# Contents


**1 Introduction** **2**

**2 Preliminary results** **4**
2.1 *Short exact sequences* . . . 4
2.2 *Local invariants* . . . 5
2.3 *Principle homogeneous spaces* . . . 5
2.4 *Torsion* . . . 7
2.5 *The plane of computations* . . . 7

**3 Calculus of cocycles** **7**
3.1 *Starting lemmas* . . . 8
3.2 *Formula for cocycles* . . . 8
3.3 *Classification of cocycles* . . . 10
3.4 *Direct calculations of cocycles* . . . 10
3.5 $\delta$ *on cocycles* . . . 12

**4 Quaternion and cyclic algebras** **13**
4.1 *Algebras corresponding to cocyles of type I* . . . 13
4.2 $\delta$ *for cocycles of type II* . . . 13
4.3 *Cross products corresponding to cocycles of type II* . . . 14
4.4 *Cyclic algebras of degree* 4 . . . 16

**5 Dihedral algebras** **18**
5.1 $\delta$ *for cocycles of type III* . . . 18
5.2 *Dihedral cross products* . . . 20
5.3 *End of the proof* . . . 21

# Algebras of exponent 2 over an elliptic curve

V.Guletskiĭ

November 15, 1999

## 1 Introduction

Let $k$ be a field, $char(k) \neq 2, 3$, and let $X$ be a smooth projective geometrically integral curve over $k$. Assume that $X$ has at least one point rational over $k$. Let $k(X)$ be the field of $k$-rational functions on $X$. The Brauer group $\mathrm{Br}(X)$ of $X$ is naturally isomorphic to the unramified Brauer group $\mathrm{Br}_{nr}(k(X)/k)$ of $k(X)/k$ (see [Lich69], [Co88]). This allows to identify $\mathrm{Br}(X)$ with $\mathrm{Br}_{nr}(k(X)/k)$. Denote by $J$ the Jacobian variety of the curve $X$. In [GMY97] the description of the 2-torsion part in $\mathrm{Br}(X)$ in terms of quaternion algebras was made under the condition of $k$-rationality of the 2-torsion subgroup of $J$. In [GY98] this result was generated on algebras of an arbitrary exponent $n$: if all points of order $n$ on $J$ are rational over $k$, then any element of order $n$ in $\mathrm{Br}(X)$ can be presented by a tensor product of cyclic algebras depending on the $n$-torsion subgroup of $J$.

Let $X = E$ be an elliptic curve over $k$. In this paper we consider the problem of a description of 2-torsion part in $\mathrm{Br}(E)$ in the case when $E$ has only one $k$-rational point of order 2 on the Jacobian $E$. Our arguments based on an explicit computation of 1-cocycles presenting elements of order 2 in the group of homogeneous spaces over $E$ and a construction of a section for some divisor mapping induced by the 2-torsion subgroup of $E$.

It should be mentioned that in [YM96], [VY96] and [V97] a complete description of the 2-torsion in $\mathrm{Br}(E)$ was made in the case of a local field $k$ and all proofs there heavily use the completeness property of the ground field $k$. In contrast to this we present a different approach which is mainly based on cohomology methods and allows to consider an arbitrary ground field $k$, $char(k) \neq 2, 3$. On the other hand we do not answer the questions about triviality and indices of algebras of exponent 2 in $\mathrm{Br}(E)$.

Since the characteristic of the ground field $k$ is not 2 or 3, the elliptic curve $E$ can be defined as the projective closure of a plane curve defined by an equation

$$y^2 = F(x) \ ,$$

where $F(x)$ is a cubic polynomial over $k$ with the leading coefficient equal to 1 without multiple roots in a separable closure $\bar{k}$ of $k$. Let $\bar{E} = E(\bar{k})$ be the group of geometric points on $E$ and let ${}_2\bar{E} = \{O, P, T, S\}$ be the 2-torsion subgroup of $\bar{E}$. Here $O$ is the infinite point on $E$ playing the rule of zero on the curve $E$. Let $x_P$, $x_T$, $x_S$ be the $x$-coordinates of the points $P$, $T$, $S$ respectively. Then we have the decomposition

$$F(x) = (x - x_P)(x - x_T)(x - x_S)$$

over $\bar{k}$. We say that $E$ is *split* if all 2-torsion points are rational over $k$. This is equivalent to the condition that all roots $x_P$, $x_T$, $x_S$ of the polynomial $F(x)$ lie in $k$. We say that $E$ is *semisplit* if there exists only one $k$-point in ${}_2\bar{E}$ denoted below by $P$. In other words, only one root $x_P$ of $F(x)$ is $k$-rational. If all non-trivial points in ${}_2\bar{E}$ are not $k$-rational, then we say that $E$ is *fully non-split.*

In the split case it is not hard to compute quaternion algebras generating ${}_2\mathrm{Br}(E)$. Recall the result of [GY98] for the group ${}_2\mathrm{Br}(E)$. Let $E$ be split. Fix any two non-trivial 2-torsion points on $\bar{E}$, for example $P$ and $T$. Then any unramified central simple algebra of exponent 2 over $k(E)$ similar to a tensor product

$$A \otimes (b, x - x_P) \otimes (c, x - x_T) \ .$$

Here $A$ is a *numerical* algebra over $k(E)$, i.e. an algebra obtained by the scalar extension of some algebra with the center $k$. The algebras $(b, x - x_P)$, $(c, x - x_T)$ are quaternion algebras over $k(E)$ with $b, c \in k^*$. Note that $(b, x - x_P)$ or $(c, x - x_T)$ can be trivial in $\mathrm{Br}(E)$. For example, if $b$ is a square in $k$ then $(b, x - x_P)$ is zero in $\mathrm{Br}(E)$.

If $E$ is fully nonsplit, then the problem of finding of all unramified central simple algebras of exponent 2 over $k(E)$ can be reduced to either a split or semisplit case. Indeed, fully nonsplitness means that $F$ is an irreducible polynomial over $k$. Then the extension $L = k(x_T)$ has degree 3 over $k$. Let $E_L = E \times \mathrm{Spec}(L)$. The composition

$$\mathrm{Br}(E) \xrightarrow{\mathrm{res}} \mathrm{Br}(E_L) \xrightarrow{\mathrm{cor}} \mathrm{Br}(E)$$

coincides with the multiplication-by-3 homomorphism on the group $\mathrm{Br}(E)$. So keeping in mind that 2 and 3 are relatively prime we get that the corestriction map

$$\mathrm{cor} : {}_2\mathrm{Br}(E_L) \longrightarrow {}_2\mathrm{Br}(E)$$

is surjective. Hence one can find algebras in ${}_2\mathrm{Br}(E)$ applying cor to algebras from ${}_2\mathrm{Br}(E_L)$.

Thus we see that the main situation is when ${}_2\mathrm{Br}(E)$ has only one non-trivial point $P$ defined over $k$. In this case

$$F(x) = (x - x_P) f(x) \tag{1}$$

where $f(x)$ is an irreducible quadratic polynomial over $k$.

Let $G = \mathrm{Gal}(\bar{k}/k)$ be the absolute Galois group of the ground field $k$, $L = k(x_T) = k(x_S)$ and $H = \mathrm{Gal}(\bar{k}/L)$. Let $U$ be a subgroup of index 2 in $H$ and $Z = \bar{k}^U$. If $U$ is normal in $G$ and $G/U$ is a cyclic group of order 4, then there exists a cyclic algebra $(Z \cdot k(E)/k(E), f(x))$ over $k(E)$, where the quadratic polynomial $f(x)$ is considered as a rational function on $E$. If $U$ is not normal in $G$ (this is equivalent to the existing of an element $g_0 \in G \backslash H$ such that $U \neq g_0^{-1} U g_0$) then one can construct a special central simple algebra $B_U$ over $k(E)$ (see Section 5.2 below), which is a cross product defined by a 2-cocycle in an explicit form. We prove the following theorem, which is the main result of this paper.

**Theorem 1.0.1** *Let $k$ be a field, $char(k) \neq 2, 3$, and let $E$ be a semisplit elliptic curve over $k$. Then any element of order 2 in the quotient group $\mathrm{Br}(E)/\mathrm{Br}(k)$ is similar to a simple algebra of one of the following three types:*

*(i)*

$$(a, x - x_P) \ ,$$

*where $(a, x - x_P)$ is a quaternion algebra over $k(E)$ with $a \in k^*$;*

*(ii)*

$$(Z \cdot k(E)/k(E), f(x)) \ ,$$

*where $(Z \cdot k(E)/k(E), f(x))$ is a cyclic algebra over $k(E)$ generated by a cyclic extension $Z/k$ of degree 4 over $k$ such that $L \subset Z$ and the polynomial $f$ is defined by (1) and is viewed as a $k$-rational function on $E$;*

*(iii) an algebra $B_U$, which is defined in Section 5.2 by a 2-cocycle in an explicit form.*

Note that the direct computation (see Proposition 5.2.1 below) shows that the algebra $B_U$ from (iii) has index at most 4. This agrees with the results of Van den Bergh (see [1], Prop. 1, p. 196) and implies that $B_U$ is similar to either a quaternion or biquaternion algebra over $k(E)$. After the paper was finished V. Chernousov inform me that $B_U$ can be decomposed in a tensor product of two explicit quaternion algebras determined by $f(x)$ and the subgroup $U$. The correspoding theorem can be formulated in the following way:

**Theorem 1.0.2** *Let $k$ be a field, char$(k) \neq 2, 3$, and $E$ be a semisplit elliptic curve over $k$. Without loss of generality the curve $E$ can be defined by the equation $y^2 = (x-p)(x^2-a)$, where $p, a \in k$ and $a$ is not a square in $k$ (hence $f(x) = x^2 - a$ and $L = k(\sqrt{a})$). Let $B_U$ be the algebra from (iii) of Theorem 1.0.1 and $b = u + v\sqrt{a}$ an element in $L$ such that $\bar{k}^U = L(\sqrt{b})$. Then $B_U$ is similar to the tensor product*

$$(v, u^2 - v^2 a) \otimes (vx + u, (u^2 - v^2 a)(x^2 - a)) \ ,$$

*where $(v, u^2 - v^2 a)$ is the numerical quaternion algebra defined by the two constants $v, u^2 - v^2 a \in k \subset k(E)$ and $(vx + u, (u^2 - v^2 a)(x^2 - a))$ is the quaternion algebra defined by the functions $vx + u, (u^2 - v^2 a)(x^2 - a) \in k(E)$.*


*Acknowledgements*

This work was supported by the Institute of Mathematics of the Academy of Sciences of Belarus and TMR ERB FMRX CT-97-0107. The author thanks Vladimir Chernousov for useful discussions.


*Notations*

Symbols $\mathbb{Z}$, $\mathbb{Q}$ denotes integers and rational numbers respectively. If $A$ is an abelian group and $n$ is a natural number, then $n : A \to A$ denotes the homomorphism of multiplication by $n$ and ${}_nA$, $A/n$ are its kernel and cokernel respectively. For any finite set $S$ we denote the number of elements in $S$ by $\#S$. If $H$ is a group, $U$ its normal subgroup and $x \in H$, we denote the left coset $xU$ by $\overline{x}$. $F^*$ denotes the multiplicative group of a field $F$. Variety is always smooth projective and geometrically integral scheme over $k$. For any variety $X$ over $k$ and for any field extension $L/k$ let $X(L)$ be the set of $L$-points on $X$ and let $\bar{X} = X(\bar{k})$ be the set of geometrical points on $X$. A curve is a variety of dimension one. A point of a curve means closed point. We denote an arbitrary curve by $X$. An elliptic curve will be always denoted by $E$.

# 2 Preliminary results

In this section we recall some well-known facts used below. All of them can be found in [Fadd51], [Mi81] and [Sch69].

## 2.1 *Short exact sequences*

Let $G = \mathrm{Gal}(\bar{k}/k)$ be the absolute Galois group of the ground field $k$, $X$ a curve of an arbitrary genus defined over $k$ such that $X(k) \neq \emptyset$ and let $\bar{k}(\bar{X})$ be the field of $\bar{k}$-rational functions on $\bar{X}$. One can associate with the curve $X$ the following discrete (left) $G$-modules: $\mathrm{Div}(\bar{X})$ is the divisor group of $\bar{X}$; $\mathrm{Div}^0(\bar{X})$ is its subgroup of degree zero divisors on $\bar{X}$; $\mathrm{P}(\bar{X})$ is the subgroup of principles divisors; $\mathrm{Pic}(\bar{X}) = \mathrm{Div}(\bar{X})/\mathrm{P}(\bar{X})$ and $\mathrm{Pic}^0(\bar{X}) = \mathrm{Div}^0(\bar{X})/\mathrm{P}(\bar{X})$. These $G$-modules are terms of the following short exact sequences

$$1 \to \bar{k}^* \longrightarrow \bar{k}(\bar{X})^* \xrightarrow{\mathrm{div}} \mathrm{P}(\bar{X}) \to 0 \ , \tag{2}$$

$$0 \to \mathrm{P}(\bar{X}) \longrightarrow \mathrm{Div}(\bar{X}) \longrightarrow \mathrm{Pic}(\bar{X}) \to 0 \ , \tag{3}$$

$$0 \to \mathrm{Pic}^0(\bar{X}) \longrightarrow \mathrm{Pic}(\bar{X}) \xrightarrow{\deg} \mathbb{Z} \to 0 \ . \tag{4}$$

Here deg is the degree homomorphism and div is the homomorphism sending $f \in \bar{k}(\bar{X})^*$ into the divisor $\mathrm{div}(f)$ of zeros and poles of the rational function $f$. Let $\bar{J}$ be the group of $\bar{k}$-points of the Jacobian variety $J$ of the curve $X$. Since we suppose that $X$ has at least one $k$-rational point, $\bar{J}$ and $\mathrm{Pic}^0(\bar{X})$ are isomorphic as discrete $G$-modules. Therefore we have the short exact sequence

$$0 \to \mathrm{P}(\bar{X}) \longrightarrow \mathrm{Div}^0(\bar{X}) \xrightarrow{\mathrm{sum}} \bar{J} \to 0 \ . \tag{5}$$

## 2.2 *Local invariants*

Denote the set of closed points on $X$ (i.e. the set of points of codimension 1 on $X$) by $X^{(1)}$. All such points $x \in X^{(1)}$ are in one-to-one correspondence with discrete valuations rings of the field $k(X)$ over $k$. Let $k(X)_x$ be the completion of $k(X)$ with respect to the valuation corresponding to a point $x \in X^{(1)}$. Denote by $k(x)$ the residue field of $X$ in $x$. Then $[k(x) : k] < \infty$ and one can identify $k(x)$ with a subfield in $\bar{k}$. Let $G_x = \mathrm{Gal}(\bar{k}/k(x))$ for any $x \in X^{(1)}$. Then $\mathrm{Br}(k(X)_x)$ is isomorphic to the direct sum of the Brauer group $\mathrm{Br}(k(x))$ and the group $\mathrm{Hom}_{cont}(G_x, \mathbb{Q}/\mathbb{Z})$ of continuous homomorphisms of the profinite group $G_x$ into the discrete group $\mathbb{Q}/\mathbb{Z}$. Let

$$\mathrm{inv}_x : \mathrm{Br}(k(X)) \longrightarrow \mathrm{Hom}_{cont}(G_x, \mathbb{Q}/\mathbb{Z})$$

be the composition of the scalar extension homomorphism

$$\mathrm{Br}(k(X)) \longrightarrow \mathrm{Br}(k(X)_x)$$

and the projection

$$\mathrm{Br}(k(X)_x) \cong \mathrm{Br}(k(x)) \oplus \mathrm{Hom}_{cont}(G_x, \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}_{cont}(G_x, \mathbb{Q}/\mathbb{Z}) .$$

The homomorphism $\mathrm{inv}_x$ maps a class of algebras $a \in \mathrm{Br}(k(X))$ into its *local invariant* $\mathrm{inv}_x(a)$. The order of $\mathrm{inv}_x(a)$ coincides with the ramification index of algebras from $a$ at the point $x \in X^{(1)}$. Algebras can be ramified only in a finite number of points. Hence one can construct the homomorphism

$$\mathrm{inv} : \mathrm{Br}(k(X)) \longrightarrow \bigoplus_{x \in X^{(1)}} \mathrm{Hom}_{cont}(G_x, \mathbb{Q}/\mathbb{Z}) .$$

By definition, its kernel is *unramified Brauer group* $\mathrm{Br}_{nr}(k(X))$ of $k(X)/k$. As it was mentioned in the beginning, the group $\mathrm{Br}_{nr}(k(X))$ can be naturally identified with the Brauer group $\mathrm{Br}(X)$ of the curve $X$.

Recall the cohomology description of the homomorphism inv. Below $H^*(G, ?)$ is the Galois cohomology functor on the category of (left) discrete $G$-modules. By Tsen theorem, the group $\mathrm{Br}(k(X))$ is isomorphic to the cohomology group $H^2(G, \bar{k}(\bar{X})^*)$. Let $M_x$ be a sumbmodule in $\mathrm{Div}(\bar{X})$ generated by points in $\bar{X}$ mapping into $x \in X^{(1)}$ under the natural projection $\bar{X} \to X$. The discrete $G$-module $M_x$ is identified with the induced $G$-module $M_G^{G_x}(\mathbb{Z})$, where $\mathbb{Z}$ is viewed as a trivial $G$-module. Then $\mathrm{Div}(\bar{X}) \cong \bigoplus_x M_G^{G_x}(\mathbb{Z})$, where $x$ runs all points in $X^{(1)}$. Thus we get

$$H^2(G, \mathrm{Div}(\bar{X})) \cong \bigoplus_x H^2(G, M_G^{G_x}(\mathbb{Z})) \cong \bigoplus_x H^2(G_x, \mathbb{Z}) \cong \bigoplus_x \mathrm{Hom}_{cont}(G_x, \mathbb{Q}/\mathbb{Z}) .$$

It can be proven that the composition

$$\mathrm{Br}(k(X)) \cong H^2(G, \bar{k}(\bar{X})^*) \xrightarrow{\mathrm{div}^*} H^2(G, \mathrm{Div}(\bar{X})) \cong \bigoplus_x \mathrm{Hom}_{cont}(G_x, \mathbb{Q}/\mathbb{Z})$$

coincides with the homomorphism inv. Here $\mathrm{div}^*$ is the homomorphism induced by div on cohomology groups. Therefore,

$$\mathrm{Br}(X) \cong \ker(\mathrm{div}^*) .$$

## 2.3 *Principle homogeneous spaces*

Consider the exact sequence

$$H^2(G, \bar{k}^*) \to H^2(G, \bar{k}(\bar{X})^*) \xrightarrow{\alpha} H^2(G, \mathrm{P}(\bar{X})) \to H^3(G, \bar{k}^*) \to H^3(G, \bar{k}(\bar{X})^*)$$

induced by (2). Since $X(k) \neq \emptyset$, the left and right homomorphisms are injective for any $n$ (see [Sch69]). Hence we have the short exact sequence

$$0 \to H^2(G, \bar{k}^*) \longrightarrow H^2(G, \bar{k}(\bar{X})^*) \xrightarrow{\alpha} H^2(G, \mathrm{P}(\bar{X})) \to 0 .$$

Taking into account the isomorphisms $H^2(G,\bar{k}^*) \cong \mathrm{Br}(k)$ and $H^2(G,\bar{k}(\bar{X})^*) \cong \mathrm{Br}(k(X))$, one can obtain the exact sequence

$$0 \to \mathrm{Br}(k) \xrightarrow{\iota} \mathrm{Br}(k(X)) \xrightarrow{\alpha} H^2(G,\mathrm{P}(\bar{X})) \to 0\ ,$$

where $\iota$ is induced by the scalar extension: if $A$ is a simple algebra with the center $k$, then $\iota([A]) = [A \otimes_k k(X)]$.

Now observe that $\mathrm{div}^* = \beta \circ \alpha$, where $H^2(G,\mathrm{P}(\bar{X})) \xrightarrow{\beta} H^2(G,\mathrm{Div}(\bar{X}))$ is the homomorphism induced by the embedding $\mathrm{P}(\bar{X}) \subset \mathrm{Div}(\bar{X})$. Since $\alpha$ is surjective, one has $\ker(\mathrm{div}^*) = \alpha^{-1}(\ker(\beta))$. Consider the exact sequence

$$H^1(G,\mathrm{Pic}(\bar{X})) \xrightarrow{\Delta} H^2(G,\mathrm{P}(\bar{X})) \xrightarrow{\beta} H^2(G,\mathrm{Div}(\bar{X}))$$

induced by (3). It follows that $\ker(\mathrm{div}^*) = \alpha^{-1}(\mathrm{im}(\Delta))$. Furthermore, consider the exact sequence

$$\mathrm{Pic}(\bar{X})^G \xrightarrow{\deg} \mathbb{Z} \to H^1(G,\mathrm{Pic}^0(\bar{X})) \to H^1(G,\mathrm{Pic}(\bar{X})) \to 0$$

induced by (4). Here $\mathrm{Pic}(\bar{X})^G$ is the group of divisor classes invariant under the action of $G$. The last sequence is ended by zero because $H^1(G,\mathbb{Z}) = 0$. Since $X(k) \neq \emptyset$, the homomorphism deg is surjective, hence the epimorphism $H^1(G,\mathrm{Pic}^0(\bar{X})) \to H^1(G,\mathrm{Pic}(\bar{X}))$ is injective. Thus we have that

$$H^1(G,\mathrm{Pic}(\bar{X})) \cong H^1(G,\mathrm{Pic}^0(\bar{X})) \cong H^1(G,\bar{J})\ .$$

Then

$$\ker(\mathrm{div}^*) = \alpha^{-1}(\mathrm{im}(\delta))\ ,$$

where $\delta : H^1(G,\bar{J}) \to H^2(G,\mathrm{P}(\bar{X}))$ is the connecting homomorphism induced by (5). Note that the condition $H^1(G_x,\mathbb{Z}) = 0$ implies that $H^1(G,\mathrm{Div}(\bar{X})) = 0$. Then the exact sequence induced by (3) yields that the connecting homomorphism $\Delta$ is injective. Hence $\delta$ is injective too. Let

$$\delta^{-1} : \mathrm{im}(\delta) \to H^1(G,\bar{J})$$

be the inverse to the isomorphism $\delta : H^1(G,\bar{J}) \to \mathrm{im}(\delta)$. Define $\pi$ as the composition

$$\pi : \mathrm{Br}(X) \cong \ker(\mathrm{div}^*) \xrightarrow{\alpha} \mathrm{im}(\delta) \xrightarrow{\delta^{-1}} H^1(G,\bar{J})\ . \tag{6}$$

The definition of $\pi$ can be illustrated by the following commutative diagram:

$$\begin{tikzcd}
 & & H^2(G,\mathrm{Div}^0(\bar{X})) \arrow[d, hook] \\
H^1(G,\bar{J}) \arrow[r, hook, "\delta"] & H^2(G,\mathrm{P}(\bar{X})) \arrow[r, "\beta"'] \arrow[ur] & H^2(G,\mathrm{Div}(\bar{X})) \\
\ker(\mathrm{inv}) \arrow[u] \arrow[r, hook] & H^2(G,\bar{k}(\bar{X})^*) \arrow[u, two heads, "\alpha"'] \arrow[ur, "\mathrm{inv}"'] & \\
\mathrm{Br}(X) \arrow[u, "\cong"] \arrow[r, hook] & \mathrm{Br}(k(X)) \arrow[u, "\cong"] &
\end{tikzcd}$$

Now we have the exact sequence

$$0 \to \mathrm{Br}(k) \xrightarrow{\iota} \mathrm{Br}(X) \xrightarrow{\pi} H^1(G,\bar{J}) \to 0\ . \tag{7}$$

It splits. Indeed, if $x \in X(k)$, then $k(x) = k$ and $\mathrm{Br}(k(X)_x) \cong \mathrm{Br}(k) \oplus Hom_{cont}(G,\mathbb{Q}/\mathbb{Z})$. One can check that the composition

$$\mathrm{Br}(k) \to \mathrm{Br}(k(X)) \to \mathrm{Br}(k(X)_x) \to \mathrm{Br}(k) \oplus Hom_{cont}(G,\mathbb{Q}/\mathbb{Z}) \to \mathrm{Br}(k)$$

is an identical map. Hence $\iota$ has a left inverse.

## 2.4 *Torsion*

Let $n$ be a natural number. If $A \xrightarrow{\iota} B$ is a homomorphism of abelian groups, then denote by ${}_nA \xrightarrow{{}_n\iota} {}_nB$ and $A/n \xrightarrow{\iota/n} B/n$ the homomorphisms induced by $\iota$. The sequence (7) induces the exact sequence

$$0 \to {}_n\mathrm{Br}(k) \xrightarrow{{}_n\iota} {}_n\mathrm{Br}(X) \xrightarrow{{}_n\pi} {}_nH^1(G, \bar{J}) \to \mathrm{Br}(k)/n \xrightarrow{\iota/n} \mathrm{Br}(X)/n \xrightarrow{\pi/n} H^1(G, \bar{J})/n \to 0\ .$$

If $\hat{\iota}$ is a left inverse to $\iota$, then $\hat{\iota}/n$ is a left inverse to $\iota/n$. Therefore $\iota/n$ is injective. Then the last exact sequence yields the short exact sequence

$$0 \to {}_n\mathrm{Br}(k) \xrightarrow{{}_n\iota} {}_n\mathrm{Br}(X) \xrightarrow{{}_n\pi} {}_nH^1(G, \bar{J}) \to 0\ .$$

We shall use the following simple

**Lemma 2.4.1** *Let $0 \to A \xrightarrow{\iota} B \xrightarrow{\pi} C \to 0$ be an exact sequence. Suppose that the homomorphism $\iota$ has a left inverse $\hat{\iota} : B \to C$. For any $c \in C$ choose $b_c \in \pi^{-1}(c)$. Then any element $b \in B$ has the unique decomposition $b = b_c + \iota(a)$, where $c = \pi(b) \in C$ and $a = \iota^{-1}(b - b_c)$. The map $\hat{\pi} : C \to B$, $c \mapsto b_c - \iota\hat{\iota}(b_c)$ is a right inverse homomorphism of $\pi$.*

## 2.5 *The plane of computations*

Now let $X = E$ be an elliptic curve over $k$. Then $\bar{J} = \bar{E}$ and there exists the split exact sequence

$$0 \to {}_2\mathrm{Br}(k) \xrightarrow{{}_2\iota} {}_2\mathrm{Br}(E) \xrightarrow{{}_2\pi} {}_2H^1(G, \bar{E}) \to 0\ .$$

For every cohomology class $c \in {}_2H^1(G, \bar{E})$ we want to choose a Brauer class $b_c \in {}_2\mathrm{Br}(E)$ such that ${}_2\pi(b_c) = c$. We shall describe classes $c \in {}_2H^1(G, \bar{E})$ in terms of explicit cocycles (Section 3). After that we construct central simple algebras representing the Brauer classes $b_c$ in $\mathrm{Br}(E)$ (Sections 4 and 5). Since by Lemma 2.4.1 any element $b \in {}_2\mathrm{Br}(E)$ has a unique decomposition $b = {}_2\iota(a) + b_c$, where $a \in {}_2\mathrm{Br}(k)$ and $c \in {}_2H^1(G, \bar{E})$, we get that a full description of 2-torsion part of $\mathrm{Br}(E)/\mathrm{Br}(k)$ is given by central simple algebras representing classes $b_c$.

The Kummer sequence

$$0 \to {}_2\bar{E} \longrightarrow \bar{E} \xrightarrow{2} \bar{E} \to 0 \tag{8}$$

yields the exact sequence

$$0 \to E(k)/2 \longrightarrow H^1(G, {}_2\bar{E}) \longrightarrow {}_2H^1(G, \bar{E}) \to 0\ . \tag{9}$$

It follows that any element in ${}_2H^1(G, \bar{E})$ can be presented by a cocycle $\phi : G \to {}_2\bar{E}$ of the group $G$ with coefficients in ${}_2\bar{E}$. Moreover, the cohomology class $\mathrm{cls}(\phi) \in {}_2H^1(G, \bar{E})$ is trivial iff the cohomology class $\mathrm{cls}(\phi) \in H^1(G, {}_2\bar{E})$ lies in the image of the embedding $E(k)/2 \hookrightarrow H^1(G, {}_2\bar{E})$. This suggests that firstly we need to describe all 1-cocycles of the group $G$ with coefficients in ${}_2\bar{E}$. It will provide the description of ${}_2H^1(G, \bar{E})$ in terms of explicit 1-cocycles of the group $G$ with coefficients in ${}_2\bar{E}$.

# 3 Calculus of cocycles

Let $E$ be a semisplit elliptic curve and let $\{O, P\}$ be the group $k$-rational 2-torsion points on $E$. Then $F(x) = (x - x_P)f(x)$, where $f(x)$ is an irreducible quadratic polynomial over $k$. If ${}_2E = \{O, P, T, S\}$ is the group of all 2-torsion points on $\bar{E}$ then $f(x) = (x - x_T)(x - x_S)$ over $\bar{k}$. Let $L/k$ be the minimal subextension in $\bar{k}/k$ such that all 2-torsion points of $E$ are rational over $L$, i.e. $L = k(x_T) = k(x_S)$. The group $H = \mathrm{Gal}(\bar{k}/L)$ has index 2 in $G$.

## 3.1 *Starting lemmas*

Consider the exact sequence

$$0 \to H^1(G/H,\, {}_2\bar{E}) \xrightarrow{\text{inf}} H^1(G,\, {}_2\bar{E}) \xrightarrow{\text{inf}} H^1(H,\, {}_2\bar{E})^{G/H} \longrightarrow H^2(G/H,\, {}_2\bar{E})$$

induced by the Hochschild-Serre spectral sequence $H^p(G/H, H^q(H,\, {}_2\bar{E})) \Rightarrow H^n(G,\, {}_2\bar{E})$ (see, for example, [Serre]). It is easy to show that $H^1(G/H,\, {}_2\bar{E}) = 0$ and $H^2(G/H,\, {}_2\bar{E}) = 0$. So we have the isomorphism

$$\text{res} : H^1(G,\, {}_2\bar{E}) \xrightarrow{\cong} H^1(H,\, {}_2\bar{E})^{G/H} . \tag{10}$$

Recall the action of $G/H$ on $H^1(H,\, {}_2\bar{E})$. Let $\psi \in H^1(H,\, {}_2\bar{E}) = Hom(H,\, {}_2\bar{E})$ and $g_0 \in G\backslash H$. Then $(g_0\psi)(g) = g_0(\psi(g_0^{-1}gg_0))$ for any $g \in G$. Note that this action does not depend on the choice of $g_0$ and we can consider the action of $g_0$ as an action of the unique non trivial element in $G/H$.

Now fix an isomorphism

$${}_2\bar{E} \cong \{O, T\} \oplus \{O, S\} .$$

Then

$$Hom(H,\, {}_2\bar{E}) \cong Hom(H, \{O, T\}) \oplus Hom(H, \{O, S\}) .$$

Let $(\psi_1, \psi_2)$ be an element in $Hom(H, \{O, T\}) \oplus Hom(H, \{O, S\})$ and $U_i = \ker(\psi_i)$, $i = 1, 2$. Then the pair $(\psi_1, \psi_2)$ lies in $(Hom(H, \{O, T\}) \oplus Hom(H, \{O, S\}))^{G/H}$ if and only if $U_2 = g_0^{-1}U_1g_0$ for some $g_0 \in G\backslash H$ (this condition does not depend on the choice of an element $g_0$ in $G\backslash H$). Therefore one can identify the set of nontrivial homomorphisms in $(Hom(H, \{O, T\}) \oplus Hom(H, \{O, S\}))^{G/H}$ with the set of subgroups $U$ of index two in $H$. A such $U$ corresponds to the homomorphism $\psi = \psi_T + \psi_S$, where $\psi_T$ is the surjective homomorphism $H \to \{O, T\}$ with the kernel $U$, and $\psi_S$ is the surjective homomorphism $H \to \{O, S\}$ with the kernel $g_0^{-1}Ug_0$.

**Lemma 3.1.1** *If $\phi : G \to {}_2\bar{E}$ is a cocycle, then $V = \ker(\phi|_H)$ is a normal subgroup in $G$.*

*Proof.* Isomorphism (10) shows that $\phi\,|_H$ is invariant under the action of $G/H$. Then either $V = H$ or $V = U \cap g_0^{-1}Ug_0$ for some subgroup $U$ of index 2 in $H$. In the second case $g_0^{-1}Vg_0 = g_0^{-1}(U \cap g_0^{-1}Ug_0)g_0 = g_0^{-1}Ug_0 \cap g_0^{-2}Ug_0^2 = g_0^{-1}Ug_0 \cap U = V$. For any element $g \in G$ one can write $g = hg_0$ for some $h \in H$. Then $g^{-1}Vg = g_0^{-1}h^{-1}Vhg_0 = g_0^{-1}Vg_0 \subset V$. □

**Lemma 3.1.2** *If $\phi : G \to {}_2\bar{E}$ is a cocycle and $\psi = \phi|\, H$, then $\psi(g^2) \in \{O, P\}$ for any $g \in G\backslash H$.*

*Proof.* Since $\psi \in H^1(H,\, {}_2\bar{E})^{G/H}$, it follows that $g_0\psi(h) = \psi(g_0^{-1}hg_0)$ for any $h \in H$. Substituting $h = g^2$ we get

$$\begin{aligned} g_0\psi(g^2) &= \psi(g_0^{-1}g^2g_0) = \psi(g_0^{-1}g) + \psi(gg_0) \\ &= \psi(gg_0) + \psi(g_0^{-1}g) \\ &= \psi(gg_0g_0^{-1}g) \\ &= \psi(g^2) \\ &\Leftrightarrow \psi(g^2) \in \{O, P\} . \end{aligned}$$

□

## 3.2 *Formula for cocycles*

Now let $g_0$ be some element in $G\backslash H$. For any $Q \in {}_2\bar{E} = \{O, P, T, S\}$ and for any homomorphism $\psi \in Hom(H,\, {}_2\bar{E})$ denote by $\phi_{Q,\psi}$ the map defined by the rule

$$\phi_{Q,\psi}(g) = \begin{cases} \psi(g)\,, & g \in H \\ g_0\psi(g_0^{-1}g) + Q\,, & g \in G\backslash H\,. \end{cases} \tag{11}$$

**Lemma 3.2.1** *Any cocycle $\phi : G \to {}_2\bar{E}$ is of the form $\phi_{Q,\psi}$ for some $Q \in {}_2\bar{E}$ and $\psi \in Hom(H, {}_2\bar{E})$. Conversely, let $Q$ and $\psi$ be as above. Then $\partial\phi_{Q,\psi} = 0$ if and only if the following two conditions hold:*

*(i) $g_0\psi(h) = \psi(g_0^{-1}hg_0)$ for any $h \in H$;*

*(ii) $\psi(g_0^2) = P$ for $Q \in \{T, S\}$ and $\psi(g_0^2) = O$ for $Q \in \{O, P\}$.*

*Proof.* If $\phi$ is a 1-cocycle with coefficients in ${}_2\bar{E}$ then for any $g \in G$ we have

$$\partial\phi(g_0, g_0^{-1}g) = g_0\phi(g_0^{-1}g) + \phi(g) + \phi(g_0) = 0$$

for some $g_0 \in G\backslash H$. Therefore $\phi = \phi_{Q,\psi}$, where $Q = \phi(g_0)$ and $\psi = \phi|_H$.

If $h_1, h_2 \in H$, then it is clear that $\partial\phi_{Q,\psi}(h_1, h_2) = 0$. Let $g \in G\backslash H$ and $h \in H$. Then

$$\begin{aligned}
\partial\phi_{Q,\psi}(g,h) &= g\psi(h) + g_0\psi(g_0^{-1}gh) + Q + g_0\psi(g_0^{-1}g) + Q \\
&= g\psi(h) + g_0\psi(g_0^{-1}g) + g_0\psi(h) + g_0\psi(g_0^{-1}g) \\
&= g\psi(h) + g_0\psi(h) \\
&= \begin{cases} 2\psi(h)\,, & \psi(h) \in \{O, P\} \\ 2g_0\psi(h)\,, & \psi(h) \in \{T, S\} \end{cases} \\
&= 0
\end{aligned}$$

Note that we replace signs "$-$" by "$+$" because $\phi_{Q,\psi}$ is a map into a 2-torsion group.

If $h \in H, g \in G\backslash H$, then for any $Q$ and $\psi$ we have

$$\begin{aligned}
\partial\phi_{Q,\psi}(h,g) &= g_0\psi(g_0^{-1}g) + Q + g_0\psi(g_0^{-1}hg) + Q + \psi(h) \\
&= g_0\psi(g_0^{-1}g) + g_0\psi(g_0^{-1}hg_0) + g_0\psi(g_0^{-1}g) + \psi(h) \\
&= g_0\psi(g_0^{-1}hg_0) + \psi(h)\,.
\end{aligned}$$

Therefore, if $\partial\phi_{Q,\psi} = 0$, then $g_0\psi(g_0^{-1}hg_0) + \psi(h) = 0$, that is

$$g_0\psi(h) = \psi(g_0^{-1}hg_0)\,. \tag{12}$$

If $g_1 \in G\backslash H, g_2 \in G\backslash H$, then for any $Q$ and $\psi$ we have:

$$\begin{aligned}
\partial\phi_{Q,\psi}(g_1,g_2) &= g_1(g_0\psi(g_0^{-1}g_2) + Q) + \psi(g_1g_2) + g_0\psi(g_0^{-1}g_1) + Q \\
&= \psi(g_0^{-1}g_2) + \psi(g_1g_2) + g_0\psi(g_0^{-1}g_1) + g_1Q + Q \\
&\overset{(12)}{=} \psi(g_0^{-1}g_2) + \psi(g_1g_2) + \psi(g_0^{-1}g_0^{-1}g_1g_0) + g_1Q + Q \\
&= \psi(g_0^{-1}g_2) + \psi(g_1g_2) + \psi(g_0^2) + \psi(g_1g_0) + g_1Q + Q\,.
\end{aligned}$$

Observe that

$$\begin{aligned}
\psi(g_0^{-1}g_2) + \psi(g_1g_2) + \psi(g_1g_0) &= \psi(g_1g_0) + \psi(g_0^{-1}g_2) + \psi(g_1g_2) \\
&= \psi(g_1g_0g_0^{-1}g_2) + \psi(g_1g_2) \\
&= \psi(g_1g_2) + \psi(g_1g_2) \\
&= 2\psi(g_1g_2) \\
&= 0
\end{aligned}$$

Hence one can continue:

$$\begin{aligned}
\partial\phi_{Q,\psi}(g_1,g_2) &= \psi(g_0^{-1}g_2) + \psi(g_1g_2) + \psi(g_0^2) + \psi(g_1g_0) + g_1Q + Q \\
&= \psi(g_0^2) + g_1Q + Q \\
&= \psi(g_0^2) + g_0Q + Q\,.
\end{aligned}$$

Therefore, if $\partial\phi_{Q,\psi} = 0$, then

$$\psi(g_0^2) = g_0Q + Q\,.$$

□

**Remark 3.2.1** *Clearly, the condition (i) is equivalent to the condition $\psi \in (Hom(H, {}_2\bar{E}))^{G/H}$ and can be deduced directly from the isomorphism 10.*

### 3.3 *Classification of cocycles*

Now one can classify all 1-cocycles $\phi = \phi_{Q,\psi}$ of the group $G$ with coefficients in ${}_2\bar{E}$ according to the number of elements in $\mathrm{im}(\psi)$.

Denote by $\xi$ the surjective homomorphism $G \to \{O, P\}$ with kernel $H$. Then $\xi = \partial T = \partial S$ and $\xi$ is a unique non-trivial 1-coboundary of $G$ with coefficients in ${}_2\bar{E}$. If $\#\,\mathrm{im}(\psi) = 1$, i.e. $\psi = 0$, then the formula 11 and Lemma 3.2.1 show that either $\phi = 0$ or $\phi = \xi$. In both cases $\mathrm{cls}(\phi) = 0$ in $H^1(G,\, {}_2\bar{E})$.

Let $\phi_{Q,\psi}$ be a cocycle. Let $\psi_T$ and $\psi_S$ are the compositions of $\psi$ with the projections of the group ${}_2\bar{E}$ on $\{O, T\}$ and $\{O, S\}$ respectively. Let $U = \ker(\psi_T)$. Then $\ker(\psi_S) = g_0^{-1} U g_0$. The condition $\#\,\mathrm{im}(\psi) = 2$ is equivalent to the condition $g_0^{-1} U g_0 = U$, $g_0 \in G\backslash H$. In this case $\psi$ is a surjective homomorphism $H \to \{O, P\}$ with kernel $U$. The group $U$ is normal in $G$ by Lemma 3.1.1. Consider the quotient group $G/U$. There are two possible cases for $G/U$: either $G/U \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ or $G/U \cong \mathbb{Z}/4$. In the first case one can choose $g_0 \in G\backslash H$ such that $g_0^2 \in U$. By Lemma 3.2.1 the point $Q$ lie in $\{O, P\}$. But $\phi_{P,\psi} + \phi_{O,\psi} = \xi = \partial T$. Consequently, we can consider only cocycles $\phi_{O,\psi}$. If $G/U \cong \mathbf{Z/4}$ then $g_0^2 \in H\backslash U$. By Lemma 3.2.1 the point $Q$ lies in $\{T, S\}$. Adding $\xi$ one can consider only cocycles $\phi_{T,\psi}$.

**Definition 3.3.1** *Let $\phi = \phi_{Q,\psi}$ be a cocycle with $\#\,\mathrm{im}(\psi) = 2$ and $U = \ker(\psi)$. If $G/U \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ and $Q = O$, then we say that $\phi$ is a cocycle of the type $I$. If $G/U \cong \mathbb{Z}/4$ and $Q = T$, then we say that $\phi$ is a cocycle of the type $II$.*

Now let us consider the case of a cocycle $\phi = \phi_{Q,\psi}$ with $\#\,\mathrm{im}(\psi) = 4$. The corresponding homomorphism can be uniquely determined by a subgroup $U$ of index 2 in $H$ such that $U \neq g_0^{-1} U g_0$ for some $g_0 \in G\backslash H$ (note that $g_0^{-1} U g_0 = g_0'^{-1} U g_0'$ for any two elements $g_0, g_0' \in G\backslash H$). Let $U_O = U \cap g_0^{-1} U g_0$. The condition $U \neq g_0^{-1} U g_0$ implies that the quotient group $G/U_O$ is noncommutative of order 8. Moreover, $G/U_O$ has 3 elements of order 2 lying in the subgroup $H/U_O$. Therefore $G/U_O$ is isomorphic to the dihedral group $D_4$ (see, for example, [Hall59], 4.4). But $D_4$ has five elements of order 2. Consequently, there exists an element $g_0$ in $G\backslash H$ such that $g_0^2$ lies in $U_O$. By Lemma 3.2.1 the point $Q$ lies $\{O, P\}$. Adding $\xi$ if it is necessary one can consider only the case $Q = O$.

**Definition 3.3.2** *Cocycles $\phi = \phi_{T,\psi}$ with $\#\,\mathrm{im}(\psi) = 4$ will be called cocycles of type $III$.*

In fact we proved the

**Proposition 3.3.1** *Any element in ${}_2H^1(G, \bar{E})$ can be represented by cocycle of one of three types $I$, $II$ and $III$.*

### 3.4 *Direct calculations of cocycles*

**Proposition 3.4.1** *Let $\phi = \phi_{Q,\psi}$ be a cocycle of the group $G$ with coefficients in ${}_2\bar{E}$ and $U = \ker(\psi)$. If $\phi$ is a cocycle of type $I$, then $\phi$ is the surjective homomorphism $G \to \{O, P\}$ with kernel $U \cup g_0 U$. If $\phi = \phi_{T,\psi}$ has type $II$, then*

$$\phi_{T,\psi}(g) = \begin{cases} O\,, & \text{if } g \in U \\ T\,, & \text{if } g \in g_0 U \\ P\,, & \text{if } g \in H\backslash U \\ S\,, & \text{if } g \in G\backslash(H \cup g_0 U) \end{cases}$$

*Proof.* Let $\phi_{O,\psi}$ be a cocycle of type $I$. Then $G/U \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ and $\mathrm{im}(\psi) = \{O, P\}$. If $g \in G\backslash(H \cup g_0 U)$, then $g_0^{-1} g \in H\backslash U$. Using formula (11) one can compute $\phi_{O,\psi}(g) = \psi(g_0^{-1} g) = P$. Moreover, for any $u \in U$ we have $\phi_{O,\psi}(g_0 u) = \psi(g_0^{-1} g_0 u) = \psi(u) = O$.

Let $\phi_{T,\psi}$ be a cocycle of type $II$. Fix the isomorphism $G/U \cong \mathbb{Z}/4$ such that $\overline{g_0}$ maps into the $1 + \mathbb{Z}$. Sometimes it is convenient to identify the group $G/U$ and $\mathbb{Z}/4$ by means of this isomorphism. Any $g \in G$ can be written in the form

$$g = g_0^i u \text{ where } i \in \{0, 1, 2, 3\} \text{ and } u \in U\,,$$

where $i$ is the *order* of an element $g$ under the element $g_0$. If the order $i$ of $g$ is even, then $g_0^i \in H$. Using formula 11 one can obtain that

$$\phi_{T,\psi}(g) = \psi(g_0^i u) = \psi(g_0^i) = \begin{cases} O \ , & \text{for } i = 0 \\ P \ , & \text{for } i = 2 \end{cases}$$

If $i$ is odd, then $g_0^i \in G \backslash H$ and hence $g = g_0^i u \in G \backslash H$. Using the same lemma we have

$$\begin{aligned} \phi_{T,\psi}(g) &= \psi(g_0^{-1} g) + T = \psi(g_0^{-1} g_0^i u) + T \\ &= \psi(g_0^{i-1} u) + T = \psi(g_0^{i-1}) + T \\ &= \begin{cases} T \ , & \text{for } i = 1 \\ S \ , & \text{for } i = 3 \end{cases} \end{aligned}$$

□

Now let us consider cocycles $\phi_{O,\psi}$ of type $III$. It follows from the definition that every such cocyle is completely determined by a subgroup $U$ of index 2 in $H$ such that $U \neq g_0^{-1} U g_0$. Here $g_0 \in G \backslash H$ and $g_0^2 \in U_O = U \cap g_0^{-1} U g_0$. If $\psi_T$ and $\psi_S$ are the compositions of $\psi$ with the projections of ${}_2\bar{E}$ on $\{O, T\}$ and $\{O, S\}$ respectively, then $\psi = \psi_T + \psi_S$ and $U = \ker(\psi_T)$, $g_0^{-1} U g_0 = \ker(\psi_T)$ (see Section 3.3). Let

$$\begin{aligned} U_S &= U \backslash (g_0^{-1} U g_0) \\ U_T &= (g_0^{-1} U g_0) \backslash U \\ U_P &= H \backslash (U \cup g_0^{-1} U g_0) \end{aligned}$$

be the cosets in $H/U_O$. Then $G/U_O = \{U_O, U_S, U_T, U_P, g_0 U_O, g_0 U_S, g_0 U_T, g_0 U_P, \}$. Schematically one can describe the quotient group $G/U_O$ by the diagram

| | |
|---|---|
| $U_S$ | $U_P$ |
| $U_O$ | $U_T$ |
| $g_0 U_S$ | $g_0 U_P$ |
| $g_0 U_O$ | $g_0 U_T$ |

Here the top four squares correspond to the group $H$ and all eight squares correspond to the whole group $G$.

**Proposition 3.4.2** *Let $\phi = \phi_{O,\psi}$ be a cocycle of type $III$. Let*

$$V_O = U_O \cup g_0 U_O \ ,$$

$$V_S = U_S \cup g_0 U_T \ ,$$

$$V_T = U_T \cup g_0 U_S \ ,$$

*and*

$$V_P = U_P \cup g_0 U_P \ .$$

*Then $V_O$ is a (not normal) subgroup in $G$ of index 4. The sets $V_O$, $V_S$, $V_T$, $V_P$ are left cosets of the group $G$ by $V_O$. The cocycle $\phi_{O,\psi}$ can be computed by the formula*

$$\phi_{O,\psi}(g) = \begin{cases} O\ , & \textit{if } g \in V_O \\ S\ , & \textit{if } g \in V_S \\ T\ , & \textit{if } g \in V_T \\ P\ , & \textit{if } g \in V_P \end{cases}$$

*Proof.* We know that $G/U_O \cong D_4$. Then this proposition can be proved by direct computation with using the formula

$$\phi_{O,\psi}(g) = \begin{cases} \psi(g)\,, & g \in H \\ g_0\psi(g_0^{-1}g)\,, & g \in G\backslash H\ . \end{cases} \tag{13}$$

and rules of multiplication in $G/U_O \cong D_4$. For example, let us prove that $V_O$ is a subgroup in $G$ and that it is not normal in $G$. By definition of a cocycle of type $III$, we have that $\overline{g_0}^2 = 1$ in $G/U_O$. Hence $V_O = U_O \cup g_0U_O$ is a subgroup in $G$. Let $h_S \in U_S$, $h_T \in U_T$ and $h_P \in U_P$. Then for any $u \in U_O$ we have:

$$\overline{h_S^{-1}g_0uh_S} = \overline{h_S}\,\overline{g_0}\,\overline{h_S} = \overline{g_0}(\overline{g_0}^{-1}\overline{h_S}\,\overline{g_0})\overline{h_S} = \overline{g_0}\,\overline{h_Th_S} = \overline{g_0}\,\overline{h_P} = \overline{g_0h_P}\ .$$

In other words, $h_S^{-1}g_0uh_S \in g_0U_P$. Hence $g_0^{-1}V_Og_0 \not\subset V_O$ (because by definition of the set $V_O$ we have that $V_O \cap g_0U_P = \emptyset$). □

We can illustrate the values of cocycle $\phi_{O,\psi}$ of type $III$ by the diagram

| | |
|---|---|
| $S$ | $P$ |
| $O$ | $T$ |

| | |
|---|---|
| $T$ | $P$ |
| $O$ | $S$ |

### 3.5 $\delta$ *on cocycles*

Now we want to lift the cohomology classes of cocycles $\phi_{Q,\psi}$ to the group ${}_2\mathrm{Br}(E)$. In other words, we want to describe unramified central simple algebras of an exponent 2 such that its classes maps into classes $\mathrm{cls}(\phi_{Q,\psi}) \in H^1(G, \bar{E})$ under the homomorphism $\pi$.

According to Section 2.3 and formula (6) the first step must be computing $\delta(\mathrm{cls}(\phi_{Q,\psi}))$ for cycles of the $I$ and $II$ types. We will determine $\delta(\mathrm{cls}(\phi_{Q,\psi}))$ in terms of explicit 2-cocycles of the group $G$ with coefficients in $\mathrm{P}(\bar{E})$.

Consider the following particular case of the short exact sequence (5):

$$0 \to \mathrm{P}(\bar{E}) \longrightarrow \mathrm{Div}^0(\bar{E}) \xrightarrow{\mathrm{sum}} \bar{E} \to 0\ .$$

For any point $W \in \bar{E}$ denote by $(W)$ the same point viewed as a divisor on $E$. Then

$$\mathrm{sum}((\mathrm{W}) - (\mathrm{O})) = \mathrm{W}\ .$$

Let $\phi$ be a continuous (in sense of the profinite topology on $G$) 1-cocycle of the group $G$ with coefficients in $\bar{E}$. Denote by $\hat{\phi}$ the continuous map

$$\hat{\phi} : G \longrightarrow \mathrm{Div}^0(\bar{E})$$

such that

$$\hat{\phi}(g) = (\phi(g)) - (O)$$

for any $g \in G$. Then $\partial\hat{\phi}$ is a 2-cocycle of $G$ with coefficients in $\mathrm{P}(\bar{E})$, and

$$\delta(\mathrm{cls}(\phi)) = \mathrm{cls}(\partial\hat{\phi}) \ .$$

The formula

$$\partial\hat{\phi}(g_1, g_2) = g_1\hat{\phi}(g_2) - \hat{\phi}(g_1 g_2) + \hat{\phi}(g_2) \tag{14}$$

allows to compute $\partial\hat{\phi}$ by $\hat{\phi}$. We need to do this for cocycles of types $I$, $II$ and $III$. First we consider the cases of cocycles of $I$ and $II$ types.

# 4 Quaternion and cyclic algebras

## 4.1 *Algebras corresponding to cocyles of type I*

**Proposition 4.1.1** *Let $\phi_{O,\psi}$ be a cocycle of type I, $U = \ker(\psi)$ and $W = U \cup g_0 U$ the subgroup of index 2 in $G$ (see Proposition 3.4.1). Consider an element $a \in k\backslash k^2$ such that $k(\sqrt{a}) = \bar{k}^W$ is the subfield invariant under the action of $W$. Then the quaternion algebra*

$$(a, x - x_P)$$

*with center $k(E)$ is unramified. The class of $(a, x - x_P)$ maps into the class $\mathrm{cls}(\phi_{O,\psi})$ under the homomorphism $\pi : \mathrm{Br}(E) \to H^1(G, \bar{E})$.*

*Proof.* Consider the 2-cocycle $\Phi_{P,a} : G \times G \to \bar{k}(\bar{E})^*$ defined by the formula

$$\Phi_{P,a}(g_1, g_2) = \begin{cases} x - x_P \ , & \text{if } (g_1, g_2) \in (G\backslash W) \times (G\backslash W) \\ 1 \ , & \text{in the other case} \end{cases}$$

The cocycle $\Phi_{P,a}$ defines the quaternion algebra $(a, x - x_P)$ over $k(E)$. If $\mathrm{div} : \bar{k}(\bar{E})^* \to \mathrm{P}(\bar{E})$ is the map sending $f \in \bar{k}(\bar{E})^*$ into the divisor $\mathrm{div}(f)$ of zeros and poles of the function $f$, then $\partial\hat{\phi}_{O,\psi} = \mathrm{div} \circ \Phi_{P,a}$. Taking into account the diagram in Section 2.3, one can see that

$$\mathrm{inv}(\mathrm{cls}(\Phi_{P,a})) = \beta(\alpha(\mathrm{cls}(\Phi_{P,a}))) = \beta(\mathrm{cls}(\mathrm{div} \circ \Phi_{P,a})) = \beta(\mathrm{cls}(\partial\hat{\phi}_{O,\psi})) = \beta(\delta(\mathrm{cls}(\phi_{O,\psi})) = 0 \ .$$

Hence the algebra $(a, x - x_P)$ is unramified and $\pi(\mathrm{cls}(\Phi_{P,a})) = \mathrm{cls}(\phi_{O,\psi})$. □

## 4.2 *$\delta$ for cocycles of type II*

**Proposition 4.2.1** *Let $\phi_{T,\psi}$ be a cocycle of type II. Then the 2-cocycle $\partial\hat{\phi}_{T,\psi} : G \times G \to \mathrm{P}(\bar{E})$ is given in the following table*

| | | | | |
|---|---|---|---|---|
| $g_2 \in G\backslash(H \cup g_0 U)$ | $0$ | $(S) - (T) + (P) - (O)$ | $2(T) - 2(O)$ | $(T) - (P) + (S) - (O)$ |
| $g_2 \in g_0 U$ | $0$ | $(T) - (S) + (P) - (O)$ | $(S) - (P) + (T) - (O)$ | $2(S) - 2(O)$ |
| $g_2 \in H\backslash U$ | $0$ | $2(P) - 2(O)$ | $(P) - (S) + (T) - (O)$ | $(P) - (T) + (S) - (O)$ |
| $g_2 \in U$ | $0$ | $0$ | $0$ | $0$ |
| | $g_1 \in U$ | $g_1 \in H\backslash U$ | $g_1 \in g_0 U$ | $g_1 \in G\backslash(H \cup g_0 U)$ |

*Proof.* By Proposition 3.4.1 we have the following explicit formula for $\hat{\phi}_{T,\psi}$:

$$\hat{\phi}_{T,\psi}(g) = \begin{cases} 0\ , & g \in U \Leftrightarrow i = 0 \\ (T) - (O)\ , & g \in g_0 U \Leftrightarrow i = 1 \\ (P) - (O)\ , & g \in H \backslash U \Leftrightarrow i = 2 \\ (S) - (O)\ , & g \in G \backslash (H \cup g_0 U) \Leftrightarrow i = 3 \end{cases} \tag{15}$$

Let $g_1, g_2 \in G$ and $i_1$, $i_2$ are the orders of $g_1$, $g_2$ respectively. It is clear that the order $i$ of $g_1 g_2$ is equal to $i_1 + i_2$ modulo 4. The direct computation with the formulas (15) and (14) gives the following explicit form of the cocycle $\partial\hat{\phi}_{T,\psi}$:

| $i_1$ | $i_2$ | $g_1\phi_{T,\psi}(g_2)$ | $-\phi_{T,\psi}(g_1 g_2)$ | $\phi_{T,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | $(T)-(O)$ | $-(T)+(O)$ | 0 | 0 |
| 0 | 2 | $(P)-(O)$ | $-(P)+(O)$ | 0 | 0 |
| 0 | 3 | $(S)-(O)$ | $-(S)+(O)$ | 0 | 0 |
| 1 | 0 | 0 | $-(T)+(O)$ | $(T)-(O)$ | 0 |
| 1 | 1 | $(S)-(O)$ | $-(P)+(O)$ | $(T)-(O)$ | $(S)-(P)+(T)-(O)$ |
| 1 | 2 | $(P)-(O)$ | $-(S)+(O)$ | $(T)-(O)$ | $(P)-(S)+(T)-(O)$ |
| 1 | 3 | $(T)-(O)$ | 0 | $(T)-(O)$ | $2(T)-2(O)$ |
| 2 | 0 | 0 | $-(P)+(O)$ | $(P)-(O)$ | 0 |
| 2 | 1 | $(T)-(O)$ | $-(S)+(O)$ | $(P)-(O)$ | $(T)-(S)+(P)-(O)$ |
| 2 | 2 | $(P)-(O)$ | 0 | $(P)-(O)$ | $2(P)-2(O)$ |
| 2 | 3 | $(S)-(O)$ | $-(T)+(O)$ | $(P)-(O)$ | $(S)-(T)+(P)-(O)$ |
| 3 | 0 | 0 | $-(S)+(O)$ | $(S)-(O)$ | 0 |
| 3 | 1 | $(S)-(O)$ | 0 | $(S)-(O)$ | $2(S)-2(O)$ |
| 3 | 2 | $(P)-(O)$ | $-(T)+(O)$ | $(S)-(O)$ | $(P)-(T)+(S)-(O)$ |
| 3 | 3 | $(T)-(O)$ | $-(P)+(O)$ | $(S)-(O)$ | $(T)-(P)+(S)-(O)$ |

Rewriting this table in more compact form we obtain the statement of the proposition. □

## 4.3 *Cross products corresponding to cocycles of type II*

We need some lemma. For short we set

$$D_P = 2(P) - 2(O) = \mathrm{div}(x - x_P)\ ,$$

$$D_T = 2(T) - 2(O) = \mathrm{div}(x - x_T)\ ,$$

$$D_S = 2(T) - 2(O) = \mathrm{div}(x - x_S)\ ,$$

and

$$D = (P) + (T) + (S) - 3(O)\ .$$

Let

$$\Gamma = \langle D, D_P, D_T, D_S \rangle$$

be the subgroup in $\mathrm{P}(\bar{E})$ generated by these principle divisors. Also let

$$\Omega = \langle y, x - x_P, x - x_T, x - x_S \rangle$$

be the subgroup in $\bar{k}(\bar{E})^*$ generated by the functions $x - x_P$, $x - x_T$, $x - x_S$ and $y$. It is clear that $\Gamma$ and $\Omega$ are discrete $G$-submodules in $\mathrm{P}(\bar{E})$ and $\bar{k}(\bar{E})^*$ respectively. The restriction of the homomorphism $\mathrm{div} : \bar{k}(\bar{E})^* \to \mathrm{P}(\bar{E})$ on the submodule $\Gamma$ is a surjective $G$-homomorphism

$$\Omega \xrightarrow{\mathrm{div}} \Gamma\ .$$

**Lemma 4.3.1** *Let $F = F\langle D, D_P, D_T, D_S\rangle$ denotes the free abelian group generated by the set $\{D, D_P, D_T, D_S\}$. Let $\tau : F \to \Omega$ be the homomorphism defined by $\tau(D_P) = x - x_P$, $\tau(D_T) = x - x_T$, $\tau(D_S) = x - x_S$, $\tau(D) = y$. Let $\mu : F \to \Gamma$ be the homomorphism which sends any element of the basis of the group $F$ to itself. Then there exists a unique homomorphism (of discrete $G$-modules) $\gamma$, which makes the diagram*

$$\begin{tikzcd} F \arrow[r, "\mu"] \arrow[dr, "\tau"'] & \Gamma \arrow[d, "\gamma"] \\ & \Omega \end{tikzcd}$$

*commutative. In particular,*

$$\operatorname{div} \circ \gamma = \mathrm{id}_\Gamma \ .$$

*Proof.* Observe that $2D = D_P + D_T + D_S$. Show that it is a unique relation in $\Gamma$. Indeed, let $l, m, n, t \in \mathbb{Z}$ and $D + mD_P + nD_T + tD_S = 0$. Then

$$l(P) + l(T) + l(S) - 3l(O) + 2m(P) - 2m(O) + 2n(T) - 2n(O) + 2t(S) - 2t(O) =$$

$$(l + 2m)(P) + (l + 2n)(T) + (l + 2t)(S) - 2(m + n + t)(O) - 3l(O) = 0 \Rightarrow$$

$$\Rightarrow \begin{cases} l + 2m = 0 \\ l + 2n = 0 \\ l + 2t = 0 \\ 2(m + n + t) + 3l = 0 \end{cases}$$

Solving this system one can see that $m = n = t$ and $l = -2m$. Hence the relation $lD + mD_P + nD_T + tD_S = 0$ is of the form $-2mD + mD_P + mD_T + mD_S = 0$, that is $2D = D_P + D_T + D_S$.

Thus we have that $\Gamma$ is the quotient group of $F = F\langle D, D_P, D_T, D_S\rangle$ by the cyclic subgroup generated by the element $D_P + D_T + D_S - 2D$. Then the existence of $\gamma$ follows from the equality

$$\tau(D_P + D_T + D_S - 2D) = \frac{(x - x_P)(x - x_T)(x - x_S)}{y^2} = \frac{y^2}{y^2} = 1 \ .$$

□

**Definition 4.3.1** *Let $\phi_{T,\psi}$ be a cocycle of type $II$ defined by a normal subgroup $U$ in $G$ such that $U \subset H$ and $G/U \cong \mathbb{Z}/4$. Let*

$$\Phi_{T,\psi} := \gamma \circ \partial\hat{\phi}_{T,\psi} \ .$$

*Since $\gamma$ is a homomorphism of discrete $G$-modules and $\partial\hat{\phi}_{T,\psi}$ is a 2-cocycle, the map $\Phi_{T,\psi}$ is a 2-cocycle of the group $G$ with coefficients in $\bar{k}(\bar{E})^*$. Let*

$$A_U$$

*be the central simple algebra over $k(E)$ which is the cross product defined by the cocycle $\Phi_{T,\psi}$.*

**Proposition 4.3.1** *Let $\phi_{T,\psi}$ be a cocycle of type $II$ and $U = \ker(\psi)$. Then the 2-cocyle $\Phi_{T,\psi}$ from Definition 4.3.1 can be explicitly given by the following table*

| | | | | |
|---|---|---|---|---|
| $g_2 \in G\backslash(H \cup g_0U)$ | 1 | $\frac{y}{x-x_T}$ | $x - x_T$ | $\frac{y}{x-x_P}$ |
| $g_2 \in g_0U$ | 1 | $\frac{y}{x-x_S}$ | $\frac{y}{x-x_P}$ | $x - x_S$ |
| $g_2 \in H\backslash U$ | 1 | $x - x_P$ | $\frac{y}{x-x_S}$ | $\frac{y}{x-x_T}$ |
| $g_2 \in U$ | 1 | 1 | 1 | 1 |
| | $g_1 \in U$ | $g_1 \in H\backslash U$ | $g_1 \in g_0U$ | $g_1 \in G\backslash(H \cup g_0U)$ |

*The cross product $A_U$ is an unramified central simple algebra of exponent 2 over the function field $k(E)$. The class of $A_U$ in $\mathrm{Br}(E)$ maps into the class $\mathrm{cls}(\phi_{T,\psi})$ under the homomorphism $\pi : \mathrm{Br}(E) \to H^1(G, \bar{E})$.*

*Proof.* To obtain the table it is sufficient to apply the homomorphism $\gamma$ to the table 4.2.1. Since $\mathrm{div} \circ \gamma = \mathrm{id}_\Gamma$, it follows that $\mathrm{div} \circ \Phi_{T,\psi} = \mathrm{div} \circ \gamma \circ \partial\hat{\phi}_{T,\psi} = \partial\hat{\phi}_{T,\psi}$. Hence $\alpha(\mathrm{cls}(\Phi_{T,\psi})) = \mathrm{cls}(\partial\hat{\phi}_{T,\psi}) = \delta(\mathrm{cls}(\phi_{T,\psi}))$. Taking into account the commutative diagram from Section 2.3, we see that

$$\mathrm{inv}(\mathrm{cls}(\Phi_{T,\psi})) = \beta \circ \alpha(\mathrm{cls}(\Phi_{T,\psi})) = \beta \circ \delta(\mathrm{cls}(\phi_{T,\psi})) = 0 \ .$$

Therefore, $\mathrm{cls}(\Phi_{T,\psi}) \in \ker(\mathrm{inv})$. This means that $A_U$ is an unramified algebra over $k(E)$. The exponent of $A_U$ is equal to 2 because $2\phi_{T,\psi} = 0$. The last assertion of the proposition is a direct consequence of the equality $\delta(\mathrm{cls}(\phi_{T,\psi})) = \alpha(\mathrm{cls}(\Phi_{T,\psi}))$ and the definition of the homomorphism $\pi$. □

## 4.4 *Cyclic algebras of degree* 4

Note that the algebra $A_U$ splits by a cyclic extension of degree four. To find a corresponding cyclic algebra we need some lemma relating to second cohomology of a cyclic group of order 4. Let $C = \{1, c, c^2, c^4\}$ be a such group with a generator $c$. Let $M$ be a $C$-module, $M^C = \{m \in M |\ cm = m\}$ and $N(M) = \{m + cm |\ m \in M\}$. Then we have the well known isomorphism

$$v : H^2(C, M) \longrightarrow M^C/N(M)$$

(see, for example, [Mac63], chapter IV, § 7).

**Lemma 4.4.1** *Let $\phi : C \times C \to M$ be a 2-cocycle of $C$ with coefficients in $M$. Then*

$$v(\mathrm{cls}(\phi)) = \phi(c^3, c) + \phi(1, 1) + \phi(c^2, c) + \phi(c, c) + N(A) \ .$$

*Proof.* The proof can be provided by comparison of two standard resolutions of the trivial $C$-module $\mathbb{Z}$ for the cyclic group $C = \{1, c, c^2, c^3\}$. □

We use Lemma 4.4.1 for computation of cyclic algebras of degree 4 similar to cross products $A_U$.

**Proposition 4.4.1** *Let $\phi_{T,\psi}$ be a cocycle of type II, $U = \ker(\psi)$, $A_U$ be the central simple algebra defined by $\Phi_{T,\psi}$ (see Definition 4.3.1). Let $Z/k$ be the cyclic field extension of degree 4 defined by $U$. Then the algebra $A_U$ is similar to the cyclic algebra*

$$(Z \cdot k(E)/k(E), f)$$

*over center $k(E)$. Here $f = f(x)$ is the polynomial from the decomposition (1) considered as an element in $k(E)$.*

*Proof.* Let $C = G/U$ be the cyclic group of order 4 with the generator $c = g_0U$, $Z = \bar{k}^C$ and $Z(E)$ be the field of $Z$-rational functions on the curve $E_Z = E \times \mathrm{Spec}(Z)$. The table from Proposition 4.3.1 shows that the 2-cocycle $\Phi_{T,\psi}$ factors through the group $C$, that is there exists the commutative square

$$\begin{tikzcd} G \times G \arrow[r] \arrow[d, "\Phi_{T,\psi}"'] & C \times C \arrow[d, "\varphi_{T,\psi}"] \\ \bar{k}(\bar{E})^* & Z(E)^* \arrow[l] \end{tikzcd}$$

where the cocyle $\varphi_{T,\psi} : C \times C \to Z(E)^*$ can be computed according to the table

| | | | | |
|---|---|---|---|---|
| $c^3$ | 1 | $\frac{y}{x-x_T}$ | $x - x_T$ | $\frac{y}{x-x_P}$ |
| $c$ | 1 | $\frac{y}{x-x_S}$ | $\frac{y}{x-x_P}$ | $x - x_S$ |
| $c^2$ | 1 | $x - x_P$ | $\frac{y}{x-x_S}$ | $\frac{y}{x-x_T}$ |
| 1 | 1 | 1 | 1 | 1 |
| | 1 | $c^2$ | $c$ | $c^3$ |

The cohomology class $\mathrm{cls}(\Phi_{T,\psi}) \in H^2(G, \bar{k}(\bar{E})^*)$ is the image of $\mathrm{cls}(\varphi_{T,\psi}) \in H^2(C, Z(E)^*)$ under the injective inflation homomorphism $\mathrm{inf} : H^2(C, Z(E)^*) \hookrightarrow H^2(G, \bar{k}(\bar{E})^*)$. In terms of central simple algebras this means that the algebra $A_U \otimes_{k(E)} Z(E)$ splits, so the class of algebra $A_U$ lies in the relative Brauer group $\mathrm{Br}(Z(E)/k(E))$.

Now observe that for $M = Z(E)^*$ the norm homomorphism $N : Z(E)^* \to Z(E)^*$ is the norm $N_{Z(E)/k(E)} : Z(E)^* \to k(E)^*$ in the sense of field extensions. According to Lemma 4.4.1 the isomorphism

$$v : H^2(C, Z(E)^*) \xrightarrow{\cong} k(E)^*/N(Z(E)^*)$$

sends $\varphi_{T,\psi}$ into the class of the rational function

$$\varphi_{T,\psi}(c^3, c) \cdot \varphi_{T,\psi}(1,1) \cdot \varphi_{T,\psi}(c^2, c) \cdot \varphi_{T,\psi}(c, c) =$$

$$= (x - x_S) \cdot \frac{y}{x - x_S} \cdot \frac{y}{x - x_P} =$$

$$= \frac{y^2}{x - x_P} = \frac{(x - x_P) \cdot f(x)}{x - x_P} = f(x) \, .$$

Let $(Z \cdot k(E)/k(E), f(x))$ be the cyclic algebra over $k(E)$ defined by the cyclic extension $Z \cdot k(E)/k(E)$, the generator $c = g_0U$ of the group $C = G/U$ and the rational function $f(x) \in k(E)$. Then $(Z \cdot k(E)/k(E), f(x))$ is the crossed product induced by the 2-cocycle

| | | | | |
|---|---|---|---|---|
| $c^3$ | 1 | $f$ | $f$ | $f$ |
| $c$ | 1 | 1 | 1 | $f$ |
| $c^2$ | 1 | $f$ | 1 | $f$ |
| 1 | 1 | 1 | 1 | 1 |
| | 1 | $c^2$ | $c$ | $c^3$ |

Using Lemma (4.4.1) once more we see that the isomorphism

$$v : H^2(C, Z(E)^*) \xrightarrow{\cong} k(E)^*/N(Z(E)^*)$$

maps the class of $\varphi'_{T,\psi}$ into the coset of the rational function

$$\varphi'_{T,\psi}(c^3, c) \cdot \varphi'_{T,\psi}(1, 1) \cdot \varphi'_{T,\psi}(c^2, c) \cdot \varphi'_{T,\psi}(c, c) = f \cdot 1 \cdot 1 \cdot 1 = f \ .$$

Thus we have that $v(\mathrm{cls}(\phi'_{T,\psi})) = v(\mathrm{cls}(\phi_{T,\psi}))$, whence $\mathrm{cls}(\phi'_{T,\psi}) = \mathrm{cls}(\phi_{T,\psi})$. In terms of central simple algebras over $k(E)$ this means that the algebra $A_U$ is similar to the algebra $(Z \cdot k(E)/k(E), f)$. □

# 5 Dihedral algebras

Now let us calculate unramified central simple algebras over $k(E)$ corresponding to cocycles $\phi_{O,\psi} : G \to {}_2\bar{E}$ of type $III$. Cocycles of type $III$ was defined in Section 3.3 and calculated in Section 3.4. *We shall use the notations of these sections.* In particular, $U$ is a subgroup in $H$ such that $[H : U] = 2$ and $U \neq g_0^{-1}Ug_0$. If $\psi_T : H \to \{O, T\}$ is the surjective homomorphism with kernel $U$ and $\psi_S : H \to \{O, T\}$ is the surjective homomorphism with kernel $g_0^{-1}Ug_0$, then $\psi = \psi_T + \psi_S$.

## 5.1 *$\delta$ for cocycles of type $III$*

**Proposition 5.1.1** *Let $\phi_{O,\psi}$ be a cocycle of type $III$ defined by a subgroup $U$ of index 2 in $H$ such that $g_0^{-1}Ug_0 \neq U$, where $g_0^2 \in U_O = U \cap g_0^{-1}Ug_0$ (see Sections 3.3 and 3.4). Let $\hat{\phi}_{O,\psi} : G \to \mathrm{Div}^0(\bar{E})$ be the map such that $\hat{\phi}_{O,\psi}(g) = (Q) - (O)$ if and only if $\phi_{O,\psi}(g) = Q \in {}_2\bar{E}$. Then the 2-cocycle $\partial\hat{\phi}_{O,\psi} : G \times G \to \mathrm{P}(\bar{E})$ can be calculated by the formula*

$$\phi_{O,\psi}(g_1, g_2) = \begin{cases} 0\ , \quad (g_1, g_2) \in (V_O \times G) \cup (G \times V_O) \\ \mathrm{div}(x - x_S)\ , \quad (g_1, g_2) \in (U_S \times V_S) \cup (g_0U_T \times V_T) \\ \mathrm{div}(x - x_T)\ , \quad (g_1, g_2) \in (U_T \times V_T) \cup (g_0U_S \times V_S) \\ \mathrm{div}(x - x_P)\ , \quad (g_1, g_2) \in V_P \times V_P \\ \mathrm{div}(\frac{y}{x - x_S})\ , \quad (g_1, g_2) \in (V_T \times V_P) \cup (U_P \times V_T) \cup (g_0U_P \times V_S) \\ \mathrm{div}(\frac{y}{x - x_T})\ , \quad (g_1, g_2) \in (V_S \times V_P) \cup (U_P \times V_S) \cup (g_0U_P \times V_T) \\ \mathrm{div}(\frac{y}{x - x_P})\ , \quad (g_1, g_2) \in ((U_S \cup g_0U_S) \times V_T) \cup ((U_T \cup g_0U_T) \times V_S) \end{cases}$$

*Proof.* For the proof we use the formula

$$\partial\hat{\phi}_{O,\psi}(g_1, g_2) = g_1\hat{\phi}_{O,\psi}(g_2) - \hat{\phi}_{O,\psi}(g_1g_2) + \hat{\phi}_{O,\psi}(g_1)$$

and the rule of multiplication in $G/U_O \cong D_4$. All calculations are in the following eight tables:

| $g_1$ | $g_2$ | $g_1\phi_{O,\psi}(g_2)$ | $-\phi_{O,\psi}(g_1g_2)$ | $\phi_{O,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| $U_O$ | $U_O$ | 0 | 0 | 0 | 0 |
| $U_O$ | $U_S$ | $(S) - (O)$ | $-(S) + (O)$ | 0 | 0 |
| $U_O$ | $U_T$ | $(T) - (O)$ | $-(T) + (O)$ | 0 | 0 |
| $U_O$ | $U_P$ | $(P) - (O)$ | $-(P) + (O)$ | 0 | 0 |
| $U_O$ | $g_0U_O$ | 0 | 0 | 0 | 0 |
| $U_O$ | $g_0U_S$ | $(T) - (O)$ | $-(T) + (O)$ | 0 | 0 |
| $U_O$ | $g_0U_T$ | $(S) - (O)$ | $-(S) + (O)$ | 0 | 0 |
| $U_O$ | $g_0U_P$ | $(P) - (O)$ | $-(P) + (O)$ | 0 | 0 |

| $g_1$ | $g_2$ | $g_1\phi_{O,\psi}(g_2)$ | $-\phi_{O,\psi}(g_1g_2)$ | $\phi_{O,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| $U_S$ | $U_O$ | 0 | $-(S)+(O)$ | $(S)-(O)$ | 0 |
| $U_S$ | $U_S$ | $(S)-(O)$ | 0 | $(S)-(O)$ | $2(S)-2(O)$ |
| $U_S$ | $U_T$ | $(T)-(O)$ | $-(P)+(O)$ | $(S)-(O)$ | $(T)-(P)+(S)-(O)$ |
| $U_S$ | $U_P$ | $(P)-(O)$ | $-(T)+(O)$ | $(S)-(O)$ | $(P)-(T)+(S)-(O)$ |
| $U_S$ | $g_0U_O$ | 0 | $-(S)+(O)$ | $(S)-(O)$ | 0 |
| $U_S$ | $g_0U_S$ | $(T)-(O)$ | $-(P)+(O)$ | $(S)-(O)$ | $(T)-(P)+(S)-(O)$ |
| $U_S$ | $g_0U_T$ | $(S)-(O)$ | 0 | $(S)-(O)$ | $2(S)-2(O)$ |
| $U_S$ | $g_0U_P$ | $(P)-(O)$ | $-(T)+(O)$ | $(S)-(O)$ | $(P)-(T)+(S)-(O)$ |

| $g_1$ | $g_2$ | $g_1\phi_{O,\psi}(g_2)$ | $-\phi_{O,\psi}(g_1g_2)$ | $\phi_{O,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| $U_T$ | $U_O$ | 0 | $-(T)+(O)$ | $(T)-(O)$ | 0 |
| $U_T$ | $U_S$ | $(S)-(O)$ | $-(P)+(O)$ | $(T)-(O)$ | $(S)-(P)+(T)-(O)$ |
| $U_T$ | $U_T$ | $(T)-(O)$ | 0 | $(T)-(O)$ | $2(T)-2(O)$ |
| $U_T$ | $U_P$ | $(P)-(O)$ | $-(S)+(O)$ | $(T)-(O)$ | $(P)-(S)+(T)-(O)$ |
| $U_T$ | $g_0U_O$ | 0 | $-(T)+(O)$ | $(T)-(O)$ | 0 |
| $U_T$ | $g_0U_S$ | $(T)-(O)$ | 0 | $(T)-(O)$ | $2(T)-2(O)$ |
| $U_T$ | $g_0U_T$ | $(S)-(O)$ | $-(P)+(O)$ | $(T)-(O)$ | $(S)-(P)+(T)-(O)$ |
| $U_T$ | $g_0U_P$ | $(P)-(O)$ | $-(S)+(O)$ | $(T)-(O)$ | $(P)-(S)+(T)-(O)$ |

| $g_1$ | $g_2$ | $g_1\phi_{O,\psi}(g_2)$ | $-\phi_{O,\psi}(g_1g_2)$ | $\phi_{O,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| $U_P$ | $U_O$ | 0 | $-(P)+(O)$ | $(P)-(O)$ | 0 |
| $U_P$ | $U_S$ | $(S)-(O)$ | $-(T)+(O)$ | $(P)-(O)$ | $(S)-(T)+(P)-(O)$ |
| $U_P$ | $U_T$ | $(T)-(O)$ | $-(S)+(O)$ | $(P)-(O)$ | $(T)-(S)+(P)-(O)$ |
| $U_P$ | $U_P$ | $(P)-(O)$ | 0 | $(P)-(O)$ | $2(P)-2(O)$ |
| $U_P$ | $g_0U_O$ | 0 | $-(P)+(O)$ | $(P)-(O)$ | 0 |
| $U_P$ | $g_0U_S$ | $(T)-(O)$ | $-(S)+(O)$ | $(P)-(O)$ | $(T)-(S)+(P)-(O)$ |
| $U_P$ | $g_0U_T$ | $(S)-(O)$ | $-(T)+(O)$ | $(P)-(O)$ | $(S)-(T)+(P)-(O)$ |
| $U_P$ | $g_0U_P$ | $(P)-(O)$ | 0 | $(P)-(O)$ | $2(P)-2(O)$ |

| $g_1$ | $g_2$ | $g_1\phi_{O,\psi}(g_2)$ | $-\phi_{O,\psi}(g_1g_2)$ | $\phi_{O,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| $g_0U_O$ | $U_O$ | 0 | 0 | 0 | 0 |
| $g_0U_O$ | $U_S$ | $(T)-(O)$ | $-(T)+(O)$ | 0 | 0 |
| $g_0U_O$ | $U_T$ | $(S)-(O)$ | $-(S)+(O)$ | 0 | 0 |
| $g_0U_O$ | $U_P$ | $(P)-(O)$ | $-(P)+(O)$ | 0 | 0 |
| $g_0U_O$ | $g_0U_O$ | 0 | 0 | 0 | 0 |
| $g_0U_O$ | $g_0U_S$ | $(S)-(O)$ | $-(S)+(O)$ | 0 | 0 |
| $g_0U_O$ | $g_0U_T$ | $(T)-(O)$ | $-(T)+(O)$ | 0 | 0 |
| $g_0U_O$ | $g_0U_P$ | $(P)-(O)$ | $-(P)+(O)$ | 0 | 0 |

| $g_1$ | $g_2$ | $g_1\phi_{O,\psi}(g_2)$ | $-\phi_{O,\psi}(g_1g_2)$ | $\phi_{O,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| $g_0U_S$ | $U_O$ | 0 | $-(T)+(O)$ | $(T)-(O)$ | 0 |
| $g_0U_S$ | $U_S$ | $(T)-(O)$ | 0 | $(T)-(O)$ | $2(T)-2(O)$ |
| $g_0U_S$ | $U_T$ | $(S)-(O)$ | $-(P)+(O)$ | $(T)-(O)$ | $(S)-(P)+(T)-(O)$ |
| $g_0U_S$ | $U_P$ | $(P)-(O)$ | $-(S)+(O)$ | $(T)-(O)$ | $(P)-(S)+(T)-(O)$ |
| $g_0U_S$ | $g_0U_O$ | 0 | $-(T)+(O)$ | $(T)-(O)$ | 0 |
| $g_0U_S$ | $g_0U_S$ | $(S)-(O)$ | $-(P)+(O)$ | $(T)-(O)$ | $(S)-(P)+(T)-(O)$ |
| $g_0U_S$ | $g_0U_T$ | $(T)-(O)$ | 0 | $(T)-(O)$ | $2(T)-2(O)$ |
| $g_0U_S$ | $g_0U_P$ | $(P)-(O)$ | $-(S)+(O)$ | $(T)-(O)$ | $(P)-(S)+(T)-(O)$ |

| $g_1$ | $g_2$ | $g_1\phi_{O,\psi}(g_2)$ | $-\phi_{O,\psi}(g_1g_2)$ | $\phi_{O,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| $g_0U_T$ | $U_O$ | $0$ | $-(S)+(O)$ | $(S)-(O)$ | $0$ |
| $g_0U_T$ | $U_S$ | $(T)-(O)$ | $-(P)+(O)$ | $(S)-(O)$ | $(T)-(P)+(S)-(O)$ |
| $g_0U_T$ | $U_T$ | $(S)-(O)$ | $0$ | $(S)-(O)$ | $2(S)-2(O)$ |
| $g_0U_T$ | $U_P$ | $(P)-(O)$ | $-(T)+(O)$ | $(S)-(O)$ | $(P)-(T)+(S)-(O)$ |
| $g_0U_T$ | $g_0U_O$ | $0$ | $-(S)+(O)$ | $(S)-(O)$ | $0$ |
| $g_0U_T$ | $g_0U_S$ | $(S)-(O)$ | $0$ | $(S)-(O)$ | $2(S)-2(O)$ |
| $g_0U_T$ | $g_0U_T$ | $(T)-(O)$ | $-(P)+(O)$ | $(S)-(O)$ | $(T)-(P)+(S)-(O)$ |
| $g_0U_T$ | $g_0U_P$ | $(P)-(O)$ | $-(T)+(O)$ | $(S)-(O)$ | $(P)-(T)+(S)-(O)$ |

| $g_1$ | $g_2$ | $g_1\phi_{O,\psi}(g_2)$ | $-\phi_{O,\psi}(g_1g_2)$ | $\phi_{O,\psi}(g_1)$ | sum |
|---|---|---|---|---|---|
| $g_0U_P$ | $U_O$ | $0$ | $-(P)+(O)$ | $(P)-(O)$ | $0$ |
| $g_0U_P$ | $U_S$ | $(T)-(O)$ | $-(S)+(O)$ | $(P)-(O)$ | $(T)-(S)+(P)-(O)$ |
| $g_0U_P$ | $U_T$ | $(S)-(O)$ | $-(T)+(O)$ | $(P)-(O)$ | $(S)-(T)+(P)-(O)$ |
| $g_0U_P$ | $U_P$ | $(P)-(O)$ | $0$ | $(P)-(O)$ | $2(P)-2(O)$ |
| $g_0U_P$ | $g_0U_O$ | $0$ | $-(P)+(O)$ | $(P)-(O)$ | $0$ |
| $g_0U_P$ | $g_0U_S$ | $(S)-(O)$ | $-(T)+(O)$ | $(P)-(O)$ | $(S)-(T)+(P)-(O)$ |
| $g_0U_P$ | $g_0U_T$ | $(T)-(O)$ | $-(S)+(O)$ | $(P)-(O)$ | $(T)-(S)+(P)-(O)$ |
| $g_0U_P$ | $g_0U_P$ | $(P)-(O)$ | $0$ | $(P)-(O)$ | $2(P)-2(O)$ |

Now one can rewrite the results of these calculations in more compact way. This yields the third assertion of the proposition. □

## 5.2 *Dihedral cross products*

Now observe that the image of the cocycle $\partial\hat{\phi}_{O,\psi}$ lies in $\Gamma$ (see Section 4.3 for the definition of $\Gamma$). Hence one can obtain the cocycle

$$\Phi_{O,\psi} = \gamma \circ \partial\hat{\phi}_{O,\psi} : G \times G \longrightarrow \Omega \subset \bar{k}(\bar{E})^* \ .$$

According Proposition 5.1.1 the cocycle $\Phi_{O,\psi}$ can be calculated by the formula

$$\Phi_{O,\psi}(g_1,g_2) = \begin{cases} 1 \ , \ \ (g_1,g_2) \in (V_O \times G) \cup (G \times V_O) \\ x - x_S \ , \ \ (g_1,g_2) \in (U_S \times V_S) \cup (g_0U_T \times V_T) \\ x - x_T \ , \ \ (g_1,g_2) \in (U_T \times V_T) \cup (g_0U_S \times V_S) \\ x - x_P \ , \ \ (g_1,g_2) \in V_P \times V_P \\ \frac{y}{x-x_S} \ , \ \ (g_1,g_2) \in (V_T \times V_P) \cup (U_P \times V_T) \cup (g_0U_P \times V_S) \\ \frac{y}{x-x_T} \ , \ \ (g_1,g_2) \in (V_S \times V_P) \cup (U_P \times V_S) \cup (g_0U_P \times V_T) \\ \frac{y}{x-x_P} \ , \ \ (g_1,g_2) \in ((U_S \cup g_0U_S) \times V_T) \cup ((U_T \cup g_0U_T) \times V_S) \end{cases}$$

**Definition 5.2.1** *Denote by $B_U$ the cross product defined by the cocycle $\Phi_{O,\psi}$ (constructed by the cocycle $\phi_{O,\psi}$ of type III). Then $B_U$ is a central simple algebra with center $k(E)$. We shall call $B_U$ a dihedral cross product because it can be splited by the normal extension $\bar{k}^{U_O}$ with Galois group $G/U_O \cong D_4$.*

**Proposition 5.2.1** *The dihedral cross product $B_U$ is an unramified central simple algebra over $k(E)$ of exponent 2 and index at most 4. The class of $B_U$ in $\mathrm{Br}(E)$ maps under the homomorphism $\pi$ into the cohomology class of the cocycle $\phi_{O,\psi}$.*

*Proof.* Taking into account the considerations in Section 2.3 one can calculate

$$\begin{aligned} \mathrm{inv}(\mathrm{cls}(\Phi_{O,\psi})) &= \beta(\alpha(\mathrm{cls}(\Phi_{O,\psi}))) \\ &= \beta(\mathrm{cls}(\mathrm{div} \circ \Phi_{O,\psi})) \\ &= \beta(\mathrm{cls}(\partial\hat{\phi}_{O,\psi})) \\ &= \beta(\delta(\mathrm{cls}(\phi_{O,\psi})) \\ &= 0 \ . \end{aligned}$$

Hence $B_U$ is unramified and $\pi([B_U]) = \mathrm{cls}(\phi_{O,\psi})$.

Denote by $\rho$ the homomorphism $H^2(G,\Gamma) \to H^2(G,\bar{k}(\bar{E})^*)$ induced by the composition $\Gamma \xrightarrow{\gamma} \Omega \subset \bar{k}(\bar{E})^*$. Then

$$\begin{aligned}
2\,\mathrm{cls}(\Phi_{O,\psi}) &= 2\,\mathrm{cls}(\gamma \circ \partial\hat{\phi}_{O,\psi}) \\
&= 2\rho\,\mathrm{cls}(\partial\hat{\phi}_{O,\psi}) \\
&= 2\rho\delta(\mathrm{cls}(\phi_{O,\psi})) \\
&= \rho\delta(\mathrm{cls}(2\phi_{O,\psi})) \\
&= 0\,.
\end{aligned}$$

Hence $B_U$ has exponent 2.

Since the restriction $\Phi_{O,\psi}|_{V_O\times V_O}$ is zero (see explicit formula for $\Phi_{O,\psi}$ below), the algebra $B_U$ splits by the field $\bar{k}^{V_O}$. But the subgroup $V_O$ has index 4 in $G$ by Proposition 5.1.1. Consequently, the index of $B_U$ is at most 4. □

### 5.3 *End of the proof*

Let $c \in {}_2H^1(G,\bar{E})$. According to Proposition 3.3.1 the class $c$ can be presented by a cocycle $\phi$ of one of three types $I$, $II$ or $III$. Let $U = \ker(\psi)$, where $\psi = \phi|_H$. If $\phi$ is a cocycle of type $I$, then $\pi([(a, x - x_P)]) = c$, where $a \in k$ such that $\bar{k}^U = k(\sqrt{a})$ (see Proposition 4.1.1). So one can put $b_c = [(a, x - x_P)] \in {}_2\pi^{-1}(c)$ (see Section 2.5). If $\phi$ is a cocycle of type $II$, then $\pi([(Z,f)]) = c$, where $Z = \bar{k}^U$ (see Propositions 4.3.1 and 4.4.1) such that $\bar{k}^U = k(\sqrt{a})$. So one can take $b_c = [(a, x - x_P)]$. At last, if $\phi$ is a cocycle of type $III$, then let $b_c = [B_U]$ (see Proposition 5.2.1). Now applying Lemma 2.4.1 we finish the proof of Theorem 1.0.1.

## References


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

[Co88] J.-L.Colliot-Thélène (with the collaboration of J.-J.Sansuc). *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.

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

[GY98] V.I.Guletskiĭ, V.I.Yanchevskiĭ. *Presentation of torsion in Brauer groups of curves by cyclic algebras.*(In Russian). Dokl. AN Belarusi, 42 (1998), no. 2, 52-55.

[YM96] V.I.Yanchevskiĭ, G.L.Margolin. *The Brauer groups and the torsion of local elliptic curves.* St.Peterburgsburg Math. J. Vol.7 (1996), no.3.

[VY96] G.B.Vasiuk, V.I.Yanchevskiĭ. *On the 2-torsion part of Brauer group of local elliptic curves with good reduction defined over the field of 2-adic numbers.*(In Russian). Dokl. AN Belarusi, 40 (1996), no.6, 31-33.

[V97] G.B.Vasiuk. *On the 2-torsion part of Brauer group of 2-adic elliptic curves in the nonsplit case of bad reduction.*(In Russian). Dokl. AN Belarusi, 41 (1997), no.6, 13-16.

[1] M. van den Bergh *The algebraic index of a division algebra.* Lect. Notes in Math. 1197 (1985) 190-206.

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

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

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

[Serre] J.-P.Serre. *Cohomologie Galoisienne.* Springer-Verlag, 1964.

[Hall59] M.Hall. *The theory of groups.* N.Y. MacMillan, 1959.

[Mac63] S.Maclane. *Homology.* Die grundlehren der mathematischen wissenschaften. Springer-Verlag, 1963.

[Pie82] R.S.Pierce. *Associative algebras.* Graduate Texts in Mathematics 88, Springer-Verlag, 1982.