, c in the integer ring $\mathcal{O}$. Its 2-torsion consists of the points O, $P = (0,0)$, $Q = (b, 0)$ and $T = (c, 0)$. As in Section 3, we may identify

$$M = \langle Q\rangle \oplus \langle T\rangle \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$$

and

$$H^1(\Gamma, M) \cong K^*/K^{*2} \oplus K^*/K^{*2}\ .$$

According to Proposition 3.3 the connecting homomorphism

$$\delta : E(K)/2 \hookrightarrow K^*/K^{*2} \oplus K^*/K^{*2}$$

is given by the formula

$$\delta(u,v) = \begin{cases} (u-c, u-b) & \text{if } u \neq b \text{ and } u \neq c, \\ (b-c, b(b-c)) & \text{if } u = b, \\ (c(c-b), c-b) & \text{if } u = c, \\ (1,1) & \text{if } u = \infty, \end{cases} \tag{15}$$

where $(u, v) \in E(K)$. Let

$$C_\alpha = [\alpha, x-c]\,, \quad C_\pi = [\pi, x-c]\,, \quad B_\alpha = [\alpha, x-b] \quad \text{and} \quad B_\pi = [\pi, x-b] \tag{16}$$

be the classes of quaternion algebras over $K(E)$. We distinguish the following three cases.

9.1 *Good reduction*

We start with the following

Lemma 9.1 *$\delta(E(K)/2)$ is generated by the pairs $(\alpha, 1)$ and $(1, \alpha)$.*

Proof. Let K^{nr}/K be a maximal unramified extension. It suffices to show that the images of our pairs under the natural map $\zeta : H^1(\Gamma, M) \to {}_2H^1(\Gamma, \overline{E})$ are trivial. To do so, first recall that, by [LT58] and [L56], we have

$$H^1(\mathrm{Gal}\,(K^{nr}/K), E(K^{nr})) = H^1(\mathrm{Gal}\,(\bar{k}/k), \widetilde{E}) = 0 \; .$$

This implies that $\mathrm{res} : H^1(\Gamma, \overline{E}) \to H^1(K^{nr}, \overline{E})$ is injective. On the other hand, obviously we have $(\mathrm{res} \circ \zeta)(\alpha, 1) = (\mathrm{res} \circ \zeta)(1, \alpha) = 1$, so the result follows. □

Proposition 9.2 *We have*

$${}_2\mathrm{Br}\, E = {}_2\mathrm{Br}\, K \oplus \{0, B_\pi, C_\pi, B_\pi + C_\pi\} \; .$$

Proof. It suffices to note that the subgroup generated by the pairs $(\pi, 1)$ and $(1, \pi)$ complements the subgroup $\delta(E(K)/2)$ and that ϵ takes these pairs to the classes B_π and C_π. □

9.2 *Additive reduction*

We may assume that $v(b) \geq 1$, $v(c) \geq 1$ and that at least one of these numbers is 1. Let $b = \pi^m d$ and $c = \pi e$, where d and e are units and $m \geq 1$. Proposition 7.2 shows that $E(K)/2$ is generated by the points P, Q, T. Applying (15) we get

Lemma 9.3 $\delta(E(K)/2)$ *is generated by the pairs*

$$\delta(P) = (-\pi e, -\pi^m d) \quad \textit{and} \quad \delta(T) = (\pi e(\pi e - \pi^m d), \pi e - \pi^m d) \; .$$

Proposition 9.4 *We have*

$${}_2\mathrm{Br}\, E = {}_2\mathrm{Br}\, K \oplus \{0, B_\alpha, C_\alpha, B_\alpha + C_\alpha\} \; .$$

Proof. It easily follows from Lemma 9.3 that the subgroup generated by the pairs $(\alpha, 1)$ and $(1, \alpha)$ complements $\delta(E(K)/2)$ in $K^*/K^{*2} \oplus K^*/K^{*2}$ and it remains to note that ϵ takes these pairs to the classes B_α and C_α. □

9.3 *Non-split multiplicative reduction*

We may assume that E is given by a minimal equation of the form

$$y^2 = x(x + \pi^m \beta)(x + \alpha) \; ,$$

with $m \geq 1$ and $\beta \in \mathcal{O}$. Note that in the notation of formulas (15) and (16) we have that

$$b = -\pi^m \beta \qquad \text{and} \qquad c = -\alpha \; .$$

Lemma 9.5 *$\delta(E(K)/2)$ is generated by the pairs $(1, \alpha)$ and $(\alpha, \pi^m\beta)$.*

Proof. Let R_1, R_2 be two points introduced in 7.2. It then follows from Lemma 7.3, Remark 7.6 and formula (15) that $\delta(R_1) = (1, \alpha)$ and $\delta(R_2) = (\alpha, \pi^m\beta)$, as required. □

Proposition 9.6 *We have*

$$ {}_2\mathrm{Br}\, E = {}_2\mathrm{Br}\, K \oplus \{0, B_\pi, C_\pi, B_\pi + C_\pi\} \; . $$

Proof. The subgroup generated by the pairs $(\pi, 1)$ and $(1, \pi)$ complements $\delta(E(K)/2)$, so the result follows. □

9.4 *Split multiplicative reduction*

We may assume that E is given by a minimal equation of the form

$$ y^2 = x(x + \pi^m\beta)(x + 1). $$

Lemma 9.7 *$\delta(E(K)/2)$ is generated by the pairs $(1, \alpha)$ and $(1, \pi)$.*

Proof. As above, we have $\delta(R_1) = (1, \alpha)$. Further, it follows from the construction that the abscissa of the point $R_2 = (u, v)$ is of the form $u = \pi d$. So applying formula (15), we obtain that $\delta(R_2) = (1, \pi u + \pi^m\beta)$. But $|\delta(E(K)/2)| = 4$, whence $v(\pi u + \pi^m\beta)$ is odd and the result follows. □

Proposition 9.8 *We have*

$$ {}_2\mathrm{Br}\, E = {}_2\mathrm{Br}\, K \oplus \{0,\, B_\alpha,\, B_\pi,\, B_{\alpha\pi}\} \; . $$

Proof. This follows from the fact that the subgroup generated by the pairs $(\alpha, 1)$ and $(\pi, 1)$ complements $\delta(E(K)/2)$. □

10 *Computing ${}_2\mathrm{Br}\, E$ over non-dyadic local fields: semisplit case*

We keep the notation introduced in Section 8. Assume that E is given by a minimal equation of the form (13). Then $E(K)/2$ and $H^1(\Gamma, M)$ are groups of order 2 and 4 respectively, so that $\delta(E(K)/2)$ can be complemented inside $H^1(\Gamma, M)$ by a single element. We will find such an element among elements $\mathrm{cor}\,(H^1(\Lambda, M))$. Recall that δ_L denotes the homomorphism $E(L)/2 \hookrightarrow H^1(\Lambda, M)$.

Lemma 10.1 *Let $\theta \in H^1(\Lambda, M)$ satisfies the condition $(\mathrm{res} \circ \mathrm{cor})\,(\theta) \notin (\delta_L \circ \mathrm{res})\,(E(K)/2)$. Then $\mathrm{cor}\,(\theta)$ complements $\delta\,(E(K)/2)$.*

Proof. By our assumption,

$$\mathrm{res}\,(\mathrm{cor}\,(\theta)) \notin (\delta_L \circ \mathrm{res})\,(E(K)/2) = (\mathrm{res} \circ \delta)\,(E(K)/2)\ ,$$

so that $\mathrm{cor}\,(\theta)$ does not lie in $\delta(E(K)/2)$. □

Let α_L and π_L be a non-square unit and a uniformizer of the integer ring $\mathcal{O}_L$ of $L = K(\sqrt{d})$ respectively.

10.1 *Good Reduction*

Proposition 10.2 ${}_2\mathrm{Br}\,E = {}_2\mathrm{Br}\,K \oplus \{0,\ [\pi, x - a]\}$.

Proof. Clearly, $(\delta_L \circ res)\,(E(K)/2)$ belongs to the unramified part of $H^1(\Lambda, M) \cong L^*/L^{*2} \oplus L^*/L^{*2}$. Since we have good reduction, d is a unit, whence $\pi_L = \pi$. We put $\theta = (1, \pi)$. The equation $(\mathrm{res} \circ \mathrm{cor})(\theta) = (\pi, \pi)$ shows that θ satisfies the condition of Lemma 10.1. It then follows from Theorem 4.12 that ${}_2\mathrm{Br}\,E$ is generated by ${}_2\mathrm{Br}\,K$ and

$$(\mathrm{cor} \circ \epsilon_L)\,[1, \pi] = \mathrm{cor}\,[\pi, x + \sqrt{d}] = [\pi, x^2 - d] = [\pi, x - a].$$

□

10.2 *Additive reduction*

Proposition 10.3 (1) *In cases* (A1) *and* (A3) *we have*

$${}_2\mathrm{Br}\,E = {}_2\mathrm{Br}\,K \oplus \{0,\ \mathrm{cor}\,[\alpha_L, x - \sqrt{d}]\}.$$

(2) *In case* (A2) *we have*

$${}_2\mathrm{Br}\,E = {}_2\mathrm{Br}\,K \oplus \{0,\ \mathrm{cor}\,[\pi_L, x - \sqrt{d}]\}.$$

Proof. It suffices to note that, by Lemma 8.3, in the first (resp. second) case the pair $\theta = (1, \alpha_L)$ (resp. $\theta = (1, \pi_L)$) satisfies the condition of Lemma 10.1. □

10.3 *Multiplicative Reduction*

Proposition 10.4 *In case* (M1) *we have*

$${}_2\mathrm{Br}\,E = {}_2\mathrm{Br}\,K \oplus \{0,\ \mathrm{cor}\,[\pi_L, x - \sqrt{d}]\}.$$

and in case (M2) *we have*

$${}_2\mathrm{Br}\,E = {}_2\mathrm{Br}\,K \oplus \{0,\ \mathrm{cor}\,[\alpha_L, x - \sqrt{d}]\}\ .$$

Proof. Denote a representative of a unique nontrivial element in $E(K)/2E(K)$ by R. Consider first case (M1). Let L^{nr} be a maximal unramified extension of L. According to Proposition 8.1 we have $\eta(R) = R_1 + 2E(L)$. Since, by construction, $R_1 \in E_0(L)$ and $E_0(L^{nr})/2E_0(L^{nr}) = 0$ (see [Sil85], p. 187), it follows that $\delta_L(\eta(R))$ belongs to the unramified part of the group $H^1(\Lambda, M) \cong L^*/L^{*2} \oplus L^*/L^{*2}$. Therefore one can take $\theta = (1, \pi_L)$ and the result follows.
In case (M2) we have $\eta(R) = R_2 + 2E(L)$. Since $v(d)$ is even, the extension L/K is unramified and E_L has split multiplicative reduction. We know that the abscissa u of R_2 is of the form $u = \pi u'$, so that $\delta_L(R_2) = (\pi u' + \sqrt{d}, \pi u' - \sqrt{d})$. It is easy to make sure that $v(\pi u' + \sqrt{d})$ is odd. Then $\theta = (1, \alpha_L)$ satisfies the condition of Lemma 10.1 and the result follows. □

References

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

[CEP71] Cassels J., Ellison W., Pfister A.: *On sums of squares and on elliptic curves over function fields.* J. of Number Theory 3, 125 – 149 (1971)

[CG00] Chernousov V., Guletskiĭ V.: 2*-torsion of the Brauer group of an elliptic curve: generators and relations.* Preprint 00 – 37, Universität Bielefeld (2000)

[Co88] Colliot-Thélène, J.-L. (with the collaboration of Sansuc, J.-J.): *The rationality problem for fields of invariants under linear algebraic groups (with special regard to the Brauer group),* Unpublished Lecture Notes from the 9th ELAM: Santiago de Chile 1988

[CSS98] Colliot-Thélène, J.-L., Skorobogatov A., Swinnerton-Dyer P.: *Hasse principle for pencils of curves of genus one whose Jacobians have rational* 2*-division points.* Invent. math. 134, 579 – 650 (1998)

[Fadd51] Faddeev, D. K.: *Simple algebras over a function field in one variable,* Proc. Steklov Inst. 38, 321 – 344 (1951); English transl. in AMS Transl. 3, 15 – 38 (1956)

[G99] Guletskiĭ, V.: *Algebras of Exponent 2 over an Elliptic Curve.* Preprint 99 – 112, Universität Bielefeld (1999)

[GMY97] Guletskiĭ, V., Margolin, G., Yanchevskiĭ V.: *Presentation of two-torsion part in Brauer groups of curves by quaternion algebras* (in Russian). Dokl. NANB. 41, no. 6, 4–8 (1997)

[Hu87] Husemöller, D.: *Elliptic Curves*, Berlin Heidelberg New York: Springer 1987

[LT58] Lang, S., Tate, J.: *Principal homogeneous spaces over abelian varieties.* Amer. J. of Math. 80, 659 – 684 (1958)

[L56] Lang, S.: *Algebraic groups over finite fields.* Amer. J. of Math. 78, 555 – 563 (1956)

[Lich69] Lichtenbaum, S.: *Duality Theorems for Curves over P-adic Fields.* Invent. Math. 7, 120 – 136 (1969)

[Mi81] Milne, J.S.: *Comparison of the Brauer group with the Tate-Šafarevič group.* J. Fac. Science, Univ. Tokyo, Sec. IA 28, 735–743 (1981)

[Mi86] Milne, J.S.: *Arithmetics Duality Theorems.* Progress in Math. Vol. 1.: Academic Press 1986

[P82] Pierce, R.S.: *Associative algebras.* Graduate Texts in Mathematics 88: Springer-Verlag 1982

[Pu98] Pumplün, S.: *Quaternion algebras over elliptic curves.* Comm. Algebra 26, no. 12, 4357–4373 (1998)

[Sch69] Scharlau, W.: *Über bie Brauer-Gruppe eines algebraischen Funktionen-körpers in einer Variabein.* J. für die reine und angew. Math. 239/240, 1–6 (1969)

[Serre64] Serre, J.-P.: *Cohomologie Galoisienne,* Berlin Heidelberg New York: Springer-Verlag 1964

[Serre79] Serre, J.-P.: *Local Fields,* New York Heidelberg Berlin: Springer-Verlag 1979

[Sil85] Silverman, J.: *The Arithmetic of Elliptic Curves,* Berlin Heidelberg New York: Springer-Verlag 1985

[S99] Skorobogatov A.: *Beyond the Manin obstruction.* Invent. math. 135, 399–424 (1999)

[Tate57] Tate, J.: *WC-groups over $\mathfrak{p}$-adic fields.* Séminaire Bourbaki, Décembre 1957, no. 1556

[YM96] Yanchevskiĭ, V., Margolin G.: *The Brauer groups and the torsion of local elliptic curves.* St. Petersburg Math. J. 7, no. 3, 473–505 (1996)

V. Chernousov
Fakultät für Mathematik
Universität Bielefeld
Postfach 100131
33615 Bielefeld
Germany
chernous@mathematik.uni-bielefeld.de

V. Guletskiĭ
Institute of Mathematics
Surganova str. 11
220072 Minsk, Belarus
guletskii@im.bas-net.by