Brauer groups of local elliptic and hyperelliptic curves and central division algebras over their function fields

by
Vyacheslav Yanchevskii
and
Gennady Margolin

Abstract. We compute the torsion part of the unramified Brauer group of the function field of any elliptic curve defined over a local field of characteristc zero. For the case of a non dyadic ground field we prove that all elements of the 2-torsion part can be represented by quaternion algebras and describe them in an explicit form. We obtain a similar result for hyperelliptic curves with good reduction such that their defining equation $y^2 = f(x)$ satisfies the condition deg $f(x) \not\equiv 0 (\bmod 4)$.

Contents

1 Introduction

Let $K|k$ be a function field, i.e. assume that the field K is finitely generated, as a field, over the field k and let $Br_{nr}(K|k)$ be the unramified Brauer group of K (with respect to k). Let X be a smooth projective connected variety over field k of characteristic zero and $K = k(X)$ be its function field. It is known (see e.g. [6]) that there is a natural inclusion of $Br\ X$ in $Br(K)$ ($Br\ X$ denotes the Brauer group of X [5]) and this inclusion identifies $Br\ X$ with uramified Brauer group $Br_{nr}(K|k)$. (Below we shall write $Br\ X$ instead of $Br_{nr}(K|k)$ keeping in mind this identification).

The group $Br\ X$ is of great importance for many problems (it is enough to mention the rationality problem of varieties, the problem of Brauer-Manin obstructions to various Hasse principles and finally the classical problem of description of finite-dimensional division algebras over function fields). (see [6],[20], [21].)

In this paper we shall be interested in the problem of the description of $Br\ X$ for smooth geometrically connected projective curves over local fields, more precisely, for finite extention k of $\boldsymbol{Q}_p$. The classical class field theory gives us a complete description of the Brauer group $Br(k)$ of k (and also of finite dimensional central division algebras over k). But if $k(X)$ is a function field of a smooth geometrically connected projective variety over k the situation is much more complicated. In spite of many results obtained in connection with the developing of multidimensional class field theory ([18],[19]), unfortunately, we have not such a complete description as in the classical situation even in case of curves X (a "complete" description here means a presentation of each element of $Br(k(X))$ by the corresponding central division algebra over $k(X)$, in other words, it means a description of all central division algebras over $k(X)$). The Tradition of local-to-global principles suggest to investigate the local before the global situation . In case of curves X over k it means to investigate the groups $Br(k_v(X_v))$ for all v, where k_v is a completion of k with respect to a valuation v of k, and $X_v = X\ \times_k\ k_v$. (By Tsen's theorem $Br(k_v(X_v))$ is trivial in case of a complex v and its structure is well-known for real v according to [1], [2], [3] and [17]).

Thus the main unknown case in this situation is the case of a non-archimedian v, so below by a local field we shall understand a finite extension of the field of p-adic numbers $\boldsymbol{Q}_p$. Let now X be a smooth geometrically connected projective curve over local field k. Then it follows from [4], that there is an exact sequence

$$0 \longrightarrow Br\ X \longrightarrow Br(k(X)) \xrightarrow{\phi} \coprod_{P\in X} \chi(G_P) \xrightarrow{\psi} \chi(G) \longrightarrow 0,$$

where for a separable closure k_s of k, $G = Gal(k_s|k)$, $G_P = Gal((k_P)_s|k_P)$, k_P is the residue field of $P \in X$ and $\chi(G_P)$, $\chi(G)$ are the groups of continuous characters of G_P and G respectively (for definitions of ϕ and ψ see [4]). In view of this sequence the group $Im\ \phi$ is known, so the group of $Br\ X$ is of main interest for the description of $Br(k(X))$. The structure of $Br\ X$ is well-known in the case of curves of genus zero, but even in the case of elliptic curves the complete structure of $Br\ X$ is unknown. More generally, one can consider a smooth connected projective model X of an affine curve defined by an equation $y^2 = f(x)$, where $f(x)$ is a polynomial with coefficients in k without multiple roots and one can ask: what is known about the structure of $Br\ X$? One of the goals of our paper is to answer some questions related to the previous one. Since $Br\ X$ is an abelian periodic group, the main problem of its description is to describe, for any m, the m-torsion part of $Br\ X$. Below we give a complete description of the abstract structure of ${}_mBr\ X$ in the case of an elliptic curve X over k. Among the groups ${}_mBr\ X$ the group ${}_2Br\ X$ is of great importance, because the elements of ${}_2Br\ X$ are represented by central division algebras with involutions and there is the following connection of ${}_2Br\ X$ with the theory of quadratic forms according to Merkuriev's result [22] saying that ${}_2Br(k(x)) \cong I^2/I^3$, where I is the fundamental ideal of the Witt ring of $k(X)$. Our next main result is an explicit presentation of elements of ${}_2Br\ X$ by quaternion algebras for the case that k is non-dyadic and X is either an elliptic or a hyperelliptic curve defined by an equation $y^2 = f(x)$, where $deg\, f(x) \not\equiv 0 (mod\, 4)$.

The paper is organized as follows. In section 2 we set up the notations, recall some definitions and results needed in the sequel. We also prove some preliminary statements on fields and curves. In section 3 we obtain a reduction of the problem of the description of ${}_mBr\ X$ for a curve over a local field k to the problem of the calculation of the m-torsion of the group $Pic^0X(k)$ of k-rational points of its jacobian. Section 4 and 5 are devoted to the calculation of 2-torsion part of ${}_2Pic^0X(k)$ for a hyperelliptic curve X with good reduction and to the presentation of all elements of ${}_2Br\ X$ by quaternion algebras over $k(X)$. In section 6 we present a complete list of minimal Weierstrass equations for arbitrary elliptic curves over local fields. In section 7 we describe all groups ${}_mBr\ X$ for elliptic curves X in terms of their group structure. The rest of the paper is devoted to the description of the presentation of elements of ${}_2Br\ X$ by quaternion algebras for arbitrary elliptic curves defined over non-dyadic fields.

The authors would like to thank J.-L. Colliot-Thélène, A.S. Merkuriev, J.-P. Tignol and U. Rehmann for helpful discussions.

Also, the first named author wants to thank the Sonderforschungsbereich 343 ("Diskrete Strukturen in der Mathematik") for its hospitality.

2 Notations and preliminary results

Below we shall use the following notations. For any set X, by $|X|$ we will denote the cardinality of X. If A is an arbitrary additively written abelian group, by ${}_nA$ (respectively by nA) will be denoted the kernel (respectively image) of multiplication by n. The character group of A will be denoted by $\chi(A)$. For any commutative ring R with unity, by R^* will be denoted the group of invertible elements (with respect to multiplication) of R. Any element $\mu_m \in R^*$ of order m will be called a primitive m-th root of unity. If F is a field and μ_m is a primitive m-th root of unity, then $(m, char\ F) = 1$. Let F_s be a separable closure of F. The Galois group of the extension $F_s|F$ will be denoted by $G(F)$. For any discrete $G(F)$-module A, by $H^i(F, A)$ we shall denote the i-th cohomology group $H^i(G(F), A)$ of $G(F)$ with coefficients in A. By $Br(F)$ we shall denote the Brauer group of F, i.e. the group of similarity classes of central simple F-algebras whose homological interpretation is $H^2(F, F_s^*)$ (if C is a central simple algebra over F, its similarity class will be denoted by $[C]$). A quaternion algebra over field F will be denoted by either $((a\,,\,b)|\,F)$ or

$$\left(\frac{a\,,\,b}{F}\right).$$

In the sequel we shall need some special information on fields and curves.

Finite fields

$\boldsymbol{F}_q$ will denote the finite field consisting of q elements. For any field $\boldsymbol{F}_q$ of odd characteristic the subgroup $(\boldsymbol{F}_q^*)^2$ of $\boldsymbol{F}_q^*$ is of index 2 in $\boldsymbol{F}_q^*$. For $u \in \boldsymbol{F}_q^*$ set $(u/q) = 1$, if $u \in (\boldsymbol{F}_q^*)^2$ and $(u/q) = -1$ otherwise. We shall say that a combination $(+,+)$ (respectively $(-,-)$) is realized (in $\boldsymbol{F}_q^*$) if there exists $u \in \boldsymbol{F}_q^*$ such that $u+1 \neq 0$ and $(u/q) = ((u+1)/q) = 1$ (respectively $(u/q) = ((u+1)/q) = -1$. Similarly we shall say that a combination $(-,+)$ (respectively $(+,-)$) is realized (in $\boldsymbol{F}_q^*$) if there exists $u \in \boldsymbol{F}_q^*$ such that $u+1 \neq 0$ and $(u/q) = -1$, $((u+1)/q) = 1$ (respectively $(u/q) = 1$, $((u+1)/q) = -1$.

We shall need also the following lemma about the realization of these combinations.

Lemma 1 *Let char $\boldsymbol{F}_q \neq 2$. Then for any $q \geq 7$ all above combinations are realized in $\boldsymbol{F}_q^*$. In $\boldsymbol{F}_5^*$ the only combination which is not realized is $(+,+)$ and in $\boldsymbol{F}_3^*$ only the combination $(+,-)$ is realized.*

Proof. The straightforward computation shows that the lemma is true in the cases $q = 3, 5$. Let $q = p$ be a prime number and $p \geq 7$. Let $\{x_n\}$ be a sequence such that $x_n = (n/p)$, $n = 1, 2, \ldots, p-2$. Since $x_1 = 1$ and there exists at least one element $x_i \notin (\boldsymbol{F}_q^*)^2$, one can conclude that the combination $(+,-)$ is realized. Observe also that the sequence $\{x_n\}$ does not coincide with the sequence $\{(-1)^{n+1}\}$. (Otherwise $x_4 = -1$ and this is not the case). It means that at least one of the combinations $(+,+)$, $(-,-)$ is realized. Let firstly $(-1/p) = -1$. If $(u/p) = ((u+1)/p) = 1$, then it follows that $((-u-1)/p) = ((-u)/p) = -1$ i.e. both of the combinations are realized. Similarly if $(u/p) = ((u+1)/p) = -1$, then $((-u-1)/p) = ((-u)/p) = 1$. Assume that the combination $(-,+)$ is not realized in $\boldsymbol{F}_q^*$. It is known that the number of squares in $(\boldsymbol{F}_q^*)^2$ is equal to the number of non-squares and is equal to $(p-1)/2$. If in $\{x_n\}$ there is an element x_i such that $i \leq (p-1)/2$, then the combination $(-,+)$ is realized. If $x_1 = x_2 = \ldots = x_{(p-1)/2} = 1$ then $(2/p) = (((p-1)/2)/p) = 1$. But in this case $(-1/p) = (((p-1)/2)/p)(2/p) = 1$ contrary to our assumption. Thus the combination $(-,+)$ is realized in $\boldsymbol{F}_q^*$ if $(-1/p) = 1$.

Let now $(-1/p) = 1$. If $(u/p) = 1, ((u+1)/p) = -1$, then $((-u-1)/p) = -1, ((-u)/p) = 1$ and the combination $(-,+)$ is realized. Assume further that the combination $(-,-)$ is not realized. Then in the sequence $\{x_n\}$ the element $(+1)$ follows to each (-1) and since $x_1 = 1$ this contradicts to the fact that numbers of squares and non-squares in $\boldsymbol{F}_q^*$ are equal. If the combination $(+,+)$ is not realized in $\boldsymbol{F}_q^*$, then in view of $(1/p) = (4/p) = 1$ one has $(2/p) = (3/p) = -1$ and $(-1/p) = (-4/p) = 1$, $(-2/p) = (-3/p) = -1$, and $2 \neq -3$. Furthermore in the sequence $\{x_n\}$ the element $(+1)$ follows to each (-1). After eliminating from $\{x_n\}$ all pairs (x_i, x_{i+1}) where $x_i = -1$, $x_{i+1} = 1$ we shall have only one element $(+1) = (-1/p)$ and at least two elements (-1) corresponding to $(3/p)$ and $(-2/p)$ but this is impossible. Thus our lemma is proved for any prime $p \geq 7$.

If m is odd, then all non-squares in $\boldsymbol{F}_q^*$ are non-squares in $\boldsymbol{F}_{q^m}{}^*$, so our lemma is true for any field $\boldsymbol{F}_{p^m}$ where m is odd and $p \geq 7$. Let m be arbitrary and $q = p^m$. Let us show that all combinations are realized in $\boldsymbol{F}_{q^2}{}^*$. Since $\boldsymbol{F}_q^* \subset (\boldsymbol{F}_{q^2}{}^*)^2$, the combination $(+,+)$ is realized in $\boldsymbol{F}_{q^2}{}^*$. One can see also that there exists an element $\mu \in \boldsymbol{F}_{q^2}{}^* \setminus \boldsymbol{F}_q^*$ such that there exist both squares and non-squares lying in the coset $\mu + \boldsymbol{F}_q$. Really, if it is not the case, consider elements $\eta, \theta \in \boldsymbol{F}_{q^2}{}^* \setminus \boldsymbol{F}_q^*$ lying in distinct cosets modulo $\boldsymbol{F}_q$. Then the elements $\theta(\eta-\theta)^{-1}+1$ and $\theta(\eta-\theta)^{-1}$ lie in one coset modulo $\boldsymbol{F}_q$ and therefore

$$\left(\frac{\theta(\eta-\theta)^{-1}+1}{q^2}\right)=\left(\frac{\theta(\eta-\theta)^{-1}}{q^2}\right).$$

It follows then

$$\left(\frac{\eta}{q^2}\right)=\left(\frac{(\eta-\theta)+\theta}{q^2}\right)=\left(\frac{(\eta-\theta)(\theta(\eta-\theta)^{-1}+1)}{q^2}\right)= \\ \left(\frac{\eta-\theta}{q^2}\right)\left(\frac{\theta(\eta-\theta)^{-1}}{q^2}\right)=\left(\frac{\theta}{q^2}\right).$$

Hence $(\eta/q^2)=(\theta/q^2)$. Since by assumption all elements of $\mu+\boldsymbol{F}_q$ simultaneously either squares or non-squares we conclude that the set $\boldsymbol{F}_{q^2}{}^* \setminus \boldsymbol{F}_q^*$ consists either of squares or of non-squares and since the cardinality of the set $\boldsymbol{F}_{q^2}{}^* \setminus \boldsymbol{F}_q^*$ is equal to q^2-q and $q^2-q>(q^2-1)/2$ we are lead to a contradiction. Hence there exists an element $\mu \in \boldsymbol{F}_{q^2}{}^* \setminus \boldsymbol{F}_q^*$ such that in coset $\mu+\boldsymbol{F}_q$ there are squares and non-squares. Let μ be a square. Consider a sequence $\{z_n\}$ defined by $z_n=((\mu+(n-1))/q^2)$. Then $z_1=1$. Since not all of the elements in $\mu+\boldsymbol{F}_q$ are squares, then we conclude that there exists such i that $z_i=1$ and $z_{i+1}=-1$. Since $z_{j+p}=z_j$ for any j we have that the combination $(-,+)$ is also realized. It is obvious that in $\boldsymbol{F}_{q^2}{}^* \setminus \boldsymbol{F}_q^*$ the number of squares is greater than the number of non-squares, therefore there exists an element $\mu \in \boldsymbol{F}_{q^2}{}^* \setminus \boldsymbol{F}_q^*$ such that the number of squares in the coset $\mu+\boldsymbol{F}_q$ is greater than the number of non-squares. But then the combination $(-,-)$ is realized among the elements of this coset. Thus our lemma is proved for all finite fields of characteristic greater than 5.

Finally, let *char* $\boldsymbol{F}_q$ be equal to either 3 or 5. In this case the proof of our lemma is quite similar to that of the proof in the above case. Let now $\boldsymbol{F}_q$ be an extension of odd degree of $\boldsymbol{F}_p$, where p is equal to either 3 or 5. If for any $\mu \in \boldsymbol{F}_q^* \setminus \boldsymbol{F}_p^*$ the coset $\mu+\boldsymbol{F}_p$ consists either only of squares or only of non-squares, then for any $\eta \in \boldsymbol{F}_q^* \setminus \boldsymbol{F}_p^*$

$$\left(\frac{1+(\eta-1)^{-1}}{q^2}\right)=\left(\frac{\eta-1}{q^2}\right)$$

and

$$\left(\frac{\eta}{q^2}\right)=\left(\frac{(\eta-1)+1}{q^2}\right)=\left(\frac{(\eta-1)(1+(\eta-1)^{-1})}{q^2}\right)= \\ \left(\frac{\eta-1}{q^2}\right)\left(\frac{1+(\eta-1)^{-1}}{q^2}\right)=\left(\frac{\eta-1}{q^2}\right)^2=1.$$

But the equality $(\eta/q^2)=1$ is impossible for every $\eta \in \boldsymbol{F}_q^* \setminus \boldsymbol{F}_p^*$. Hence there exists an element $\mu \in \boldsymbol{F}_q^* \setminus \boldsymbol{F}_p^*$ such that the coset $\mu+\boldsymbol{F}_p$ contains squares and non-squares. Therefore one can conclude that the combinations $(+,-)$ and $(-,+)$ are realized in $\boldsymbol{F}_q^*$. If $\mu+\boldsymbol{F}_p$ is a coset containing squares and non-squares, $\mu \in \boldsymbol{F}_q^* \setminus \boldsymbol{F}_p^*$, then since it consists of odd number of elements we conclude that at least one of the combinations $(+,+)$, $(-,-)$ is realized in $\mu+\boldsymbol{F}_p$. If the combination $(+,+)$ is realized but $(-,-)$ is not realized, then the number of squares in $\mu + \boldsymbol{F}_p$ is greater than the number of non-squares and since the numbers of squares and non-squares in $\boldsymbol{F}_q^* \setminus \boldsymbol{F}_p^*$ are equal we have that the number of squares in$\boldsymbol{F}_q^* \setminus (\boldsymbol{F}_p \bigcup (\mu + \boldsymbol{F}_p^*))$ is greater than the number of non-squares. Therefore there exists $\tau \in \boldsymbol{F}_q^* \setminus (\boldsymbol{F}_p \bigcup (\mu + \boldsymbol{F}_p^*))$, such that the combination $(-,-)$ is realized in $\tau + \boldsymbol{F}_p$. Similar arguments are true in the case, where the combination $(-,-)$ is realized but it is not the case for $(+,+)$.

Q.E.D.

Proposition 1 *Let $s(x) = \alpha(x^2 + ax + b)$ be a polynomial in $\boldsymbol{F}_q[x]$ without multiple roots and $q \geq 7$, q odd. Then there exist elements $u, v \in \boldsymbol{F}_q$ such that $u \neq -a/2, v \neq 0$ with the property $v^2 = \alpha(u^2 + au + b)$.*

Proof. Set $\Delta = a^2 - 4b$. Then

$$s(x) = -\frac{\alpha\Delta}{4}(\frac{-4}{\Delta}(x + a/2)^2 + 1).$$

Let

$$a) \quad -\Delta \in (\boldsymbol{F}_q^*)^2, \alpha \in (\boldsymbol{F}_q^*)^2.$$

Then $-\alpha\Delta/4, -4/\Delta \in (\boldsymbol{F}_q^*)^2$. By lemma 1 there exists $c \in \boldsymbol{F}_q^*$ such that $c^2 + 1 = t^2, t \in \boldsymbol{F}_q^*$. Set $u = -a/2 + \sqrt{-\Delta c^2/4}$. Then $s(u) = -\alpha\Delta t^2/4$ and $v = t\sqrt{-\alpha\Delta/4}$ is satisfied our condition. Similar arguments work in cases

$$b) \quad -\Delta \in (\boldsymbol{F}_q^*)^2, \alpha \notin (\boldsymbol{F}_q^*)^2;$$

$$c) \quad -\Delta \notin (\boldsymbol{F}_q^*)^2, \alpha \in (\boldsymbol{F}_q^*)^2;$$

$$d) \quad -\Delta \notin (\boldsymbol{F}_q^*)^2, \alpha \notin (\boldsymbol{F}_q^*)^2,$$

so that the proposition is proved.

Let us denote by $\boldsymbol{F}_q^*(\delta)$ the set of specializations (lying in $\boldsymbol{F}_q^*$) of the polynomial $x^2 + \delta$ $(\delta \in \boldsymbol{F}_q^*)$ by means of elements in $\boldsymbol{F}_q^*$.

Corollary 1 *Let $q \geq 7$ and q odd. Then the set $\boldsymbol{F}_q^*(\delta)$ contains both squares and non-squares. The set $\boldsymbol{F}_5^*(\delta)$ contains both squares and non-squares, if $\delta \notin (\boldsymbol{F}_5^*)^2$ and consists only of non-squares otherwise. The set $\boldsymbol{F}_3^*(\delta)$ is empty, if $\delta \notin (\boldsymbol{F}_3^*)^2$ and consists of non-square otherwise.*

Local fields of characteristic zero

Any such field k is a finite extention of the field $\boldsymbol{Q}_p$ of p-adic numbers for a suitable prime number p. The unique extension to k of the canonical valuation on $\boldsymbol{Q}_p$ will be denoted by v_k. O_k, M_k, $\bar{k}$ will denote respectively the valuation ring of v_k, its maximal ideal and the residue field O_k/M_k. For any $a \in O_k$, $\bar{a}$ will denote the image under canonical epimorphism from O_k onto O_k/M_k. If $f(x) = \sum_{i=0}^n a_i x^i$ is a polynomial with coefficients in O_k, then $\bar{f}(x)$ will denote the polynomial $\sum_{i=0}^n \bar{a}_i x^i$. Any generator of M_k will be called a prime element of k. A dyadic field is a field k such that *char* $\bar{k} = 2$. The group of units of k is the group O_k^*. The subgroup $1 + M_k = \{1 + a | a \in M_k\}$ has the property which is a consequence of more general one.

Proposition 2 *Let F be a field with a henselian valuation v, $M(F)$ be its maximal ideal and $\bar{F}$ be the residue field of F. If $(n, char\ \bar{F}) = 1$, then for any $a \in 1 + M(F)$ there exists the unique element $b \in 1 + M(F)$ such that $b^n = a$.*

Thus $u \in O_k^*$ is the n-th power in k^* if and only if $\bar{u} \in (\bar{k}^*)^n$ $((n, char\ k) = 1)$. In particular, $u \in O_k^*$ is a square in a non-dyadic field k if and only if $\bar{u}$ is a square in $\bar{k}^*$.

¿From now on we fix for the case of a non-dyadic k an element $\alpha \in O_k^* \setminus (O_k^*)^2$ and a prime element π of k.

Hyperelliptic curves

Let F be a field and $char\ F = 0$. By $\boldsymbol{P}^n$ we shall denote the n-dimensional projective space over algebraic closure of F. Any point of $\boldsymbol{P}^n$ with homogeneous coordinates $x_0, \ldots, x_n$ will be denoted by $(x_0 : x_1 : \ldots : x_n)$. Let also $\boldsymbol{A}_i^n$ be the subset of $\boldsymbol{P}^n$ consisting of points with non-zero i-th homogeneous coordinate. For any polynomial $f(x) \in F[x]$ of degree m without multiple roots let $C_0|F$ be an affine plane curve given by the equation $y^2 = f(x)$ and g be the genus of C_0, so that

$$g = \begin{cases} (m-1)/2 & \text{if } m \text{ is odd,} \\ (m-2)/2 & \text{if } m \text{ is even.} \end{cases}$$

Then the closure C of the image of C_0 under the mapping

$$\phi:\ C \longrightarrow \boldsymbol{P}^{g+2},\ \ (x, y) \mapsto (1 : x : x^2 : x^3 : \ldots : x^{g+1} : y)$$

is called a hyperelliptic curve corresponding to the curve defined by the equation $y^2 = f(x)$. It is known that C is a smooth geometrically connected projective curve and

$$C = \begin{cases} (C \bigcap \boldsymbol{A}_0^{g+2}) \bigcup P_\infty & \text{if } m \text{ is odd,} \\ (C \bigcap \boldsymbol{A}_0^{g+2}) \bigcup P_{\infty_1} \bigcup P_{\infty_2} & \text{if } m \text{ is even,} \end{cases}$$

where C_0 and $C \bigcap \boldsymbol{A}_0^{g+2}$ are isomorphic under the map ϕ, $P_\infty, P_{\infty_1}, P_{\infty_2} \in \boldsymbol{A}_{g+1}^{g+2}$ and $P_\infty = (0 : 0 : \ldots : 1 : 0)$, $\{P_{\infty_1, P_{\infty_2}}\} = \{(0 : 0 : \ldots : 1 : \pm\sqrt{a_m})\}$, a_m is the leading coefficient of $f(x)$. We shall denote by ϕ_C the hyperelliptic projection $\phi_C :\ C \longrightarrow \boldsymbol{P}^1$ given by

$$\phi_C(P) = \begin{cases} (x : 1) & \text{if } P = (1 : x : x^2 : \ldots : x^{g+1} : y), \\ (1 : 0) & \text{if } P \notin \boldsymbol{A}_0^{g+2} \end{cases}$$

for any point $P \in C$. If $F_s(C)$ (respectively $F(C)$) is the field of rational (respectively F-defined rational) functions on C, then the hyperelliptic projection induces an embedding

$$\phi_C^* :\ F_s(x) \hookrightarrow F_s(C)\ \ (\phi_C^*|_{F(x)} :\ F(x) \longrightarrow F(C)), \text{ i.e.}$$

$$\phi_C^* :\ F_s(x) \hookrightarrow F_s(x)(\sqrt{f(x)})\ \ (\phi_C^*|_{F(x)} :\ F(x) \longrightarrow F(x)(\sqrt{f(x)})).$$

Let now $P \in C$ and $F_s[C]_P$ be the local ring of C at P. Then the canonical valuation $\bar{v}_P$ on $F_s[C]_P$ extends uniquely to $F_s(C)$, so that for any $P \in C$ we have a canonical valuation v_P on $F(C)$ (v_P is the restriction of $\bar{v}_P$ on $F(C)$).We shall need also to know an explicit description of $F(C)_{v_P}$ which is the completion of $F(C)$ with respect to valuation v_P and explicit description of embedding of $F(C)$ into $F(C)_{v_P}$. Below we shall write $F(C)_P$ instead of $F(C)_{v_P}$.

Let $L < z >$, for any field L, denote the field of formal power series in z over L. Then the needed description can be done as follows.

Lemma 2 *Let C be as above, $P \in C$, $\phi_C(P) = (a:1)$, $h(x)$ be the minimal polynomial of a over F. Then*

$$F(C)_P \cong \begin{cases} F(a)(\sqrt{f(a)}) < h >, & \text{if } h(x) \text{ does not divide } f(x), \\ F(a) < h > (\sqrt{g(a)h(\tilde{x})}), & \text{if } f(x) = g(x)h(x), \end{cases}$$

where $F(C)$ is embedded in $F(C)_P$ by sending x to some series $\tilde{x} \in F(a) < h >$ such that $\tilde{x} \equiv a (mod\, h(x))$. We shall identify $F(C)$ with the corresponding subfield in $F(C)_P$ and x with $\tilde{x}$ in $F(C) \subset F(C)_P$.

Lemma 3 *Let C be as above. Then*

$$F(C)_{P_\infty} \cong F < \sqrt{x^{-1}} >,$$

$$F(C)_{P_{\infty_i}} \cong F < x^{-1} > (\sqrt{a_m}),\ i = 1, 2$$

and $F(C)$ is embedded in $F(C)_{P_\infty}$ (in $F(C)_{P_{\infty_i}}$) by sending x to x^{-1}.

The proofs of both lemmas follow immediately from the above description of points of C and the definition of v_P.

We also recall the structure of the restrictions to $k(x)$ of v_P. Any such restriction is a discrete valuation of $k(x)$ and it is of the following form. If $P \neq P_\infty$ then there exists an irreducible polynomial $f(x)$ such that the restriction $v_{f(x)}$ of v_P is a discrete valuation with $f(x)$ as a uniformizer. If the v_∞ is the restriction of v_{P_∞} to $k(x)$, then it is a discrete valuation with x^{-1} as a uniformizer. The completions of $F(x)$ with respect to $v_{f(x)}$ and v_∞ are respectively of the form $F(\theta) < f(x) >$, $F < x^{-1} >$, where θ is a root of $f(x)$ and the embedding $F(x) \hookrightarrow F(\theta) < f(x) >$ sends x to some series $\tilde{x}$ such that $\tilde{x} \equiv \theta (mod\, f(x))$. For convenience we shall denote by $F(C)_\infty$ any completion of $F(C)$ such that its restriction to $F(x)$ is v_∞. Both such completions are isomorphic.

We shall need some facts about hyperelliptic curves defined over local fields. One can prove without difficulties the following lemma.

Lemma 4 *Let C_0 be a plane curve defined by an equation $y^2 = f(x)$, where $f(x)$ is a polynomial over non-dyadic local field k of zero characteristic and $f(x)$ has no multiple roots. Then C_0 is k-isomorphic to a plane curve defined by an equation $y^2 = Af_0(x)$, where $f_0(x)$ is a unitary polynomial with coefficients in O_k without multiple roots and $A \in \{1, \alpha, \pi, \pi\alpha\}$. In the case of odd $deg\, f(x)$ without loss of generality one can assume that $A = 1$.*

One says that a hyperelliptic curve $C|k$ has *good reduction* if it corresponds to a curve with defining equation $y^2 = Af_0(x)$ as in the above lemma where $A \in \{1, \alpha\}$ and $\bar{f}_0(x) \in \bar{k}[x]$ is a polynomial without multiple roots.

Elliptic curves

An elliptic curve $E|F$ is a smooth geometrically connected projective curve of genus one with an F-rational point. It is well-known that any elliptic curve is isomorphic to the projective closure of a plane curve defined by an equation

$$y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in F,$$

which is called a Weierstrass equation. (Below we shall denote by P_∞ the point $(0:1:0) \in E$). A Weierstrass equation is unique up to change of variables of the form:

$$x = u^2x' + r, \quad y = u^3y' + su^2x' + t, \text{ with } u, r, s, t \in F, u \neq 0.$$

Moreover, any smooth plane projective curve defined by a Weierstrass equation over F is an elliptic curve over F. A change of the variable y to $(y - a_1x - a_3)/2$ gives in case of *char* $F \neq 2$ a Weierstrass equation

$$y^2 = 4x^3 + b_2x^2 + b_4x + b_6, \text{ where}$$

$$b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6.$$

Set also

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 - a_2a_3^2 - a_4^2,$$

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

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad j = c_4^3/\Delta, \text{if } \Delta \neq 0.$$

A condition $\Delta \neq 0$ is equivalent to smoothness of the curve defined by a Weierstrass equation, so that for an elliptic curve the j-invariant j is always defined and moreover, any two elliptic curves defined over F are F_s-isomorphic if and only if they have the same j-invariants. If E is defined by an equation $y^2 = x(x^2 + Ax + B)$, then

$$c_4 = 16(A^2 - 3B), \quad c_6 = 32A(2A^2 + 9B), \quad \Delta = 16B^2(A^2 - 4B).$$

Let now k be a local field, *char* $k = 0$ and E an elliptic curve defined over k. Then a Weierstrass equation of E can be chosen satisfying condition $a_i \in O_k$. For any extension K of k let $E(K)$ will denote the set of K-rational points of E. There is a group law on $E(K)$ with point $(0:1:0)$ as a neutral element and such that for any $P_0 = (x_0, y_0) \in E$ $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$, the x-coordinate of point $2P_0$ is defined by

$$x(2P_0) = \frac{x_0^4 - b_4x_0^2 - 2b_6x_0 - b_8}{4x_0^3 + b_2x_0^2 + 2b_4x_0 + b_6},$$

and for any two points $P_1 = (x_1, y_1),\ \ P_2 = (x_2, y_2)$ satisfying condition $P_1 \neq \pm P_2$

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2.$$

In particular, if the curve equation is of the form $y^2 = x(x^2 + Ax + B)$, then $x(2P_0) = (x_0^2 - B)^2/(4y_0^2)$ provided $y_0 \neq 0$ and $2P_0 = 0$ if $y_0 = 0$.

The natural homomorphism $O_k \longrightarrow O_k/M_k = \bar{k}$ leads us to the definition of reduction $\tilde{E}|\bar{k}$ of E as the closure in $\boldsymbol{P}^2$ of a curve defined by the equation

$$y^2 + \bar{a}_1xy + \bar{a}_2y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6.$$

Since any point in $E(k) \subset \boldsymbol{P}^2(k)$ has homogeneous coordinates belonging to O_k, so there exists a uniquely determined reduction mapping $R : E(k) \longrightarrow \tilde{E}(\bar{k})$. In general $\tilde{E}$ is not an elliptic curve, therefore it is natural to consider the set $\tilde{E}_{ns}(\bar{k})$ of smooth points of $\tilde{E}$ and two subsets in $E(k)$

$$E_0(k) = \{P \in E(k) : R(P) \in \tilde{E}_{ns}(\bar{k})\}$$

$$E_1(k) = \{P \in E(k) : R(P) = 0\}$$

It is clear that the group law $E(k)$ induces by means of reduction mapping the group law on $\tilde{E}_{ns}(\bar{k})$ and the restriction R to $E_0(k)$ is an epimophism of $E_0(k)$ onto $\tilde{E}_{ns}(\bar{k})$ with the kernel E_1. All elliptic curves are divided into two classes. The first class consists of curves E with good reduction i.e. $\tilde{E}$ is an elliptic curve. The second one consists of curves E with bad reduction (i.e. $\tilde{E}$ is not an elliptic curve). In the last case one distinguishes additive and multiplicative reduction according to whether $\tilde{E}$ has as a singular point a cusp or a node. In the case of multiplicative reduction one distinguishes also split and non-split multiplicative reduction according to whether both tangent lines to the singular point either are defined over $\bar{k}$ or not.

We shall need also some information on groups $E_0(k)$, $E_1(k)$, $\tilde{E}_{ns}(\bar{k})$ and $E(k)/E_0(k)$.

Proposition 3 *If E is an elliptic curve over k, then in case of additive reduction $\tilde{E}_{ns}(\bar{k})$ is isomorphic to additive group $\bar{k}^+$ of $\bar{k}$ and in case of multiplicative reduction $\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^*$.*

Proposition 4 *$E_1(k)$ is non-torsion group and if $(m, char\ \bar{k}) = 1$, then $E_1(k)$ is uniquely m-divisible.*

¿From the last proposition follows:

Proposition 5 *If $(m, char\ \bar{k}) = 1$, then ${}_mE(k) \cong {}_m\tilde{E}_{ns}(\bar{k})$.*

Theorem 1 (Kodaira,Neron) *If E has split multiplicative reduction over k, then the group $E(k)/E_0(k)$ is cyclic of order $v_k(\Delta) = -v_k(j)$. In all other cases, $E(k)/E_0(k)$ is a finite group of order at most 4.*

In view of the discretness of v_k there exists a Weierstrass equation for E with coefficients in O_k and with minimal value of $v_k(\Delta)$. Each such an equation is called a minimal one for E. It is known that minimal equation for E is uniquely defined up to change of coordinates of the form

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t, \quad \text{where } u \in O_k^*,\ r, s, t \in O_k.$$

Moreover, $\Delta = u^{12}\Delta'$, where Δ' is the discriminant of the equation for E after a change of coordinates. In non-dyadic case it always exists a minimal Weierstrass equation for E such that $a_1 = a_3 = 0$. Really, if a minimal Weierstrass equation such that at least one of the coefficients $a_1 = a_3$ is non-zero, the the change of variables $x = (1/2)x'$, $y = (1/2)y' - (a_1/4)x' - a_3/4$ leads us to the equation

$$(y')^2 = (x')^3 + A(x')^2 + Bx' + C,$$

which is minimal in view of $\Delta' = 2^{12}\Delta$. If now $y^2 = x^3 + A_1x^2 + B_1x + C_1$ and $y^2 = x^3 + A_2x^2 + B_2x + C_2$ are two minimal Weierstrass equations for E, then it is clear that the type of splitting of polynomials is the same and this gives us the possibility after the change of variable $x = x' - a$ to differ three following types of minimal Weierstrass equations.

1.Split case: $y^2 = x(x-e_1)(x-e_2)$, $e_1, e_2 \in O_k$.

2.Semi-split case: $y^2 = x(x^2+Ax+B)$, $A, B \in O_k$ and the polynomial $x(x^2+Ax+B)$ is ireducible over k.

3.Non-split case: $y^2 = x^3+Mx^2+Nx+P$, $M, N, P \in O_k$ and the polynomial $x^3 + Mx^2+Nx+P$ is irreducible over k.

Below we shall need the following simplified variant of Tate's algorithm [7] (together with the corresponding information on the group $E(k)/E_0(k)$), describing the procedure of finding a minimal Weierstrass equation for E given by a Weierstrass one with coefficients in O_k.

So, let $char\ \bar{k} \neq 2$ and a curve E be given by a Weierstrass equation

$$y^2 = f(x), \tag{1}$$

where $f(x) = x^3+a_2x^2+a_4x+a_6$, $a_2, a_4, a_6 \in O_k$ and $\Delta = -8(2a_2^2+a_4^2+64a_6^2-36a_2a_4a_6)$. Then the equation (1) is minimal in all listed below cases $1-6$ with one exceptional case $6c_4$. Let us consider this cases.

1. If $\Delta \in O_k^*$, then E is a curve with good reduction and $E(k)/E_0(k) =<0>$.

   Below $\Delta \notin O_k^*$. In this case the polynomial $\bar{f}(x)$ has a multiple root $\tilde{u}$. Then the change $x' = x-u$, where $\bar{u} = \tilde{u}$, shows that without loss of generality one may assume $a_4, a_6 \in M_k$.

2. Let $a_2 \in O_k^*$. Then E is a curve with multiplicative reduction and $E(k)/E_0(k) \cong \boldsymbol{Z}/m$.

   Below $a_2, a_4, a_6 \in M_k$.

3. If $v_k(a_6) = 1$, then $E(k)/E_0(k) =<0>$.

4. Let $\pi^2 | a_6$ and $v_k(a_4) = 1$. Then $E(k)/E_0(k) \cong \boldsymbol{Z}/2$.

5. If $v_k(a_6) = 2$, $\pi^2 | a_4$, then $E(k)/E_0(k) \cong \boldsymbol{Z}/3$, if $\overline{a_6\pi^{-2}} \in (\bar{k}^*)^2$, and $E(k)/E_0(k) = < 0 >$ otherwise.

6. Let π^3 divides a_6, π^2 divides a_4 and π divides a_2. Then by means of the change of variables $x = \pi x', y = \pi^2 y'$ we lead to the equation

$$\pi(y')^2 = P(x'), \text{ where } P(x') = \frac{1}{\pi^3} f(\pi x'). \tag{2}$$

$6a$ The polynomial $\bar{P}(x)$ has no multiple roots. In this case $[E(k) : E_0(k)] = 1+$(the number of roots of $\bar{P}(x)$ in $\bar{k}$).

$6b$ The polynomial $\bar{P}(x)$ has a double root. In this case the index $[E(k) : E_0(k)]$ is equal either 2 or 4.

$6c$ If $\bar{P} = (x-\beta)^3$, $\beta \in \bar{k}$, then the change of variables $x = x'-u$, $\bar{u} = \beta$ shows that without loss of generality one may assume, that $\beta = 0$. It then follows that π divides a_2, π^3 divides a_4 and π^4 divides a_6.

$6c_1$ Let $v_k(a_6)=4$. Then $E(k)/E_0(k)\cong \boldsymbol{Z}/3$, if $\overline{a_6\pi^{-4}}\in(\bar{k}^*)^2$ and $E(k)/E_0(k)\ =<0>$ otherwise.

$6c_2$ If $\pi^5|a_6$ and $v_k(a_4)=3$, then $E(k)/E_0(k)\cong \boldsymbol{Z}/2$.

$6c_3$ If $v_k(a_6)=5,\ \pi^4|a_4$, then $E(k)/E_0(k)=<0>$..

$6c_4$ If $\pi^6|a_6$ and $\pi^4|a_4$, then the equation (1) is not minimal.

Below we shall also need the following

Proposition 6 *Let $E|k$ be a curve with additive reduction. Then*

1. If k is non-dyadic, then $[E(k):E_0(k)]=3$ if and only if one has non-split case and E can be given by the minimal equation of the form $y^2=x^3+a_2x^2+a_4x+a_6$ and one of the following conditions is satisfied

(i) $\pi|a_2,\pi^2|a_4,v_k(a_6)=2$ *and* $a_6\in(k^*)^2$,

(ii) $\pi^2|a_2,\pi^3|a_4,v_k(a_6)=4$ *and* $a_6\in(k^*)^2$.

2. If k is dyadic, then $[E(k):E_0(k)]=3$ if and only if E can be given by an equation of the form $y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ and one of the following conditions is satisfied

(i) $\pi|a_1,v_k(a_3)=1,\pi|a_4,\pi^2|a_6,\pi^3|(a_2a_3^2-a_4^2)$ *and the polynomial* $x^2+\overline{a_3\pi^{-1}}x+\overline{a_6\pi^{-2}}$ *has roots in* $\bar{k}$,

(ii) $\pi|a_1,\pi^2|a_3,\pi^3|a_4,\pi^4|a_6$, *and the polynomial* $x^2+\overline{a_3\pi^{-1}}x+\overline{a_6\pi^{-2}}$ *has distinct roots in* $\bar{k}$.

Proof. In view of a simplified variant of Tate's algorithm for a non-dyadic field k it follows that $[E(k):E_0(k)]=3$ holds only in two cases:

$a)$ one has the case 5 together with the condition $\overline{a_6\pi^{-2}}\in(k^*)^2$ and this leads us just to the condition $1(i)$;

$b)$ one has the case $6c_1$ together with condition $\overline{a_6\pi^{-4}}\in(k^*)^2$ and this leads us to the condition $1(ii)$.

Consider now the case of dyadic field k. By using the general algorithm of Tate one concludes that in case of additive reduction $[E(k):E_0(k)]=3$ if and only if one has one of the two following cases (in notations of [7]).

$a)$ one has the case IV with the following additional condition: the polynomial $x^2+\overline{a_3\pi^{-1}}x+\overline{a_6\pi^{-2}}$ has roots in $\bar{k}$,

$b)$ one has the case IV^* and the polynomial $x^2+\overline{a_3\pi^{-2}}x+\overline{a_6\pi^{-4}}$ has roots in $\bar{k}$.

To obtain necessary and sufficient conditions on coefficients of minimal equations corresponding to the cases IV and IV^* let us repeat partially Tate's algorithm.

Since the reduction of the curve is bad we may assume that $\pi|a_3, \pi|a_4$ and $\pi|a_6$. The additivity of the reduction implies the condition $\pi|b_2$ and in the dyadic case it is equivalent to $\pi|a_1$.

The case denoted by Kodaira's symbol II is not realized, so $\pi^2|a_6$.

The case III can be excluded by assuming $\pi^3|b_8$, and this is equivalent to $\pi^3|(a_2a_3^2-a_4^2)$.

Then the case IV is realized if and only if either $\pi^3|\bar{|}b_8$ or $v(a_3)=1$.

Let now $\pi^2|a_3$. Then one may assume that $\pi|a_1, \pi|a_2, \pi^2|a_3, \pi^2|a_4$ and $\pi^3|a_6$.

Omitting the cases I_0^* and I_ν^* in which we are not interested, we obtain that the polynomial $x^3+\overline{a_2\pi^{-1}}x^2+\overline{a_4\pi^{-2}}x+\overline{a_6\pi^{-3}}$ has a root of multiplicity 3. Then without loss of generality we may assume that $\pi^2|a_2, \pi^3|a_4$ and $\pi^4|a_6$.

Finally, to have the case IV^* we need to satisfy a condition: the polynomial $x^2+\overline{a_3\pi^{-2}}x+\overline{a_6\pi^{-3}}$ has distinct roots.

Q.E.D.

3 Torsion of Brauer groups of curves and their Jacobians

Let k be a field of zero characteristic, C a smooth geometrically irreducible projective curve, defined over k and $\bar{C}=C\times_k k_s$. We shall also denote by $Pic(C)$ (respectively $Pic^0(C)$) the Picard group of C (respectively the subgroup of $Pic(C)$ consisting of divisor classes of degree zero). All other notations being as in section 2.

One has the following exact sequence [5]

$$0\longrightarrow Pic(C)\longrightarrow H^0(k,Pic(\bar{C}))\longrightarrow Br(k)\xrightarrow{\alpha} BrC\longrightarrow$$
$$\longrightarrow H^1(k,Pic(\bar{C}))\longrightarrow H^3(k,k_s^*)$$

Let now k be a local field. Then $H^3(k,k_s^*)=0$ ([8]) and we have an exact sequence

$$0\longrightarrow Pic(C)\longrightarrow H^0(k,Pic(\bar{C}))\longrightarrow Br(k)\xrightarrow{\alpha} BrC\longrightarrow$$
$$\longrightarrow H^1(k,Pic(\bar{C}))\longrightarrow 0$$

If I is the index of X (i.e. the greatest common divisor of degrees of k-rational divisors on C), then by Roquette-Lichtenbaum theorem the order of the kernel of α is equal to I, so we have from the last sequence a new one:

$$0\longrightarrow Br(k)/(\boldsymbol{Z}/I)\longrightarrow BrC\longrightarrow H^1(k,Pic(\bar{C}))\longrightarrow 0.$$

Passing in this sequence to n-torsion we shall have

$$0\longrightarrow \boldsymbol{Z}/n\longrightarrow {}_nBrC\longrightarrow {}_nH^1(k,Pic(\bar{C}))\longrightarrow 0$$

or equivalently by

$${}_nBrC\cong \boldsymbol{Z}/n\oplus {}_nH^1(k,Pic(\bar{C})).$$

So to determine the group ${}_nBrC$ one needs to compute the group ${}_nH^1(k, Pic(\bar{C}))$. To do this let us consider an exact sequence of G-modules

$$0 \longrightarrow Pic^0(\bar{C}) \longrightarrow Pic(\bar{C}) \xrightarrow{deg} \boldsymbol{Z} \longrightarrow 0$$

which is induced by the degree homomorphism. The corresponding part of the long exact sequence is

$$H^0(k, Pic(\bar{C})) \xrightarrow{deg_*} \boldsymbol{Z} \longrightarrow H^1(k, Pic^0(\bar{C})) \longrightarrow H^1(k, Pic(\bar{C})) \longrightarrow H^1(k, \boldsymbol{Z}) = 0.$$

If P is a period of C (i.e. the greatest common divisor of degrees of divisor classes in $H^0(k, Pic(\bar{C}))$), then we have an exact sequence

$$0 \longrightarrow \boldsymbol{Z}/P \longrightarrow H^1(k, Pic^0(\bar{C})) \longrightarrow H^1(k, Pic(\bar{C})) \longrightarrow 0.$$

The last sequence induces the following exact one

$$0 \longrightarrow {}_n(\boldsymbol{Z}/P) \longrightarrow {}_nH^1(k, Pic^0(\bar{C})) \longrightarrow {}_nH^1(k, Pic(\bar{C})) \longrightarrow$$
$$\longrightarrow (\boldsymbol{Z}/P)/n \longrightarrow H^1(k, Pic^0(\bar{C}))/n \longrightarrow H^1(k, Pic(\bar{C}))/n \longrightarrow 0.$$

So we have the exact sequence

$$0 \longrightarrow \boldsymbol{Z}/(P,n) \longrightarrow {}_nH^1(k, Pic^0(\bar{C})) \longrightarrow {}_nH^1(k, Pic(\bar{C})) \longrightarrow \tag{3}$$
$$\longrightarrow \boldsymbol{Z}/(P,n) \longrightarrow H^1(k, Pic^0(\bar{C}))/n \longrightarrow H^1(k, Pic(\bar{C}))/n \longrightarrow 0.$$

We shall need a specialization of this to the case of hyperelliptic (elliptic) curve. To obtain it let us prove firstly the following

Lemma 5 *Let C be a hyperelliptic (elliptic) curve, then $I = P$.*

Proof. In elliptic case the lemma is known (see [5]). And in hyperelliptic case it follows easy from Lichtenbaum's theorem ([5]). Really, by this theorem P divides the number $g-1$, where g is the genus of C, $I = P$ or $2P$ and if $I = 2P$, then $(g-1)/P$ is odd. One knows also (see [23]) that I equals either 1 or 2. So we have $I, P \leq 2$. In case $P = 2$ it is clear that $I = 2$. In the case $P = 1, I \neq 1$ by Lichtenbaum's theorem $g-1$ is odd. But then g is even and in this situation (see [23]) C has a k-rational point, so $I = 1$ and this contradiction proves lemma in this case.

Corollary 2 *The period of hyperelliptic (elliptic) curve is equal either* 1 *or* 2*. If C has a k-rational point, then it follows that $P = 1$. In particular, $P = 1$ for elliptic curve C.*

Now we have

Lemma 6 *Let C be either elliptic or hyperelliptic. Then*

i) For C having the index $I = 1$ (in particular if C has a k-rational point)

$${}_nH^1(k, Pic^0(\bar{C})) \cong {}_nH^1(k, Pic(\bar{C}))$$

ii) For C being a hyperelliptic curve with $I = 2$ we have an isomorphism

$$ {}_nH^1(k, Pic^0(\bar{C})) \cong {}_nH^1(k, Pic(\bar{C})) $$

if n is odd, and the following exact sequence if n is even

$$ 0 \longrightarrow \mathbf{Z}/2 \longrightarrow {}_nH^1(k, Pic^0(\bar{C})) \longrightarrow {}_nH^1(k, Pic(\bar{C})) \longrightarrow \mathbf{Z}/2 \longrightarrow $$

$$ \longrightarrow H^1(k, Pic^0(\bar{C}))/n \longrightarrow H^1(k, Pic(\bar{C}))/n \longrightarrow 0. $$

iii) If k is non-dyadic and C has good reduction, then

$$ {}_2H^1(k, Pic^0(\bar{C})) \cong {}_2H^1(k, Pic(\bar{C})). $$

Proof. All things except the last isomorphism immediately follow from the sequence (3). The last result will be obtained in lemma 9, because in this case $I = 1$.

It is clear now that for calculation of the group $H^1(k, Pic(\bar{C}))$ one needs to calculate the group $H^1(k, Pic^0(\bar{C}))$. Let now C be as at the beginning of the section. Then we have

Lemma 7

$$ {}_nH^1(k, Pic^0(\bar{C})) \cong J_C(k)/n, $$

where $J_C(k)$ is the group of k-rational points of the Jacobian J_C of $\bar{C}$ (see [16]).

Proof. By Tate's duality [9]

$$ H^1(k, J_C) \cong \chi(\hat{J}_C(k)), $$

where $\hat{G}_C$ is dual to J_C and $\chi(\hat{J}_C(k))$ is the character group of the group of k-rational points of $\hat{J}_C$. Clearly,

$$ {}_nH^1(k, J_C) \cong {}_n\chi(\hat{J}_C(k)). $$

Since k-varieties J_C and $\hat{J}_C$ are k-isomorphic, so we have

$$ {}_nH^1(k, J_C) \cong {}_n\chi(J_C(k)) $$

and

$$ {}_nJ_C(k) \cong Hom(J_C(k), \mathbf{Z}/n) \cong Hom(J_C(k)/n, \mathbf{Z}/n) \cong J_C(k)/n $$

(the last isomorphism is valid in view of finiteness of the group $J_C(k)/n$). Finally, observe that J_C and $Pic^0(\bar{C})$ are isomorphic as G-modules, so ${}_nH^1(k, J_C) \cong {}_nH^1(k, Pic^0(\bar{C}))$.

The above consideration gives the following

Proposition 7 *Let C be a hyperelliptic (elliptic) curve over a local field k. Then*

$$ {}_nBr\ C \cong {}_nBr(k) \oplus J_C(k)/n $$

in the following cases:

i) *C is elliptic;*

ii) *C is hyperelliptic, $I = 1$;*

iii) *C is hyperelliptic, n is odd;*

iv) *$n = 2$, $I = 2$, k is non-dyadic and C has good reduction.*

The proof follows immediately from the previous lemma.
Furthermore one has the following

Theorem 2 *Let C be as in i)–iv) of the above proposition. Then*

i) $|\,{}_nBr\ C| = n|\,{}_nJ_C(k)||\bar{k}|^{v_k(n)}$,

ii) *$Br\ C \cong {}_nBr(k) \oplus {}_nJ_C(k)$, if n is relatively prime to char $\bar{k}$.*

Proof. It is known (see [10]) that $|J_C(k)/n| = |\,{}_nJ_C(k)||\bar{k}|^{v_k(n)}$, so i) follows immediately from proposition 7. To prove ii) observe firstly that, if n is prime, then an isomorphism ${}_nJ_C(k)$ and $J_C(k)$ follows from the fact they have the same orders. Furthermore, without loss of generality one can assume that $n = p^r$, where p is prime and $(p, char\ k) = 1$. There exists s such that for every $r > s$ ${}_{p^r}J_C(k) = {}_{p^s}J_C(k)$. Then for any $r \geq s$ let us consider the canonical isomorphism

$$\phi_r : p^r J_C(k)/(\,{}_{p^r}J_C(k) \bigcap p^r J_C(k) \cong (\,{}_{p^r}J_C(k) + p^r J_C(k))/p^r J_C(k).$$

Since ${}_{p^{r+1}}J_C(k) = {}_{p^r}J_C(k)$, then ${}_{p^r}J_C(k) \bigcap p^r J_C(k) = <0>$. In fact $x \in {}_{p^r}J_C(k) \bigcap p^r J_C(k)$, then $p^r x = 0$ and $x = p^r y, y \in J_C(k)$. So one concludes that $p^{2r} y = 0$ and $y \in {}_{p^{2r}}J_C(k)$. But ${}_{p^{2r}}J_C(k) = {}_{p^r}J_C(k)$ and therefore $p^r y = 0$, i.e. $x = 0$. Since the orders of the groups ${}_{p^r}J_C(k)$ and $J_C(k)/p^r$ are coincided (see [10]), then the composition of ϕ_r and the embedding $(\,{}_{p^r}J_C(k) + p^r J_C(k))/p^r J_C(k) \longrightarrow J_C(k)/p^r$ is an isomorphism. Thus for $r \geq s$ proposition 7 can be reformulated as follows

$${}_{p^r}Br\ C \overset{\theta_r}{\cong} {}_{p^r}Br(k) \oplus {}_{p^r}J_C(k).$$

Let now $1 \leq r \leq s$ and $x \in {}_{p^r}Br\ C$. Since ${}_{p^r}Br\ C \subset {}_{p^r}Br\ C$, then for an isomorphism θ_s we have $p^r \theta_s(x) = \theta_s(p^r x) = 0$. If $\theta_s(x) = a+b$, $\quad a \in {}_{p^s}Br(k)$, $\quad b \in {}_{p^s}J_C(k)$, then $p^r a = 0$ and $p^r b = 0$. This means that $a \in_{p^r} (\,{}_{p^s}Br(k)) = {}_{p^r}Br(k)$ and $b \in_{p^r} (\,{}_{p^s}J_C(k)) = {}_{p^r}J_C(k)$, so we have $\theta_s(\,{}_{p^r}Br\ C) \subset {}_{p^r}Br(k) \oplus {}_{p^r}J_C(k)$. In view of proposition 7 and the equality of orders of groups ${}_{p^r}J_C(k)$ and $J_C(k)/p^r$ one has immediately that the last inclusion is in fact an equality. Thus the second part of the proposition is proved.

Q.E.D.

Corollary 3 *Let C be as in the preceding theorem. Then ${}_nJ_C(k) \cong J_C(k)/n$.*

4 The group ${}_2Pic^0(\bar{C})(k)$

In view of the above considerations it follows immediately that in order to describe the group ${}_2Br\ C$ we need to know the group ${}_2Pic^0(\bar{C})(k)$. Let us begin with description of the group ${}_2Pic^0\ \bar{C}$. Assume all notations and conventions on curve C from section 2 are valid and P_∞ in the case of elliptic curve is the infinite point $(0:1:0)$.

Proposition 8 *Let C be either elliptic or hyperelliptic, and let $m = deg\, f$ be odd. Then ${}_2Pic^0\, \bar{C}$ is the group of order 2^{m-1} and consists of elements*

$$[0],\quad \left[\sum_{i\in I} P_i - P_\infty\right],\ \text{where } I \subset \{1,2\dots,m\}, |I| < \frac{m}{2}.$$

Let m be even. Then ${}_2Pic^0\, \bar{C}$ is the group of order 2^{m-2} and consists of the elements

$$[0],\quad \left[\sum_{i\in I} P_i - \frac{I}{2}(P_{\infty_1} + P_{\infty_2})\right],\ \text{where } I \subset \{1,2\dots,m\}, |I| \le \frac{m}{2}, |I| \text{ is even }.$$

Moreover,

$$\left[\sum_{i\in I} P_i - \frac{I}{2}(P_{\infty_1} + P_{\infty_2})\right] = \left[\sum_{j\in J} P_j - \frac{J}{2}(P_{\infty_1} + P_{\infty_2})\right]$$

if and only if m is even, $|I| = |J| = m/2$ and $I \bigcap J = \{1, 2, \dots, m\}$.

Proof. By the well-known formula $|\ {}_2Pic^0\ \bar{C}| = 2^{2g}$, so $|\ {}_2Pic^0\ \bar{C}| = 2^{m-1}$ if m is odd and $|\ {}_2Pic^0\ \bar{C}| = 2^{m-2}$ if m is even. Let m is odd. Then it is easy to see that the principal divisor $(x - e_i)$ is equal to $2P_i - 2P_\infty$, so that $2[P_i - P_\infty] = [0]$. Therefore $[P_i - P_\infty] \in {}_2Pic^0(\bar{C})$. We have also $2(y) = (y^2) = (f(x)) = (\prod_{i=1}^m (x-e_i)) = \sum_{i=1}^m (x-e_i) = \sum_{i=1}^m (2P_i - 2P_\infty) = 2(\sum_{i=1}^m P_i - mP_\infty)$, i.e. $(y) = \sum_{i=1}^m -mP_\infty$. For any non-zero divisor class N from the group generated by $\{[(P_i - P_\infty)]\}$, $(i = 1, 2, \dots, m)$ we have for an appropriate $I \subset \{1, 2, \dots, m\}$ $N = [\sum_{i\in I} P_i - |I|P_\infty]$ and keeping in mind $(y) = [\sum_{i=1}^m P_i - mP_\infty]$ we may assume that $0 < |I| < m/2$. Let us show now that for any $J \subset \{1, 2, \dots, m\}$ such that $0 < |J| < m/2$ we have $[\sum_{i\in I} P_i - |I|P_\infty] = [\sum_{j\in J} P_j - |J|P_\infty]$ if and only if $I = J$. To prove this let us observe first of all that without loss of generality we may assume that $I \bigcap J = \{\emptyset\}$. Moreover, it follows from the equality $(x-e_j) = [2P_j - 2P_\infty]$ that $[-P_j + P_\infty] = [P_j - P_\infty]$, so the equality $[\sum_{j\in J} P_j - |J|P_\infty - (\sum_{i\in I} P_i - |I|P_\infty)]$ is equivalent to $[\sum_{i\in I\bigcup J} P_i - |I \bigcup J|P_\infty)] = 0$, where $|I \bigcup J| < m$. Therefore to prove our statement we need only to prove that for any $0 < |I| < m$ the divisor $\sum_{i\in I} P_i - |I|P_\infty$ is principal. Really, assume that there exists an element $u \in k_s(C)$ such that $(u) = \sum_{i\in I} P_i - |I|P_\infty$. Let $v = \prod_{i\in I}(x - e_i)$. Then $(v) = \sum_{i\in I}(x - e_i) = 2(\sum_{i\in I} P_i) - 2P_\infty = 2(u) = (u^2)$ and we have that $u^2 = c\prod_{i\in I}(x-e_i)$, $c \in k_s$, i.e. $\prod_{i\in I}(x-e_i) \in (k_s(C)^*)^2$. Since $k_s(C) = k_s(x)(\sqrt{f(x)})$ and $\prod_{i\in I}(x-e_i) \notin (k_s(x)^*)^2$, we have $f = g^2\prod_{i\in I}(x-e_i)$, $g \in k_s(x)$, where $g = P(x)/Q(x)$, $(P(x), Q(x)) = 1$. Hence $Q(x)^2 f = P(x)^2\prod_{i\in I}(x - e_i)$ i.e.$Q(x)^2\prod_{i\notin I}(x - e_i) = P(x)^2$, and this is possible if and only if I is either $\{\emptyset\}$ or $\{1, 2, \dots, m\}$. Now it is clear that the number of distinct elements of the form $[\sum_{i\in I} P_i - |I|P_\infty]$, $|I| < m/2$ is equal to 2^{m-1}, so the proposition is proved in case of odd m.

In case of even m $(x - e_i) = 2P_i - P_{\infty_1} - P_{\infty_2}$. So that $2[P_i + P_j - P_{\infty_1} - P_{\infty_2}] = [2P_i - P_{\infty_1} - P_{\infty_2}] + [2P_j - P_{\infty_1} - P_{\infty_2} = [0] + [0] = [0]$, i.e. $[P_i + P_j - P_{\infty_1} - P_{\infty_2}] \in {}_2Pic^0(\bar{C})$. Furthermore, $(y) = \sum_{i=1}^m P_i - (m/2)(P_{\infty_1} + P_{\infty_2})$, therefore the non-zero elements of the group generated by $\{[P_i + P_j - P_{\infty_1} - P_{\infty_2}]\}$ consists of elements $[\sum_{i\in I} P_i - (|I|/2)(P_{\infty_1} + P_{\infty_2})$, where $I \in \{1, 2, \dots, m\}$, $|I|$ is even and $|I| \le m/2$. Let us show that $\sum_{i\in I} P_i - (|I|/2)(P_{\infty_1} + P_{\infty_2})$ is not a principal divisor if I is not equal either to $\{\emptyset\}$ or $\{1, 2, \dots, m\}$. Similarly to the above arguments, let $\sum_{i\in I} P_i - (|I|/2)(P_{\infty_1} + P_{\infty_2}) = (u)$, where $u \in k_s(C)$ and $v = \prod_{i\in I}(x - e_i)$. Then $(v) = 2(u)$, $v/(u^2) \in k_s$, i.e. $v \in (k_s(C)^*)^2$. Hence

$\prod_{i\in I}(x-e_i) \in (k_s(x)(\sqrt{f})^*)^2$ and this is impossible. Now the rest of the proof is as follows. Similarly to the case of odd m one can prove that for any $J \subset \{1,2,\ldots,m\}$ such that $|J|$ is even and $0 < |J| < m/2$

$$[\sum_{i\in I} P_i - \frac{|I|}{2}(P_{\infty_1} + P_{\infty_2})] = [\sum_{j\in J} P_j - \frac{|J|}{2}(P_{\infty_1} + P_{\infty_2})]$$

if and only if $|I| = |J| = m/2, I \bigcap J = \{\emptyset\}, I \bigcup J = \{1,2,\ldots,m\}$. Finally, one can observe that the number of distinct elements of the form $[\sum_{i\in I} P_i - (|I|/2)(P_{\infty_1} + P_{\infty_2})]$, where $0 \le |I| < m/2$ is equal to 2^{m-2}, so the proposition is proved.

Now we prove the following

Theorem 3 *Let C be either elliptic or hyperelliptic curve and $m \not\equiv 0(mod\, 4)$. Then*

i) *in case of odd m $({}_2Pic^0(\bar{C}))(k)$ consists of $[0]$ and pairwise distinct non-zero elements of the form $[\sum_{i\in I} P_i - |I|P_\infty]$, where $0 < |I| < m/2$ and the set $\{P_1, P_2, \ldots, P_{|I|}\}$ is $G(k)$-invariant;*

ii) *in case of even m, $m \not\equiv 0(mod\, 4)$ $({}_2Pic^0(\bar{C}))(k)$ consists of $[0]$ and of pairwise distinct non-zero elements of the form $[\sum_{i\in I} P_i - (|I|/2)(P_{\infty_1} + P_{\infty_2})]$, where $|I|$ is even, $0 < |I| < m/2$ and the set $\{P_1, P_2, \ldots, P_{|I|}\}$ is $G(k)$-invariant.*

Proof. In view of proposition 8 in case i) to prove the theorem it is enough to see that from

$$[\sum_{i\in I} P_i - |I|P_\infty] = [\sum_{i\in I} P_i - |I|P_\infty]^g$$

for the above I and any $g \in G(k)$ it follows $\{P_1, P_2, \ldots, P_{|I|}\}$ is $G(k)$-invariant. We have

$$[\sum_{i\in I} P_i - |I|P_\infty]^g = [\sum_{i\in I} P_i^g - |I|P_\infty],$$

so that

$$[\sum_{i\in I} P_i - |I|P_\infty] + [\sum_{i\in I} P_i^g - |I|P_\infty] = [0].$$

In view of proposition 8 and keeping in mind $[0] = [2P_i - 2P_\infty]$ one can conclude that $\{P_1, P_2, \ldots, P_{|I|}\} = \{P_1^g, P_2^g, \ldots, P_{|I|}^g\}$. Since g is an arbitrary element of $G(k)$ the set $\{P_1, P_2, \ldots, P_{|I|}\}$ is $G(k)$-invariant. Similar arguments work in case ii).

Corollary 4 *There is a bijective correspondence between elements of $({}_2Pic^0(\bar{C}))(k)$ and monic divisors of $f(x)$ defined over k of degree less than $m/2$ in case i) and monic divisors of $f(x)$ defined over k of even degree less than $m/2$ in case ii).*

Proof. For any $G(k)$-invariant set one can associate a divisor $\prod_{i\in I}(x - e_i)$ of $f(x)$.

5 Presentation of elements of ${}_2Br\ C$ by central simple algebras (case of elliptic and hyperelliptic curves with good reduction)

In this section we shall use notations and conventions of sections 2 and 3 and k will be assumed to be non-dyadic. In particular, our curve C will correspond to the affine curve defined by the equation $y^2 = f(x)$, $f(x) = Af_0(x)$, where f_0 is a monic polynomial in $O_k[x]$, $\bar{f}(x)$ has no multiple roots and A is either 1 or α (α is any fixed non-square in O_k^*), m is the degree of $f(x)$ and $A = 1$ if m is odd.

To find central simple algebras for presentation of elements of ${}_2Br\ C$ we shall need to prove some preliminary statements.

Lemma 8 *Let $g(x)$ be a divisor of $f(x)$ and let either m be odd or $deg\, g(x)$ even. Then a quaternion algebra $((B\ ,\ g(x)\ )|\ k(C))$ is unramified over $k(C)$ for any $B \in k^*$.*

Proof. It is enough to prove that $((B\ ,\ g(x)\ )|\ k(C)) \otimes_{k(C)} k(C)_{f_i}$ is unramified over $k(C)_{f_i}$ for any monic irreducible divisor f_i of $g(x)$, $((B\ ,\ g(x)\ )|\ k(C)) \otimes_{k(C)} k(C)_{P_\infty}$ is unramified over $k(C)_{P_\infty}$ in case of odd m and $((B\ ,\ g(x)\ )|\ k(C)) \otimes_{k(C)} k(C)_{P_{\infty_i}}$ $(i = 1, 2)$ is unramified over $k(C)_{P_{\infty_i}}$ in case m is even. Let f_i be a polynomial as above and $F_i(\theta_i) = 0,\ \theta_i \in k_s$. Then

$$\left(\frac{B\ ,\ g(x)}{k(C)}\right) \otimes_{k(C)} k(C)_{f_i} \sim \left(\frac{B\ ,\ (g/f_i)(\theta)f_i(x)}{k(C)_{f_i}}\right) \sim$$

$$\left(\frac{B\ ,\ (g/f_i)(\theta_i)f_i(x)}{k(\theta_i) < f_i(x) > (\sqrt{(f/f_i)(x)f_i(x)})}\right) \sim \left(\frac{B\ ,\ (g/f_i)(\theta_i)(f/f_i)(\theta_i)}{k(\theta_i) < f_i > (\sqrt{(f/f_i)(\theta_i)f_i(x)})}\right).$$

The last algebra comes from the one over $k(\theta_i)$, so that it is unramified over $k(C)_{f_i}$.

If $g(x)$ is of even degree, $deg\, g(x) = 2t$, m is odd one has

$$\left(\frac{B\ ,\ g(x)}{k(C)}\right) \otimes_{k(C)} k(C)_{P_\infty} \sim \left(\frac{B\ ,\ g(1/z)}{k < z > (\sqrt{f(1/z)})}\right) \sim$$

$$\left(\frac{B\ ,\ g(1/z)z^{2t}}{k < z > (\sqrt{f(1/z)})}\right) \sim \left(\frac{B\ ,\ 1 + zP(z)}{k < z > (\sqrt{f(1/z)})}\right),$$

where $P(z)$ is the corresponding polynomial from $k[z]$. Since $1 + zP(z)$ is a square in $k < z >$ the last algebra is trivial and so it is unramified over $k(C)_\infty$. The same argument works in the case of even m for algebras $((B\ ,\ g(x)\ )|\ k(C)) \otimes_{k(C)} k(C)_{P_{\infty_i}}, i = 1, 2$. Let now $deg\, g(x) = 2t + 1$, $m = 2e + 1$. Then

$$\left(\frac{B\ ,\ g(1/z)}{k < z > (\sqrt{f(1/z)})}\right) \sim \left(\frac{B\ ,\ g(1/z)z^{2t+2}}{k < z > (\sqrt{f(1/z)})}\right) \sim$$

$$\left(\frac{B\ ,\ z(1 + zP(z))}{k < z > (\sqrt{f(1/z)})}\right) \sim \left(\frac{B\ ,\ z}{k < z > (\sqrt{f(1/z)})}\right).$$

Moreover,

$$k(C)_\infty \cong k<z>(\sqrt{z^{2e+2}f(1/z)}) \cong k<z>(\sqrt{Az}) \cong k<z>(\sqrt{z}),$$

so that

$$\left(\frac{B\ ,\ z}{k<z>(\sqrt{f(1/z)})}\right) \sim \left(\frac{B\ ,\ z}{k<z>(\sqrt{z})}\right) \sim \left(\frac{B\ ,\ 1}{k<z>(\sqrt{z})}\right).$$

The last algebra is obviously unramified over $k(C)_{P_\infty}$ and lemma is proved.

Proposition 9 *Let A be either 1 or α, $g = Bg_0$, B either 1 or α and $g_0 \in O_k[x]$ be a monic divisor of $f(x)$, $f_0 = g_0\hat{g}_0$. If $\bar{g}_0 \notin \bar{k}[x]^2$, $\bar{\hat{g}}_0 \notin \bar{k}[x]^2$ then*

$$P = \left(\frac{\pi\ ,\ g}{k(C)}\right) \not\sim 1.$$

Proof. Let $P \sim 1$. Then $k(x)(\sqrt{f(x)})$ is a splitting field for P, and therefore is isomorphic to a maximal subfield of $((\pi\ ,\ g\ )|\ k(x))$. It is known that in this case $f(x) = \varepsilon_1^2\pi + \varepsilon_2^2 g - \varepsilon_3^2\pi g$, $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in k(x)$. If s is a common denominator of $\varepsilon_1, \varepsilon_2, \varepsilon_3$, then $s^2 f = \mu_1^2\pi + \mu_2^2 g - \mu_3^2\pi g$, where $\mu_1, \mu_2, \mu_3 \in k[x]$. Since g_0 divides $f(x)$ it also divides μ_1. Hence $As^2\hat{g}_0 = \eta_1^2\pi g_0 + B\eta_2^2 - B\eta_3^2\pi$, where $\eta_1 = \mu_1 g_0^{-1}, \eta_i = \mu_i, i = 2,3$. Let now $\pi^{-n_i} = cont_\pi \eta_i$ be the content of a polynomial η_i, $n = \max_{1\le i\le 3}\{\eta_i\}, t = s\pi^n, \delta_i = \eta_i\pi^n$. Then $t^2 A\hat{g}_0 = \delta_1^2\pi g_0 + B\delta_2^2 - B\delta_3^2\pi$ and $\delta_i \in O_k[x]$, so we have $t \in O_k[x]$. If $n = n_2$, it implies that both δ_2 and t are primitive and it follows that $\bar{A}\bar{t}^2\bar{\hat{g}}_0 = \bar{B}\bar{\delta}_2^2, \overline{AB\hat{g}_0} \in \bar{k}[x]^2$. The last condition contradicts to our assumption if $A = B$ and impossible if $A \neq B$. So we should conclude that $cont_\pi\delta_2 = \pi^r, r > 0$. It implies that $cont_\pi t = \pi^l, l > 0$, $cont_\pi(t^2\hat{g}_0) = \pi^{2l}$, $cont_\pi(\delta^2) = \pi^{2r}$, so that a polynomial $\delta_1^2\pi g_0 - B\delta_3^2\pi$ has no π as its content. So one can conclude that $\bar{\delta}_1^2\bar{g}_0 - \bar{B}\bar{\delta}_3^2 = 0$. If δ_1 is primitive, then $\bar{g}_0 = \bar{B}(\bar{\delta}_3/\bar{\delta}_1)^2$ and this is impossible if $B = \alpha$ and contradicts to our assumption on $\bar{g}$ otherwise. If δ_1 is not primitive, then $n > n_2$, $n > n_1$, so that $n = n_3$ and δ_3 is primitive. This property of δ_3 in view of the equality $\bar{\delta}_1^2\bar{g}_0 - \bar{B}\bar{\delta}_3^2 = 0$ implies that $\bar{\delta}_1 \neq 0$, $\bar{B}\bar{g}_0 \in \bar{k}[x]^2$ and we have again a contradiction.

Q.E.D.

Before proving our main result we need to prove the following

Lemma 9 *Let k be a non-dyadic local field and let C have good reduction. If $((\pi\ ,\ \alpha\ )|\ k)$ is the quaternion division algebra over k, then $((\pi\ ,\ \alpha\ )|\ k(C))$ is a division algebra.*

Proof. Let $((\pi\ ,\ \alpha\ )|\ k(C)) \sim 1$. Then $k(C)$ is a splitting field for the division algebra $D_2 = ((\pi, \alpha)|\, k(x))$, so that $k(C)$ is a maximal subfield of D_2. Since C has good reduction $f(x) = Af_0(x)$, $A \in \{1, \alpha\}$ and the polynomial $f_0(x) \in O_k[x]$ is monic. Without loss of generality we may assume that $f(x) = P^2(x)\lambda(x)^{-2}$, where $P(x) \in ((\pi\ ,\ \alpha\ )|\ k) \otimes_k k[x]$, $\lambda(x) \in O_k[x]$ is primitive. Then it follows that $P(x)$ is also primitive, so we may consider the reduction of the above equality $\bar{f}(x) = \bar{P}^2(x)\bar{\lambda}(x)^{-2}$, so that $\bar{f}(x)$ has multiple roots and this contradicts to our assumption on reduction of C.

Now we can prove our main result on presentation of elements of ${}_2Br\ C$ by central simple algebras.

Theorem 4 *Let C be either an elliptic or a hyperelliptic curve with good reduction defined over non-dyadic local field and let $m \not\equiv 0(mod 4)$. Then ${}_2Br\ C$ has the following presentaition by central simple algebras.*

${}_2Br\ C$ consists of the following pairwise distinct elements:

$$\left[\left(\frac{\pi\ ,\ 1}{k(C)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha}{k(C)}\right)\right], \left[\left(\frac{\pi\ ,\ g(x)}{k(C)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha g(x)}{k(C)}\right)\right],$$

where:

i) if m is odd then $g(x)$ runs through all monic divisors of $f(x)$ of degree less than $m/2$;

ii) if m is even then $g(x)$ runs through all monic divisors of $f(x)$ of even degree less than $m/2$.

Proof. Let us observe firstly that the set of elements in the above list is the subgroup of ${}_2Br\ C$ both in both cases i) and ii). Really, all algebras except the first one are non-trivial by lemma 9 and proposition 9. Algebras $((\pi\ ,\ 1)|k(C))$ and $((\pi\ ,\ \alpha)|k(C))$ are unramified. Any other algebra from the list is unramified by lemma 8 and in view of the fact that the tensor product of two unramified algebras is also the unramified one. Algebras from the list are not pairwise isomorphic because the tensor products of two such algebras is similar to the algebra of the same form. Finally, the number of all elements in the list is equal to the order of the group ${}_2Br\ C$.

Q.E.D.

Remark 1 *In fact, the result similar to the theorem is true even in the case, where $m \equiv 0(mod 4)$ but its proof is more complicated. We shall publish it elsewhere.*

6 Minimal Weierstrass equations of elliptic curves over non-dyadic fields

In this section k will denote a non-dyadic local field.

Our main purpose is to obtain a list of minimal Weierstrass equations for elliptic curves defined over k. For the split case one has the following

Theorem 5 *Let E be an elliptic curve and assume we are in the splitting case. Then the following list contains a minimal Wierstrass equation of E and any equation of the list is the minimal Weierstrass equation for the curve defined by it.*

For the case of good reduction $y^2 = x(x-e_1)(x-e_2),\ e_1, e_2 \in O_k, \overline{e_1 e_2} \neq 0, \bar{e_1} \neq \bar{e_2}$.

For case of bad reduction *and appropriate $a, b \in O_k^*$ one has*

I_1. $y^2 = x(x+\alpha)(x-\pi^m a),\ \ m > 0$ (non-split multiplicative reduction).

I_2. $y^2 = x(x+1)(x-\pi^m a),\ \ m > 0$ (split multiplicative reduction).

II. $y^2 = x(x-\pi a)(x-\pi b),\ \ \bar{a} \neq \bar{b}$ (additive reduction).

III. $y^2 = x(x-\pi a)(x-\pi^m b),\ \ m > 1$ (additive reduction).

Proof. To prove theorem we can use Tate's algorithm. As was observed before, E has a minimal equation $(y')^2 = (x')^3 + A(x')^2 + Bx' + C$. If $x = x' - s$, where s is one of the roots of the equation, then E has a minimal equation of the form

$$y^2 = x(x - e_1)(x - e_2). \tag{4}$$

for appropriate $e_1, e_2 \in O_k$. In the case of good reduction we have immediately that $\bar{e}_1\bar{e}_2 \neq 0$ and $\bar{e}_1 \neq \bar{e}_2$.

Let now E has bad reduction. Then without loss of generality we may assume that $\bar{e}_2 = 0$ and

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_2 = -(e_1 + e_2)$, $a_4 = e_1e_2$, $a_6 = 0$ and $\pi | a_4$. If $\bar{e}_1 \neq 0$, then $v_k(a_2) = 0$ and we are in the case of multicative reduction. If $-e_1 \in (k^*)^2$ then replacing x by $x = x'(-e_1)$ gives an equation of the form

$$y^2 = x(x + 1)(x - \pi^m a),\ m > 0, a \in O_k^*$$

and reduction of E is split multiplicative. If $-e_1 \notin (k^*)^2$, then replacing x by $x = -\alpha e_1 x'$ gives an equation of the form

$$y^2 = x(x + \alpha)(x - \pi^m a),\ m > 0, a \in O_k^*$$

and reduction of E is non-split multiplicative.

Let E has additive reduction and $\bar{e}_1 = 0$, $\pi | a_2$. Since $a_6 = 0$, then the cases $3, 5$ of Tate's algorithm are not realized. Furthermore, $b_8 = -e_1e_2$, $\pi^3 | b_8$, and therefore the case is not realized. In the case 6 let us consider the polynomial $\bar{P}(T) = T(T - \overline{e_1\pi^{-1}})(T - \overline{e_2\pi^{-1}})$. For the case $6a$ we shall have an equation

$$y^2 = x(x - \pi a)(x - \pi b),\ a, b \in O_k^*, \bar{a} \neq \bar{b}.$$

In the case $6b$ there are three possibilities

$\alpha)$ $e_1\pi^{-1}, e_1\pi^{-1} \in O_k^*, \overline{e_1\pi^{-1}} = \overline{e_1\pi^{-1}}$;

$\beta)$ $e_1\pi^{-1} \in O_k^*, e_2\pi^{-1} \in M_k$;

$\gamma)$ $e_1\pi^{-1} \in M_k, e_2\pi^{-1} \in O_k^*$;

In the first case replacement x by $x' = x - e_1$, leads us to an equation of the form III.

In cases $\beta)$ and $\gamma)$ we have from the beginning an equation of the form III. Since $a_6 = 0$, then it follows that cases $6c_1$, $6c_3$ are not realized. It follows also from the minimality of initial equation that we do not need to consider the case $6c_4$. Finally, it remains to consider the case $6c_2$ for which $v_k(a_4) = 3$ and $\bar{e}_1 = \bar{e}_2 = 0$. From $a_4 = e_1e_2$ we can deduce that either $v_k(e_1) = 1$ and $v_k(e_2) = 2$ or $v_k(e_1) = 2$ and $v_k(e_2) = 1$. In both cases we leads to the equation of the form III with $m = 2$.

Q.E.D.

Theorem 6 *Let $E|k$ be an elliptic curve and assume we are in the semi-splitting case. Then the following list contains a minimal Weirstrass equation for E and any equation of the list is a minimal Weierstrass equation for the curve defined by it.*

For the case of good reduction $y^2 = x(x^2 + tx + n)$, $t, n \in O_k, \bar{t}^2 - 4\bar{n} \notin (\bar{k}^*)^2 \bigcup \{0\}$.

In the case of bad reduction we distinguish two possibilities $(a, b, c \in O_k^*)$

- *E has additive reduction.*

  A.a) 1. $y^2 = x(x^2 + \pi^m ax + \pi b),\ m > 0;$
  2. $y^2 = x(x^2 + \pi b);$
  3. $y^2 = x(x^2 + \pi^m ax + \pi^3 b),\ m > 1;$
  4. $y^2 = x(x^2 + \pi^3 b).$

  A.b) $b \notin (k^*)^2$.
  1. $y^2 = x(x^2 + \pi^m ax + \pi^2 b),\ m > 1, -1 \in (k^*)^2;$
  2. $y^2 = x(x^2 + \pi ax + \pi^2 b),\ \bar{a}^2 - 4\bar{b} \notin (\bar{k}^*)^2;$
  3. $y^2 = x(x^2 + \pi^2 b),\ -1 \in (k^*)^2.$

  A.c) $b \in (k^*)^2$.
  1. $y^2 = x(x^2 + \pi^2 b),\ -1 \notin (k^*)^2;$
  2. $y^2 = x(x^2 + \pi^m ax + \pi^2 b),\ m > 1, -1 \notin (k^*)^2;$
  3. $y^2 = x(x^2 + \pi ax + \pi^2 b),\ \bar{a}^2 - 4\bar{b} \notin (\bar{k}^*)^2 \bigcup \{0\};$
  4. $y^2 = x(x^2 + \pi ax + \pi^2 b),\ a/\sqrt{b} = 2 + \pi^{2r}c, r > 0, c \notin (k^*)^2.$

  A.d) $y^2 = x(x^2 + \pi ax + \pi^2 b),\ a/\sqrt{b} = 2 + \pi^{2r+1}c, r \geq 0, c\sqrt{b} \notin (k^*)^2.$

  A.e) $y^2 = x(x^2 + \pi ax + \pi^2 b),\ a/\sqrt{b} = 2 + \pi^{2r+1}c, r \geq 0, c\sqrt{b} \in (k^*)^2.$

  (In cases A.c)4, A.d) and A.e) elements $b \in (k^*)^2$ and $\sqrt{b}$ would be chosen satisfying condition $\overline{a/\sqrt{b}} = 2$.

- *E has multiplicative reduction.*

$$y^2 = x((x + a)^2 + \pi^s bx),\ s > 0.$$

  M.a) $s = 2m + 1$, *E has split reduction iff* $-a \in (k^*)^2$.

  M.b) $s = 2m, -a \notin (k^*)^2, -b \in (k^*)^2$, *$E$ has non-split reduction.*

  M.c) $s = 2m, -1 \in (k^*)^2, a \in (k^*)^2, b \notin (k^*)^2$, *$E$ has split reduction.*

  M.d) $s = 2m, -1 \notin (k^*)^2, a \notin (k^*)^2, b \in (k^*)^2$, *$E$ has split reduction.*

Proof. Let $y^2 = (x')^3 + A(x')^2 + Bx' + C,\ A, B, C \in O_k$ be a minimal Weirstrass equation for E. In semi-split case $(x')^3 + A(x')^2 + Bx' + C = (x' - \mu)((x')^2 + \nu x' + \tau)$ and replacing x by $x = x' - \mu$ we lead to an equation of the form

$$y^2 = x(x^2 + tx + n), \tag{5}$$

where $t, n \in O_k$ and the polynomial is irreducible over k $(a_2 = t, a_4 = n, a_6 = 0, b_8 = -n^2)$.

In the case of good reduction the discriminant $\bar{t}^2 - 4\bar{n} \notin (\bar{k}^*)^2 \bigcup \{0\}$.

Let us consider the case of bad reduction. In this case the polynomial $x^2 + \bar{t}x + \bar{n}$ has a double root $\beta \in \bar{k}$.

If $\beta = 0$, then we have the case of additive reduction. Since $a_6 = 0$, the cases 3 and 5 from Tate's algorithm are not realized. If $v_k(n) = 1$ we have the case 4 and the equation (5) can be transformed either to $y^2 = x(x^2 + \pi^m ax + \pi b)$, or to $y^2 = x(x^2 + \pi b)$.

Let $\pi^2|n$. Then for the equation (5) we have one of the cases $6a-6c_3$. Let us consider the polynomial $\bar{P}(x)=x^3+\overline{t\pi^{-1}}x^2+\overline{n\pi^{-2}}x$.

In the case $6a$ we have $v_k(n)=2$ (i.e. $n=\pi^2 b$). Since the polynomial $x^2+\overline{t\pi^{-1}}x+\overline{n\pi^{-2}}$ has no multiple roots $(\overline{\pi^{-1}t})^2\neq 4\bar{b}$.

In case $\pi^2|t$ the last condition is valid so the equation (5) can be transformed to one of the following forms

$$y^2=x(x^2+\pi^m ax+\pi^2 b),\ m>1,$$

$$y^2=x(x^2+\pi^2 b).$$

If $t=\pi a$, then condition $\bar{a}^2\neq 4\bar{b}$ leads us either to the case $A.c)3$ or to the case $A.b)2$. Let us observe that in the case $6b$ of Tate's algorithm zero is not a double root of $P(x)$. Otherwise the polynomial $\bar{P}(x)/x$ would be split in two relatively prime factors and this is impossible because of Hensel lemma. Thus $n=\pi^2 b$ and $x^2+\overline{t\pi^{-1}}x+\overline{n\pi^{-2}}=(x-r)^2,\ r\neq 0$.

Then it follows that the equation (5) can be transformed to the form

$$y^2=x(x^2+\pi ax+\pi^2 b),$$

where $b\in(k^*)^2$, since $b=\gamma^2$ and $\bar{a}^2=4\bar{b}$. The case $6c_2$ corresponds just to cases $A.a)3, A.a)4$. Let us observe finally that cases $6c_1, 6c_3$ are not realized in view of $a_6=0$.

Let now $\beta\neq 0$. Since then $x^2+\bar{t}x+\bar{n}=(x-\beta)^2$, so $\bar{n}=\beta^2$ and there exist an element $a\in O_k^*$ such that $n=a^2$. $(\bar{t})^2=(2\bar{a})^2$, one can choose an element a such that $\bar{t}=2\bar{a}$ and $t=2a+\pi^s b,\ s>0$. In view of irreducibility x^2+tx+n over k we have $t\neq 2a$. Thus the equation (7) can be rewritten in the form

$$y^2=x((x+a)^2+\pi^s bx),\ s>0.$$

Finally, let us consider the non-split case. We shall need one preliminary result.

Lemma 10 *Let $f(x)=x^3+tx^2+\pi^l bx+\pi^m c$, where $b,c\in O_k^*, t\in M_k$ and $m\geq 2l>0$. Then $f(x)$ is reducible over k.*

Proof. We shall show that $f(x)$ has a root in k by using Newton's method. Firstly we have $f'(x)=3x^2+2tx+\pi^l bx$ $m>2l$, then $v_k(f(0))>2v_k(f'(0))$, since $v_k(f(0))=m$, and $v_k(f'(0))=l$. It implies that $f(x)$ has a root in k. Let $m=2l$ and $\mu=-cb^{-1}\pi^l$. Then $v_k(f(\mu))=v_k((-cb^{-1})^3\pi^{3l}+t(cb^{-1})^2\pi^{2l})>2l$. On the other hand $v_k(3(cb^{-1})^2\pi^{2l}+2(-cb^{-1})\pi^l t+\pi^l b)=l$, so $v_k(f(\mu))>2v_k(f'(\mu))$ and therefore $f(x)$ again has a root in k.

Let us prove the following

Theorem 7 *Let $E|k$ be an elliptic curve and assume we are in the non-split case. Then E has a minimal Weierstrass equation of the form $y^2=f(x)$, where $f(x)=x^3+\pi^r ax^2+\pi^l bx+\pi^m c$, $a,b\in O_k^*\bigcup\{0\}, c\in O_k^*, r,l,m\geq 0$, which is contained in the following list and any equation of the list is a minimal Weirstrass equation for the curve defined by it.*

i) E has good reduction. The polynomial $\bar{f}(x)$ is irreducible over k.

ii) E has additive reduction. Then it will satisfy one of the following conditions $1-5$.

1. $m=1$.

2. $m = 2$, *provided either* $b = 0$, *or* $l \geq 2$.

3. $m = 3$, $x^3 + \overline{\pi^{r-1}a}x^2 + \overline{\pi^{l-2}b}x + \bar{c}$ *is irreducible over* k *and either* $b = 0$ *or* $l \geq 2$.

4. $m = 4$, *and two following conditions are satisfied*

a) *either* $a = 0$ *or* $r \geq 2$,

b) *either* $b = 0$ *or* $l \geq 3$.

5. $m = 5$, *and two following conditions are satisfied*

a) *either* $a = 0$ *or* $r \geq 2$,

b) *either* $b = 0$ *or* $l \geq 4$.

Proof. Let $y^2 = x^3 + a_2x^2 + a_4x + a_6$ be a minimal Weirstrass equation for E. Set $a_2 = \pi^r a, a_4 = \pi^l b, a_6 = \pi^m c$, where $r, l, m \geq 0$ and $a, b, c \in O_k^* \bigcup \{0\}$. Since one has a non-split case, then it is clear that $c \in O_k^*$. Thus a minimal Weirstrass equation for E can be rewritten in the form $y^2 = f(x)$ for appropriate $r, l, m \geq 0$ and $a, b \in O_k^* \bigcup \{0\}, c \in O_k^*$. In view of irreducibility of $f(x)$ over k the polynomial $\bar{f}(x)$ over $\bar{k}$ is either irreducible or of the form $(x - \delta)^3$ for an appropriate $\delta \in \bar{k}$. In the first case E has good reduction and we are done. In the second one reduction *i)* is additive. Then without loss of generality one can assume that $r, l, m > 0$ and an equation $y^2 = f(x)$ corresponds to one of the cases of Tate's algorithm. In cases $3 - 5$ we lead to the following restrictions for m, l, b.

3. $m = 1$.

4. $m \geq 2, l = 1, b \in O_k^*$.

5. $m = 2$ and either $b = 0$, or $l \geq 2$.

In case 6 $m \geq 3$ and $\pi^2 | \pi^l b$, i.e. either $l \geq 2$ or $b = 0$. Furthemore, the polynomial $P(x) = 1/\pi^3 f(\pi x)$ is irreducible over k (in view of irreducibility of $f(x)$), therefore $\bar{P}$ either is irreducible over $\bar{k}$ or has a multiple root of multiplicity 3. Thus the case $6b$ for the equation $y^2 = f(x)$ is not realized. In the case $6a$ the polynomial $\bar{P}(x)$ would be irreducible over k and since provided $m > 3$ $\bar{P}(x)$ is divided by x, then it follows that $m = 3$. Let us now consider the case $6c$. In this case $\bar{P}(x)$ has a root β of multiplicity 3. The replacement x by $x' = x - u$, where u is a preimage of β in k under reduction homomorphism, lead us to conclusion that without loss of generality one can assume that $m \geq 4$ and two following conditions are realized $a)$ either $a = 0$ or $r \geq 2$, $b)$ either $b = 0$ or $l \geq 3$. Furthermore, if for an equation $y^2 = f(x)$ the possibility $6c_1$ is realized, then $m = 4$. If one has the possibility $6c_2$ for $y^2 = f(x)$ then $m \geq 4, l = 3$ and the following condition either $a = 0$ or $r \geq 2$ is satisfied. Finally, if one has $6c_3$, then $m = 5$ and two following condition are satisfied: $a)$ either $a = 0$ or $r \geq 2$, $b)$ either $b = 0$ or $l \geq 4$. It is clear that minimality of the equation $y^2 = f(x)$ implies that the possibility $6c_4$ is not realized. Thus in case of additive reduction we are obtained the following restrictions on coefficients of our equation $y^2 = f(x)$.

$\alpha)$ $m = 1, r > 0, l > 0$.

$\beta)$ $m = 2, r > 0, l > 0$.

$\gamma)$ $m = 3, r > 0$ and $l = 1, b \in O_k^*$ or the following conditions are satisfied

$a)$ either $b = 0$ or $l \geq 2$,

$b)$ $\bar{P}(x)$ is irreducible over $\bar{k}$.

$\delta)$ $m = 4, r > 0$ and $l = 1, b \in O_k^*$ or the following conditions are satisfied

$a)$ either $a = 0$ or $r \geq 2$,

$b)$ either $b = 0$ or $l \geq 3$.

$\sigma)$ $m = 5, r > 0$ and

$\sigma_1)$ $b = 0$ and the following condition is satisfied: either $a = 0$ or $r \geq 2$.

$\sigma_2)$ $b \in O_k^*, l = 1$.

$\sigma_3)$ $b \in O_k^*, l \geq 2$ and the following condition is satisfied: either $a = 0$ or $r \geq 2$.

One can observe that it is possible that $m \geq 6$ in a minimal Weierstrass equation, but we shall show below that in this case $f(x)$ is reducible over k.

To finish the proof of the theorem let us choose from the above minimal Weierstrass equations those of them which correspond to the non-split case. In case $\alpha)$ $f(x)$ is irreducible over k, because it is an Eisenstein polynomial. In case $\beta)$ if $l = 1$ and $b \in O_k^*$ then f reducible over k by lemma 10. And for the case where either $b = 0$ or $l \geq 2$ f irreducible over k. In fact if f has a root $\mu \in k$, then $\mu = \pi^s e, e \in O_k^*, s > 0$. And we have $\pi^{3s}e^3 + \pi^{r+2s}ae^2 + \pi^{l+s}be = -\pi^2 c$. The impossibility of the last equality can be proved by comparison of the values of valuation of both sides. In case $\gamma)$ if $b \in O_k^*, l = 1$ $f(x)$ is reducible over k by lemma 10. If either $b = 0$ or $l \geq 2$, but $\bar{P}(x)$ is irreducible over $\bar{k}$, then $P(x)$ is irreducible over k, and $f(x)$ is also irreducible over k. In case $\delta)$ if $b \in O_k^*$ and $l = 1, 2$ then $f(x)$ is reducible by lemma 10. Let either $b = 0$ or $l \geq 3$ and let us consider the polynomial $P(x)$. If $r \geq 2$ or $a = 0$, $P(x)$ is an Eisenstein polynomial. Then it follows $f(x)$ is irreducible over k. But if $a \in O_k^*$ and $r = 1$, then $\bar{P}(x) = x^2(x + \bar{a})$. Hence both $P(x)$ and $f(x)$ are reducible over k. Finally, let us consider the case $\sigma)$. For the case, where $b \in O_k^*$ and $l = 1, 2$, $f(x)$ is reducible over k. Finally, let us consider the case σ. For the case, where $b \in O_k^*$ and $l = 1, 2$, $f(x)$ is reducible over k by lemma 10. Let now either $b = 0$ or $l \geq 3$. The polynomial $P(x)$ in this case is of the form $x^3 + \pi^{r-1}ax^2 + \pi^{l-2}bx + \pi^2 c$. If $b \in O_k^*, l = 3$, then $f(x)$ is reducible over k. Let now either $b = 0$ or $l \geq 4$, then if we shall argue as in the case $\beta)$ we shall conclude that both $P(x)$ and $f(x)$ are irreducible over k.

Finally, we shall show that if $m \geq 6$, then there no exists a minimal Weierstrass equation of the form $y^2 = f(x)$ with irreducible over k polynomial $f(x)$.

In fact, if such an equation exists, then either $b = 0$ or $l \geq 4$ (otherwise $f(x)$ is reducible over k by lemma 10). Furthermore, if either $a = 0$ or $r \geq 2$, then replacing x by $\pi^2 x$, y by $\pi^3 y$ we shall obtain an equation with discriminant which has the value less than the value of previous one. Hence $a \in O_k^*$ and $r = 1$. But then $\bar{P}(x) = x^2(x + \bar{a})$ and we shall have that $P(x)$ (and hence $f(x)$) is reducible over k.

Q.E.D.

7 Torsion of local elliptic curves

Let k be as above, $m > 1$ a natural number relatively prime to characteristic of $\bar{k}$. The goal of this section is to describe the group ${}_mE(k)$. It is clear that it is enough to describe all groups ${}_{p^n}E(k)$, where n, p are natural numbers and p is prime, $(p, char\ \bar{k}) = 1$.

Let $|\bar{k}^*| = p^s u$, where $(u,p) = 1$, $d = \min\{n, s\}$, $c = (p^n, v_k(j(E)))$ if $v_k(j(E)) \neq 0$ and

$$r = \min_{0<i\leq c}\{i \in \boldsymbol{Z} | \bar{u}^{i/c} \in \bar{k}^*\}, \text{ where } \bar{u} = \overline{j(E)\pi^{-v_k(j(E))}}.$$

Then the description of ${}_{p^n}E(k)$ can be given as follows.

Theorem 8 *Let k be a non-dyadic field and $E|k$ be an elliptic curve.*

G. If E has good reduction, then

$${}_{p^n}E(k) \cong {}_{p^n}\tilde{E}(\bar{k}).$$

A. If E has additive reduction, then one has the following description of ${}_{p^n}E(k)$.

A1. ${}_{p^n}E(k) \cong <0>$ if $p > 3$.

A2. ${}_{3^n}E(k) \cong <0>$ in the split and semi-split cases.

A3. In the non-split case

$${}_{3^n}E(k) \cong \begin{cases} \boldsymbol{Z}/3 & \text{if } [E(k) : E_0(k)] = 3, \\ <0> & \text{otherwise.} \end{cases}$$

A4. ${}_{2^n}E(k) = {}_2E(k) \cong (\boldsymbol{Z}/2)^2$ in the split case.

A5. In the semi-split case

$${}_2E(k) \cong \boldsymbol{Z}/2,$$

and provided $n \geq 2$

$${}_{2^n}E(k) \cong \begin{cases} \boldsymbol{Z}/2 & \text{in the cases } A.a) - A.d), \\ \boldsymbol{Z}/4 & \text{in the case } A.e). \end{cases}$$

A6. ${}_{2^n}E(k) \cong <0>$ in the non-split case.

M. If E has multiplicative reduction then one has the following description of ${}_{p^n}E$.

M.1 In the split case, where E has non-split reduction,

$${}_{p^n}E(k) \cong \begin{cases} \boldsymbol{Z}/p^d & \text{if } p > 2, \\ \boldsymbol{Z}/2^d \oplus \boldsymbol{Z}/2 & \text{if } p = 2. \end{cases}$$

M.2 In the semi-split case, where E has non-split reduction,

$${}_{p^n}E(k) \cong \begin{cases} \boldsymbol{Z}/p^d & \text{if } p > 2,\ m \text{ is odd}, \\ \boldsymbol{Z}/2^d & \text{if } p = 2,\ m \text{ is even and } 2^n || |\bar{k}^*|, \\ \boldsymbol{Z}/2^{d+1} & \text{if } p = 2,\ m \text{ is even and } 2^n \not| |\bar{k}^*|. \end{cases}$$

M.3 In the split and semi-split cases, where E has split reduction,

$$_{p^n}E(k) \cong <\mu_{p^n}> \oplus \boldsymbol{Z}/(c/r),$$

where $<\mu_{p^n}>$ is a group of roots of unity of degree p^n lying in k.

Remark 2 *¿From the assertion G of the theorem it follows that the study of $_{p^n}E(k)$ in the case of good reduction of E can be reduced to the study of $_{p^n}\tilde{E}(\bar{k})$ for reduced curve $\tilde{E}$ over a finite field. An information about the group $_{p^n}\tilde{E}(\bar{k})$ can be found for example in [11], [12], in [13] or in [24].*

To prove the theorem we shall need some preliminary results.

Lemma 11 *Let $(m, char\ \bar{k}) = 1$. Then the restriction of the reduction map R to $_mE_0(k)$ is an isomorphism of $_mE_0(k)$ and $_m\tilde{E}_0(\bar{k})$.*

Proof. It is easy to see that $R(\ _mE_0(k)) \subset\ _m\tilde{E}_0(\bar{k})$. Furthermore, $Ker|_{\ _mE_0(k)} = E_1 \bigcap\ _mE_1(k)$. Since the last group does not contain points of order m, then $Ker|_{\ _mE_0(k)} =< 0 >$. Let $\tilde{Q} \in\ _m\tilde{E}_{ns}(\bar{k})$. In view of surjectivity of restriction of reduction map to $E_0(k)$ (see [14], p.174, prop.2.1), there exists a point Q_0 such that $\bar{Q}_0 = \tilde{Q}$. It is clear that $\overline{mQ_0} = m\bar{Q}_0 = m\tilde{Q} = 0$, so $Q' = mQ_0 \in E_1(k)$. Since the group $E_1(k)$ is uniquely m-divisible, then there exists the unique point $Q_1 \in E_1(k)$ such that $Q'_1 = mQ_1$. Hence $mQ_0 = mQ_1$, and one has immediately $Q_0 - Q_1 \in\ _mE_0(k)$. Then for $Q = Q_0 - Q_1$ one will have $\bar{Q} = \bar{Q}_0 = \tilde{Q}$. Thus the restriction of R to $_mE_0(k)$ is surjective.

Q.E.D.

Proposition 10 *Let $E|k$ be an elliptic curve with split multiplicative reduction. Then there exists an element $q \in M_k$, such that E is isomorphic to the Tate curve E_q defined by the equation*

$$y^2 + xy = x^3 + a_4x + a_6,$$

$$\textit{where } a_4 = -5\sum_{n\geq 1} n^3q^n/(1-q^n), \quad a_6 = -\frac{1}{2}\sum_{n\geq 1}(7n^5 + 5n^3)q^n/(1-q^n),$$

and in fact

$$j(E) = \frac{1}{q} + 744 + 196884q + \dots,$$

$$\textit{in particular } v_k(q) = -v_k(j(E)), \quad \overline{q\pi^{-v_k(q)}} = (\overline{j(E)\pi^{-v_k(j(E))}})^{-1}.$$

Moreover, abelian groups $E_q(k)$ and $k^*/<q>$, where $<q>$ is the subgroup of k^* generated by q are isomorphic.

For the proof see [14], p.356.

Proposition 11 *If $E|k$ has non-split multiplicative reduction, then*

$$[E(k) : E_0(k)] = \begin{cases} 1, & \textit{if } v_k(\Delta(E)) \textit{ is odd,} \\ 2, & \textit{if } v_k(\Delta(E)) \textit{ is even.} \end{cases}$$

For the proof see [15], p. 266.

Proposition 12 *If E has additive reduction, then $[E(k):E_0(k)]\leq 4$. Moreover, if k is non-dyadic and one is either in the split or in the semi-split case, then $[E(k):E_0(k)]\neq 3$.*

Proof. The first statement is a part of Kodaira-Neron theorem. To prove the second, let us use the simplified variant of Tate's algorithm (see the preliminaries). Let a minimal Weierstrass equation of E be given by

$$y^2=f(x),\quad f(x)=x^3+a_2x^2+a_4x+a_6,\quad a_2,a_4,a_6\in O_k.$$

Since E has additive reduction the cases 1, 2 are not realized and therefore $a_2,a_4,a_6\in M_k$. It is easy to see now to prove our proposition we need to consider only cases

$5)_0$. $v_k(a_6)=2,\ \pi^2|a_4,\ \overline{a_6\pi^{-2}}\in(\bar{k}^*)^2$,

$6a)_0$. $\pi^3|a_6,\ pi^2|a_4$, the polynomial $\bar{P}(x)$ has just two roots in $\bar{k}$,

$6c_1)_0$. $v_k(a_6)=4,\ \pi^2|a_4$ and $\overline{a_6\pi^{-4}}\in(\bar{k}^*)^2$.

But the case $(6a)_0$ is not realized because of $\bar{P}(x)$ is defined over $\bar{k}$. Furthermore, since we consider either split or semi-split cases it follows from the above lists of minimal Weierstrass equations that without loss of generality we may assume $a_6=0$. But this condition contradicts to cases $5)_0, 6c_1)_0$.

Q.E.D.

Proposition 13 *Let E be an arbitrary elliptic curve defined over local field k. Then*

$${}_{p^n}E(k)\cong E(k)/p^n,\quad {}_{p^n}BrE\cong\ {}_{p^n}Br(k)\oplus\ {}_{p^n}E(k).$$

This proposition is a direct consequence of theorem 2.

Lemma 12 *Let E have additive reduction and $p>3$. Then ${}_{p^n}E(k)=<0>$.*

Proof. Since $([E(k):E_0(k)],p)=1$, then by Kodaira-Neron theorem ${}_{p^n}E(k)=\ {}_{p^n}E_0(k)\cong {}_{p^n}\tilde{E}_{ns}(\bar{k})$ (the last isomorphism by lemma 11). But in view of additivity of reduction $\tilde{E}(\bar{k})\cong\bar{k}^+$. Since the additive group $\bar{k}^+$ of $\bar{k}$ has trivial p^n- torsion one has immediately ${}_{p^n}E(k)=<0>$.

Proposition 14 *Let E have additive reduction and char $\bar{k}\neq 3$. Then*

$${}_{3^n}E(k)\cong\begin{cases}\boldsymbol{Z}/3 & \textit{if } [E(k):E_0(k)]=3\ ,\\ <0> & \textit{otherwise}\ .\end{cases}$$

Proof. Assume that $[E(k):E_0(k)]=3$. First of all we have $E_1(k)=3E_1(k)$ and $E_1(k)\subset E_0(k)$. Hence $E_1(k)\subset 3E_0(k)$. Furthermore, $E_0(k)/3E_0(k)$ is a homomorphic image of $E_0(k)/E_1(k)$ and the order of the last group is equal to $|\bar{k}|$ and is relatively prime to 3, then the order of $E_0(k)/3E_0(k)$ is relatively prime to 3. On the other hand, this group killed by multiplication by 3 and therefore has an order 3^m for appropriate m.

Hence $m = 0$ and $E_0(k) = 3E_0(k)$. Since $3E(k) \subset E_0(k)$ and $E_0(k) = 3E_0(k) \subset 3E(k)$, then $E_0(k) = 3E(k)$.

Let now $x \in E(k) \setminus E_0(k)$. From the equality $[E(k) : E_0(k)] = 3$ one concludes that $3x \in E_0(k)$, and therefore $3x = 3e_0$ for some $e_0 \in E_0(k)$. Thus $x - e_0 \in {}_3E(k)$, and $x - e_0 \neq 0$. Hence ${}_3E(k) \neq <0>$. Furthermore, if $x_1, x_2 \in {}_3E(k)$ and $x_1 - x_2 \in E_0(k)$, then $x_1 - x_2 \in {}_3E_0(k)$, therefore $x_1 = x_2$. Since $E_0(k)/E_1(k) \cong \tilde{E}_{ns}(\bar{k})$, we have $y = |\bar{k}|(x_1 - x_2) \in E_1(k)$ and $3y = 0$. The group $E_1(k)$ has no non-trivial 3-torsion, so that $y = 0$ and $x_1 = x_2$ (because 3 is relatively prime to $|\bar{k}|$).

Thus different elements from ${}_3E(k)$ are contained in different cosets modulo $E_0(k)$. Since ${}_3E(k_s) \cong (\boldsymbol{Z}/3)^2$ and $[E(k) : E_0(k)] = 3$ the group ${}_3E(k)$ is isomorphic either $\boldsymbol{Z}/3$ or $(\boldsymbol{Z}/3)^2$. But, if ${}_3E(k) \cong \boldsymbol{Z}/3$, then $E(k)/E_0(k)$ has an order at least 9 and this contradicts to additivity of reduction of E. Conversely, if $[E(k) : E_0(k)] \neq 3$, then 3 is relatively prime to $[E(k) : E_0(k)]$, and since ${}_3E_0(k) = <0>$ so ${}_3E(k) = <0>$.

Q.E.D.

Corollary 5 *Let E have additive reduction char $\bar{k} \neq 2, 3$ and assume the split or semi-split case. Then ${}_3E(k) = <0>$.*

Proof. By proposition 6 $([E(k) : E_0(k)], 3) = 1$.

Finally, let us describe 2-primary torsion of $E(k)$.

Lemma 13 *Let E have an additive reduction, char $\bar{k} \neq 2$. Then*

$$
{}_2E(k) \cong \begin{cases} <0>, & \text{in the non-split case,} \\ \boldsymbol{Z}/2, & \text{in the semi-split case,} \\ \boldsymbol{Z}/2 \oplus \boldsymbol{Z}/2, & \text{in the split case.} \end{cases}
$$

The proof is well-known.

Lemma 14 *Let E have an additive reduction, char $\bar{k} \neq 2$. Then for any $n \geq 2$ ${}_{2^n}E(k) = {}_4E(k)$.*

Proof. Let $x \in {}_{2^n}E(k) \setminus {}_4E(k), n > 2$ and $y = [E(k) : E_0(k)]x$. It is clear that $y \in {}_{2^n}E_0(k)$ and therefore $y = 0$. If $[E(k) : E_0(k)]$ equals either 2 or 4, then the equality $y = 0$ is impossible in view of $x \notin {}_4E(k)$. If $[E(k) : E_0(k)]$ is odd, then from $[E(k) : E_0(k)]x = 0$ and $2^n x = 0$ one can deduce that $x = 0$, but this is not the case.

Thus the description of 2-primary torsion of $E(k)$ in the case of curves with additive reduction can be reduced to the one of groups ${}_4E(k)$.

Lemma 15 *Let E, k be as in lemma 14 and assume either the split or the semi-split case. Then*

$$
{}_4E(k) \cong \begin{cases} {}_2E(k), & \text{if } E(k)/E_0(k) \ncong \boldsymbol{Z}/4, \\ \boldsymbol{Z}/4, & \text{if } E(k)/E_0(k) \cong \boldsymbol{Z}/4. \end{cases}
$$

In the non-split case ${}_4E(k) = <0>$.

Proof. Let $E(k)/E_0(k) \not\cong \boldsymbol{Z}/4$ and $x \in {}_4E(k) \setminus {}_2E(k)$. Let also $y = [E(k) : E_0(k)]x$. By Kodaira-Neron theorem $[E(k) : E_0(k)] \leq 4$, and therefore $y \neq 0$. But $y \in E_0(k)$ and $4y = 0$. In view of triviality of the group ${}_4E_0(k)$ we have a contradiction. Let now $E(k)/E_0(k) \cong \boldsymbol{Z}/4$. Then arguments similar to those of in the proof of proposition 14, give us $E_0(k) = 4E_0(k) = 4E(k)$. Furthermore, let $x \in E(k) \setminus E_0(k)$ such that $x + E_0(k)$ is a generator of $E(k)/E_0(k)$. Let also $e = 4x,\ e \in E_0(k)$. In view of $E_0(k) = 4E_0(k)$ we have $e = 4e_0,\ e_0 \in E_0(k)$. Hence $4(x - e_0) = 0,\ x - e_0 \neq 0$ and $x - e_0 \in {}_4E(k)$. Observe that $2(x - e_0) \neq 0$. In fact, otherwise $2x = 2e_0 \in E_0(k)$, and then $x + E_0(k)$ is an element in $E(k)/E_0(k)$ order at most 2. Furthermore, as in the proof of proposition 14 one can deduce that any two different elements from ${}_4E(k)$ lie in different cosets modulo $E_0(k)$. Hence $|\,{}_4E(k)| \leq 4$. To finish proof of the lemma it is enough to observe that in view of existence in ${}_4E(k)$ of an element $x - e_0$ of order 4 one has $\boldsymbol{Z}/4 \subset {}_4E(k)$.

Q.E.D.

Proposition 15 *Let k be a non-dyadic field and let $E|k$ have additive reduction. Then in the semi-split case*

$$ {}_4E(k) \cong \begin{cases} {}_2E(k), & \text{in cases } A.a) - A.d), \\ \boldsymbol{Z}/4, & \text{in case } A.e). \end{cases} $$

Proof. Let $y^2 = x(x^2 + Ax + B)$ be a minimal Weierstrass equation for E. If $Q \in {}_4E(k) \setminus {}_2E(k)$, then $2Q \in {}_2E(k) \setminus \{0\}$. It means that $2Q = (0,0)$ and $x(2Q) = 0$. On the other hand $x(2Q) = (x(Q)^2 - B)^2/(4y(Q)^2)$. So we have $B \in (k^*)^2$. In cases $A.a)$ and $A.b)$ from the conditions of theorem 6 one has $B \notin (k^*)^2$. Hence in these cases ${}_4E(k) = {}_2E(k)$. Furthermore, $x(Q)(x(Q)^2 + Ax(Q) + B) \in (k^*)^2$ and since $x(Q)^2 = B$, then $A + 2x(Q) \in (k^*)^2$. It is clear that conditions:

$$ x(Q)^2 = B \text{ and } A + 2x(Q) \in (k^*)^2 $$

are necessary and sufficient ones for $Q \in {}_4E(k) \setminus {}_2E(k)$. In cases $A.c) - A.e)$ $B = \pi^2 b,\ b \in (O_k^*)^2$, it means that $v_k(x(Q)) = 1$, and therefore $v_k(A) = 1$, i.e. $A = \pi a,\ a \in O_k^*$ (otherwise $v_k(A + 2x(Q)) = 1$, and this contradicts to $A + 2x(Q) \in (k^*)^2$)). Hence for the cases $A.c)1 - A.c)2$ we have ${}_4E(k) = {}_2E(k)$. For remaining cases $x(Q) = \pm\pi\sqrt{b}$. The necessary and sufficient condition for $Q \in {}_4E(k) \setminus {}_2E(k)$ can be rewritten as either $\pi(a + 2\sqrt{b}) \in (k^*)^2$ or $\pi(a - 2\sqrt{b}) \in (k^*)^2$. Therefore $\bar{a}^2 - 4\bar{b} = 0$ and in the case $A.c)3$ ${}_4E(k) = {}_2E(k)$. In the remaining cases let us fix $\sqrt{b}$ as follows: $\overline{a/\sqrt{b}} = 2$. We shall have then $a + 2\sqrt{b} = 4\sqrt{b} + \pi^m c\sqrt{b}$ ($m = 2r$ for the equation $A.c)4$ and $m = 2r + 1$ in the cases $A.d), A.e)$). Then $v_k(\pi(4\sqrt{b} + \pi^m c\sqrt{b})) = 1$ and $\pi(4\sqrt{b} + \pi^m c\sqrt{b}) \notin (k^*)^2$. In the second case we shall have $\pi(a - 2\sqrt{b}) = \pi^{m+1}c\sqrt{b}$. The last element is a square in k^* iff one has a case $A.e)$.

Q.E.D.

Proposition 16 *Let k be a non-dyadic field and let $E|k$ have additive reduction. Then in the split case*

$$ {}_4E(k) \cong {}_2E(k). $$

Proof. If the proposition is not true, then by lemma 15 ${}_4E(k) \cong \boldsymbol{Z}/4$. On the other hand, ${}_2E(k) \subset {}_4E(k)$ and ${}_2E(k) \cong \boldsymbol{Z}/2 \oplus \boldsymbol{Z}/2$.

By Hensel lemma, if E has multiplicative reduction we have only split and semi-split cases.

Proposition 17 *Let E have non-split multiplicative reduction given by the equation $y^2 = x(x+\alpha)(x - a\pi^m)$, $a \in O_k^*, \alpha \in O_k^* \setminus (O_k^*)^2, m > 0$. Then*

$$ {}_{p^n}E(k) \cong \begin{cases} \boldsymbol{Z}/p^d, & \text{if } p \neq 2, \\ \boldsymbol{Z}/2^d \oplus \boldsymbol{Z}/2, & \text{if } p = 2. \end{cases} $$

Proof. Set $x^2 + Ax + B = (x+\alpha)(x - a\pi^m)$. Then the discriminant Δ of the equation $y^2 = x(x^2 + Ax + B)$ is equal to $16b^2(A^2 - 4B) \in (k^*)^2$, therefore $v_k(\Delta) = 2r$. By proposition 11 $[E(k) : E_0(k)] = 2$. Furthermore, since the point $(0,0) \in E(k) \setminus E_0(k)$ has an order 2, then $E(k) = E_0(k) \oplus <(0,0)>$. For odd p

$$ {}_{p^n}E(k) = {}_{p^n}E_0(k) \oplus {}_{p^n}<(0,0)> \cong {}_{p^n}\bar{k}^* \cong \boldsymbol{Z}/p^d. $$

If $p = 2$, then

$$ {}_{2^n}E(k) = {}_{2^n}E_0(k) \oplus {}_{2^n}<(0,0)> \cong {}_{p^n}\bar{k}^* \oplus \boldsymbol{Z}/2 \cong \boldsymbol{Z}/p^d \oplus \boldsymbol{Z}/2. $$

Proposition 18 *Let $E|k$ be a curve with non-split multiplicative reduction given by $y^2 = x((x+a)^2 + \pi^m cx)$, $a, c \in O_k^*, m > 0, -a \notin (k^*)^2$ (the semi-split case). Then*

$$ {}_{p^n}E(k) \cong \begin{cases} \boldsymbol{Z}/p^d, & \text{either if } p > 2 \text{ or } m \text{ is odd}, \\ \boldsymbol{Z}/2^d, & \text{if } p = 2,\ m \text{ is even and } 2^n \mid |\bar{k}^*|, \\ \boldsymbol{Z}/2^{d+1}, & \text{if } p = 2,\ m \text{ is even and } 2^n \nmid |\bar{k}^*|. \end{cases} $$

Proof. Firstly, let p be odd. If $Q \in {}_{p^n}E(k)$, then $Q = (p^n + 1)Q$. Since $[E(k) : E_0(k)]$ is equal either 1 or 2 and $p^n + 1$ is even, then $(p^n+1)Q \in E_0(k)$, and it means that $Q \in E_0(k)$. Thus ${}_{p^n}E(k) = {}_{p^n}E_0(k) \cong {}_{p^n}\bar{k}^* \cong \boldsymbol{Z}/p^d$. If E is defined by an equation $y^2 = x(x^2 + Ax + B)$, then $\Delta(E) = 16A^2(A^2 - 4B)$. In our situation $x^2 + Ax + B = x^2 + (2a + \pi^m c)x + a^2$ and therefore $A = 2a + \pi^m c$, $B = a^2$, $\Delta = 16(2a + \pi^m c)^2(4ac\pi^m + c^2\pi^{2m})$, $v_k(\Delta) = m$.

If $p = 2$ and m is odd, $v_k(\Delta(E))$ is also odd and by proposition 11 $E(k) = E_0(k)$. It follows from multiplicativity of reduction of E that ${}_{p^n}E(k) \cong \boldsymbol{Z}/2^d$. Furthermore, let $p = 2$ and m is even, then $[E(k) : E_0(k)] = 2$, so we have $2E(k) \subset E_0(k)$. As it was observed above in case $(2, char\ \bar{k}) = 1$ the orders of groups ${}_2E(k)$ and $E(k)/2$ coincided, and it follows from $2E(k) \subset E_0(k) \subset E(k)$ that $E_0(k) = 2E(k)$. It means that the restriction of the multiplication by 2 to $E(k)$ is a surjective homomorphism and this implies 2-divisibility of elements from $E_0(k)$. Then it is clear that multiplication by 2 maps ${}_{2^{n+1}}E(k)$ onto ${}_{2^n}E_0(k)$ with the kernel $<0, (0,0)>$. In fact, this map is epimorphic because $E_0(k)$ is 2-divisible and any element from ${}_{2^n}E_0(k)$ lies in ${}_{2^{n+1}}E_0(k)$. It means that $|\,{}_{2^n}E(k)| = 2|\,{}_{2^{n-1}}E_0(k)|$ for any $n \geq 2$. On the other hand in view of ${}_{2^n}E_0(k) \cong {}_{2^n}\bar{k}^*$ we have

$$ |\,{}_{2^n}E_0(k)| = \begin{cases} 2|\,{}_{2^{n-1}}E_0(k)|, & \text{if } 2^n \,|\, |\bar{k}^*|, \\ |\,{}_{2^{n-1}}E_0(k)|, & \text{if } 2^n \nmid |\bar{k}^*|. \end{cases} $$

Therefore $|{}_{2^n}E(k)| = |{}_{2^n}E_0(k)|$, if $2^n \mid |\bar{k}^*|$ and $|{}_{2^n}E(k)| = 2|{}_{2^n}E_0(k)|$, if $2^n \not| |\bar{k}^*|$. In the first case in view ${}_{2^n}E_0(k) \subset {}_{2^n}E(k)$ we have ${}_{2^n}E(k) = {}_{2^n}E_0(k) \cong \boldsymbol{Z}/2^d$. In the second one in view of $2^n \not| |\bar{k}^*|$ we have ${}_{2^n}E_0(k) = {}_{2^{n-1}}E_0(k)$ and this implies the surjectivity of multiplication by 2 acting from ${}_{2^n}E(k)$ to ${}_{2^n}E_0(k)$. Now if z is a generator of ${}_{2^n}E_0(k)$ which is of order 2^d, then $(1/2)z$ is of order 2^{d+1}.

Q.E.D.

Finally, let us consider the case of split multiplicative reduction.

Lemma 16 *Let $q = u\pi^s, u \in O_k^*, s > 0, (m, char\ \bar{k}) = 1$. Then*

$$_m(k^*/<q>) \cong <\mu_m> \oplus \boldsymbol{Z}/((m,s)/r),$$

where $<\mu_m>$ is the group of m-th roots of unity lying in k, $r = \min_{0<i\le(m,s)}\{i \in \boldsymbol{Z} | u^{i/(m,s)} \in k\}$.

Remark 3 *The condition $u^{i/(m,s)} \in k$ means that the polynomial $x^m - u^{mi/(m,s)}$ has a root in k.*

Proof of lemma. Let us firstly show that the condition $u^{j/(m,s)} \in k$ is satisfied if and only if $r|j$. Really, if $r|j$, then the above condition is obviously satisfied. Let now $u^{j/(m,s)} \in k$, but $r \not| j$. Then for $\delta = (r,j)$, $\delta < r$ and there exist $f, t \in \boldsymbol{Z}$ such that $fr + tj = \delta$. Hence $u^{\delta/(m,s)} = (u^{r/(m,s)})^f \cdot (u^{j/(m,s)})^t \in k$, and this contradicts to minimality of r. In particular, $r|(m,s)$.

Let $x = v\pi^n$, $v \in O_k^*, n \in \boldsymbol{Z}$ and $v\pi^n + <q> \in {}_m(k^*/<q>)$. Then $v^m\pi^{nm} \in <q>$, i.e. $v^m\pi^{nm} = u^l\pi^{ls}$ for an appropriate $l \in \boldsymbol{Z}$. It follows then $mn = sl$ and $v^m = u^l$. Furthermore, $s|mn$ if and only if $s/(m,s)|mn/(m,s)$. The last condition is equivalent to divisibility of n by $s/(m,s)$ and that is equivalent to the existence of $i \in \boldsymbol{Z}$ such that $n = si/(m,s)$. And this means that $l = mn/s = mi/(m,s)$. Thus an element $v\pi^n + <q>$ lies in ${}_m(k^*/<q>)$ if and only if $n = si/(m,s)$ and $v^m = u^{mi/(m,s)}$ for some $i \in \boldsymbol{Z}$. The single restriction on i is that: there exists $v_0 \in k^*$ such that $v_0^m = u^{mi/(m,s)}$. Then all of v corresponding to given i will differ from v_0 by a factor lying in $<\mu_m>$. It follows now from the fact which was obtained at the beginning of the proof that $r|i$, $i = rj$, $n = srj/(m,s)$, $v_0 = u^{rj/(m,s)}$. Let us fix an element $u^{r/(m,s)} \in k$. Then it is easy to see that

$$_m(k^*/<q>) \cong <\mu_m> \oplus <u^{r/(m,s)}\pi^{rs/(m,s)}>,$$

so the lemma is proved.

Proposition 19 *Let E have split multiplicative reduction. Then*

$$_{p^n}E(k) \cong <\mu_{p^n}> \oplus \boldsymbol{Z}/(c/r).$$

Proof. By proposition 10 E is isomorphic to some Tate curve E_q. Then ${}_{p^n}E(k) \cong {}_{p^n}(k^*/<q>)$. Let $q = u\pi^s$. Using lemma 16 we shall have

$$_{p^n}E(k) \cong <\mu_{p^n}> \oplus <u^{r/(p^n,s)}\pi^{rs/(p^n,s)}> .$$

By proposition 10 $s = -v_k(j(E_q)) = -v_k(j(E)), \bar{u} = (\overline{j(E)\pi^s})^{-1}, c = (p^n, s)$.

.

Now the proof of this theorem follows immediately from lemmas 12-15 and propositions 14-19.

The description of p-primary torsion in the dyadic case is given by

Theorem 9 *Let k be a dyadic field, $E|k$ an elliptic curve and p an odd prime number. Then we shall have the following statements.*

G_2. *If E has good reduction, then*

$$ {}_{p^n}E(k) \cong {}_{p^n}\tilde{E}(\bar{k}). $$

A_2. *If E has additive reduction and $p > 3$, then*

$$ {}_{p^n}E(k) = <0>, $$

If $p = 3$, then

$$ {}_{3^n}E(k) \cong \boldsymbol{Z}/3, \ \textit{if } [E(k) : E_0(k)] = 3, \ \textit{and} $$

$$ {}_{3^n}E(k) \cong <0> \ \ \textit{otherwise} . $$

M_2. *If E has multiplicative reduction, then if E has non-split reduction*

$$ {}_{p^n}E(k) \cong \boldsymbol{Z}/p^d, $$

and if E has split reduction

$$ {}_{p^n}E(k) \cong <\mu_{p^n}> \oplus \boldsymbol{Z}/(c/r), $$

where d, r and c are just the same as in theorem 8.

Proof. The assertions G_2, A_2 are true because of lemmas 11, 12 and of proposition 14. In the case of non-split multiplicative reduction the proof is similar to the one of proposition 18. In the case of split multiplicative reduction everything follows from proposition 19.

8 The group ${}_2BrE$. The case of good reduction

Theorem 10 *Let k be non-dyadic and $E|k$ be an elliptic curve with good reduction. Then there is the following presentation of elements of ${}_2Br\ E$ by quaternion algebras over $k(E)$.*

- *In the split case*

$$ \left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right], \left\{\left[\left(\frac{\pi\ ,\ x}{k(E)}\right)\right]\right\}, \left\{\left[\left(\frac{\pi\ ,\ x-e_i}{k(E)}\right)\right]\right\}_{i=1,2}, $$

$$ \left\{\left[\left(\frac{\pi\ ,\ \alpha x}{k(E)}\right)\right]\right\}, \left\{\left[\left(\frac{\pi\ ,\ \alpha(x-e_i)}{k(E)}\right)\right]\right\}_{i=1,2}. $$

- *In the semi-split case*

$$\left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right],\left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right],\left[\left(\frac{\pi\ ,\ x}{k(E)}\right)\right],\left[\left(\frac{\pi\ ,\ \alpha x}{k(E)}\right)\right].$$

- *In the non-split case*

$$\left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right],\left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right].$$

Of course this theorem is a particular case of the theorem of section 5, but if we should like to have a closed exposition for all elliptic curves we need to repeat our arguments using specific results for elliptic curves. Firstly we prove two preliminary statements.

Lemma 17 *Let* $[((f\ ,\ g\ )|\ k(E))] \in Br(k(E))$ *and* E *be defined by an equation* $y^2 = x(x^2 + ax + b)$. *If* f *is a monic polynomial over* k, *then* $k(E)_\infty$*-algebra* $((f\ ,\ g\ )|\ k(E))_\infty$ *is trivial.*

Proof. It is clear that $k(E) = k(z)(\sqrt{z(1+az+bz^2)})$, where $z = x^{-1}$, and $k(E)_\infty \overset{\mu}{\cong} k <z> (\sqrt{z(1+az+bz^2)}) = k <z> (\sqrt{z})$. Furthermore, since $f(x)$ is unitary, then polynomial $\tilde{f}(z) = f(1/z)((\sqrt{z})^{deg\, f})^2$ is of the form $1 + zP(z)$ and therefore is a square, i.e.$\tilde{f}(z) = c^2$, where $c \in k <z> (\sqrt{z})$, so that

$$\left(\frac{f\ ,\ g}{k(E)}\right)_\infty \cong \left(\frac{c^2\ ,\ \tilde{g}}{k(E)_\infty}\right),$$

where $\tilde{g} = \mu(g)$.

Corollary 6 *Let* f, g *be as in lemma 17. Then*

$$\left(\frac{f\ ,\ g}{k(E)}\right) \not\cong \left(\frac{\pi\ ,\ \alpha}{k(E)}\right).$$

Proof. Let us consider algebras $((\pi\ ,\ \alpha\ )|\ k(E))_\infty, ((f\ ,\ g\ )|\ k(E))_\infty$. Then $((\pi\ ,\ \alpha\ )|\ k(E))_\infty$ is non-trivial over $k(E)_\infty$, but by lemma 17 it is not the case for $((f\ ,\ g\ )|\ k(E))_\infty$.

Proof of the theorem. Since $((\pi\ ,\ \alpha\ )|\ k(E))$ is not trivial (because $((\pi\ ,\ \alpha\ )|\ k(E))_\infty$ is non-trivial) one has that the theorem is true in non-split case because in this case $|\ {}_2Br\ E| = 2$ (proposition). In view of the unramifiedness of the algebra $((\pi\ ,\ \alpha\ )|\ k(E))$ over $k(E)$ to prove that all algebras listed in the theorem are unramified it is enough to prove $((\pi\ ,\ x\ )|\ k(E))$ and $((\pi\ ,\ x - e_i\ )|\ k(E))$, $i = 1, 2$ are unramified in split case and $((\pi\ ,\ x\ )|\ k(E))$ is unramified in semi-split one. To prove this let us observe firstly all these algebras are trivial after extension of scalars to $k(E)_\infty$, and therefore they are unramified over $k(E)_\infty$. Hence an algebra $((\pi\ ,\ x - e_i\ )|\ k(E))$ is unramified at least at points different from the point defined by polynomial $x - e_i$. Furthermore,

$$\left(\frac{\pi\ ,\ x - e_i}{k(E)_{x-e_i}}\right) = \left(\frac{\pi\ ,\ \frac{y^2}{x(x-e_j)}}{k(E)_{x-e_i}}\right) =$$

$$\left(\frac{\pi\ ,\ x(x-e_j)}{k(E)_{x-e_i}}\right)=\left(\frac{\pi\ ,\ e_i(e_i-e_j)}{k(E)_{x-e_i}}\right),$$

where $j\neq i$. It is clear that the last algebra is unramified. Therefore $((\pi\,,x-e_i)|k(E))_{x-e_i}$ is unramified. In a similar way one can prove that in split case $((\pi\,,x)|k(E))$ is unramified. In semi-split case one has

$$\left(\frac{\pi\ ,\ x}{k(E)_x}\right)=\left(\frac{\pi\ ,\ \frac{y^2}{x^2+ax+b}}{k(E)_x}\right)=\left(\frac{\pi\ ,\ x^2+ax+b}{k(E)_x}\right)=\left(\frac{\pi\ ,\ b}{k(E)_x}\right).$$

So one has $((\pi\ ,\ x\ )|\ k(E))$ is also unramified over $k(E)$. To finish proof it is sufficient to prove that all algebras listed in the theorem except $((\pi\ ,\ 1\ )|\ k(E))$ and $((\pi\ ,\ \alpha\ )|\ k(E))$ are non-trivial. Let $z_i=x-e_i$. Appropriate replacement of variable x reduces everything in split case to the proof of non-triviality of algebra $((\pi\ ,\ z\ )|\ k(E))$ for E defined by equation $y^2=z(z^2+mz+n)$, where the polynomial $z^2+\bar{m}z+\bar{n}$ has no multiple roots. Let $\bar{X}|\bar{k}$ be a curve given by an equation $V^2=\bar{\alpha}(\bar{\alpha}^2U^4+\bar{m}\bar{\alpha}U^2+\bar{n})$. In view of the above remark the polynomial $\bar{\alpha}(\bar{\alpha}^2U^4+\bar{m}\bar{\alpha}U^2+\bar{n})$ has no multiple roots and therefore $\bar{X}|\bar{k}$ is a smooth curve. By Weil unequality for sufficiently big odd prime p $\bar{X}$ has $\boldsymbol{F}_{|\bar{k}|^p}$-rational point $(\bar{\delta},\bar{\gamma})$.

Let L be the unramified extension of k of degree p. Then the smooth point $(\bar{\delta},\bar{\gamma})$ can be lifted to L-rational point (δ,γ) of X defined over L by the equation $V^2=\alpha(\alpha^2U^4+m\alpha U^2+n)$. Thus $\alpha\delta^2(\alpha^2\delta^4+m\alpha\delta^2+n)\in(k(\alpha\delta^2)^*)^2$. Denote by $f(z)$ the minimal polynomial of $\alpha\delta^2$ over k. Then

$$k(E)_{f(z)}\cong k(\alpha\delta^2)(\sqrt{\alpha\delta^2(\alpha^2\delta^4+m\alpha\delta^2+n)})<\mu>,$$

where μ is a prime element of $k(E)_{f(z)}$. Then $k(E)_{f(z)}\cong k(\alpha\delta^2)<\mu>$, and either $k(\alpha\delta^2)=k$, or $[k(\alpha\delta^2):k]=p$. Then it follows that

$$\left(\frac{\pi\ ,\ z}{k(E)_{f(z)}}\right)\cong\left(\frac{\pi\ ,\ \alpha\delta^2}{k(E)_{f(z)}}\right)\cong\left(\frac{\pi\ ,\ \alpha}{k(\alpha\delta^2)<\mu>}\right)\cong\left(\frac{\pi\ ,\ \alpha}{k<\mu>}\right)\otimes_{k<\mu>}k(\alpha\delta^2)<\mu>.$$

Since the degree of the extension $k(\alpha\delta^2)<\mu>|k<\mu>$ is equal either p or 1 and the algebra $((\pi\,,\alpha)|k<\mu>)$ is non-trivial, so the algebras $((\pi\,,z)|k(E)_{f(z)})$ and $((\pi\,,z)|k(E))$ are non-trivial. Passing to the consideration of the semi-split case, observe that the proof of the non-triviality of $((\pi\ ,\ x\ )|\ k(E))$ is just the same as in the split case. Furthermore, algebras $((\pi\ ,\ x\ )|\ k(E))$ and $((\pi\ ,\ \alpha\ )|\ k(E))$ are not $k(E)$-isomorphic in view of corollary to lemma 17. It follows then $((\pi\ ,\ \alpha x\ )|\ k(E))$ is non-trivial and is isomorphic neither $((\pi\ ,\ \alpha\ )|\ k(E))$, nor $((\pi\ ,\ x\ )|\ k(E))$, and we are done in semi-split case. To finish proof of the theorem in split case it is sufficient to show that all algebras listed in the theorem which correspond to split case are not pairwise $k(E)$-isomorphic. Since all elements of $Br(k(E))$ corresponding to these algebras are of order at most 2, then for the proof of the above statement it is sufficient to observe that all of them except $((\pi\ ,\ 1\ )|\ k(E))$ are non-trivial. But for the algebras $((\pi\ ,\ \alpha\ )|\ k(E))$, $((\pi\ ,\ x\ )|\ k(E))$, $((\pi\ ,\ x-e_i\ )|\ k(E))_{i=1,2}$ the was established before and as for the algebras $((\pi\ ,\ \alpha(x-e_i)\ )|\ k(E))$ one has

$$\left(\frac{\pi\ ,\ \alpha(x-e_i)}{k(E)}\right)\sim\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\otimes_{k(E)}\left(\frac{\pi\ ,\ x-e_i}{k(E)}\right).$$

By corollary to lemma 17 we have that algebras $((\pi\ ,\ \alpha\ )|\ k(E))$, $((\pi\ ,\ x-e_i\ )|\ k(E))$ and $((\pi\ ,\ x-e_i)|\ k(E))$ are not $k(E)$-isomrphic and hence $((\pi\ ,\ \alpha(x-e_i))|k(E))$ are non-trivial.

Q.E.D.

9 The group ${}_2Br\ E$. The split case of bad reduction

In this section we shall consider the split case of bad reduction for E defined over non-dyadic field. In this case E is isomorphic over k to one of the curves defined by the equations of the following forms.

I_1. $y^2 = x(x+\alpha)(x-\pi^m a),\ \ m>0.$

I_2. $y^2 = x(x+1)(x-\pi^m a),\ \ m>0.$

II. $y^2 = x(x-\pi a)(x-\pi b),\ \ \bar{a} \neq \bar{b}.$

III. $y^2 = x(x-\pi a)(x-\pi^m b),\ \ m>1,$

where $a, b \in O_k^*$.

Then a description of elements of ${}_2Br\ E$ can be given in the following manner.

Theorem 11 *Any element of ${}_2Br\ E$ has the following form.*

In case I_1

$$\left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ x}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha x}{k(E)}\right)\right],$$

$$\left[\left(\frac{\pi\ ,\ x+\alpha}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha(x+\alpha)}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ x-\pi^m a}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha(x-\pi^m a)}{k(E)}\right)\right].$$

In case I_2

$$\left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ x}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha x}{k(E)}\right)\right],$$

$$\left[\left(\frac{\alpha\ ,\ x}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ \pi x}{k(E)}\right)\right], \left[\left(\frac{\pi\alpha\ ,\ x}{k(E)}\right)\right], \left[\left(\frac{\pi\alpha\ ,\ \alpha x}{k(E)}\right)\right].$$

In cases II and III

$$\left[\left(\frac{\alpha\ ,\ 1}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ \pi}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ x}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ x-\pi a}{k(E)}\right)\right],$$

$$\left[\left(\frac{\alpha\ ,\ \pi(x-\pi a)}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ \pi x}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ x-\pi^m b}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ \pi(x-\pi^m b)}{k(E)}\right)\right].$$

(where $m=1$ in case II and $m>1$ in case III).

Proof. We shall consider cases I_1 and I_2 simultaneously. To do this we shall assume that E is given the by equation $y^2 = x(x+b)(x-\pi^m a)$, where $b \in O_k^*$. It is easy to see that the set of all elements from ${}_2Br\ E$ listed in the case I_1 (the same also true in the case I_2) is a group of order at most 8. So we need only to prove that corresponding quaternion algebras are non-trivial, unramified and pairwise non-isomorphic. It is clear that $((\pi\ ,\ \alpha)|\,k(E))$ is unramified over $k(E)$ and non-trivial. For the point of $k(E)$ defined by the polynomial x, one has $k(E)_x \cong k<x>(\sqrt{x(x+b)(x-\pi^m a)}) \cong k<x>(\sqrt{-ab\pi^m x})$. Then for $u \in k^*$

$$\left(\frac{u\ ,\ x}{k(E)_x}\right) \cong \left(\frac{u\ ,\ -ab\pi^m}{k(E)_x}\right)$$

and therefore algebras $((\pi\,,\,x\,)|\,k(E))$ and $((\alpha,\,x\,)|\,k(E))$ are unramified over $k(E)_x$, but in view of lemma 17 they are also unramified over $k(E)_\infty$, so they are unramified over $k(E)$. By similar reasons algebras $((\pi\,,\,x+b\,)|\,k(E))$ and $((\pi\,,\,x-\pi^m a\,)|\,k(E))$ are unramified over $k(E)_\infty$. Let us show these algebras are unramified respectively at points defined by polynomials $x+b$ and $x-\pi^m a$. In fact,

$$k(E)_{x+b} \cong k <x+b> (\sqrt{(x+b)(-b)(-b-\pi^m a)}) \cong k <x+b> (\sqrt{x+b}),$$

$$k(E)_{x-\pi^m a} \cong k <x-\pi^m a> (\sqrt{(x-\pi^m a)(\pi^m a)(\pi^m a+b)}) \cong$$

$$k <x-\pi^m a> (\sqrt{ab\pi^m(x-\pi^m a)}).$$

Hence

$$\left(\frac{\pi\,,\,x+b}{k(E)_{x+b}}\right) \cong \left(\frac{\pi\,,\,x+b}{k <x+b> (\sqrt{x+b})}\right), \cong \left(\frac{\pi\,,\,1}{k <x+b> (\sqrt{x+b})}\right),$$

$$\left(\frac{\pi\,,\,x-\pi^m a}{k(E)_{x-\pi^m a}}\right) \cong \left(\frac{\pi\,,\,ab\pi^m}{k(E)_{x-\pi^m a}}\right).$$

Thus algebras $((\pi\,,\,x+b\,)|\,k(E))$ and $((\pi\,,\,x-\pi^m a\,)|\,k(E))$ are uramified over $k(E)$. As to remaining quaternion algebras appearing in cases I_1 and I_2 of the theorem all of them are similar to tensor products of the above ones, so they also unramified over $k(E)$. Finally, let us show that all quaternion algebras from I_1, I_2 except $((\pi\,,\,1\,)|\,k(E))$ are non-trivial. Let L be the unramified cubic extention of k. By lemma 1 there exists an element $\tilde{v} \in \bar{L}^*$ such that $\tilde{v} \notin (\bar{L}^*)^2, \tilde{v}+1 \in (\bar{L}^*)^2$, if $b \in (\bar{k}^*)^2$ and $\tilde{v} \in (\bar{L}^*)^2, \tilde{v}+1 \notin (\bar{L}^*)^2$, if $b \notin (\bar{k}^*)^2$. Let also $\tilde{u}^2 = \bar{b}\tilde{v}/\bar{\alpha}$, where u is a preimage $\tilde{u}$ in L, $\theta = \alpha u^2$ and $f(x)$ is the minimal polynomial of θ over k. Then

$$k(E)_{f(x)} \cong k(\theta) <f(x)> (\sqrt{\theta(\theta+b)(\theta-\pi^m a)}) = k(\theta) <f(x)> (\sqrt{\theta+b}).$$

One claims now that $\theta + b \in (k(\theta)^*)^2$. In fact, $\theta + b = \alpha u^2 + b$ and the last element (since L is non-dyadic) is a square in L^* if and only if $\bar{\alpha}\tilde{u}^2 + \bar{b} \in (\bar{L}^*)^2$. But $\bar{\alpha}\tilde{u}^2 + \bar{b} = \bar{b}\tilde{v} + \bar{b} = \bar{b}(\tilde{v}+1) \in (\bar{L}^*)^2$. Thus $\theta + b \in (L^*)^2$, and since $L|k$ is of degree either 1 or 3, then $\theta + b \in (k(\theta)^*)^2$. Hence $k(E)_{f(x)} \cong k(\theta) < f(x) >$ and therefore the degree $[k(E)_{f(x)} : k <f(x)>]$ is equal either 1 or 3. We also have

$$\left(\frac{\pi\,,\,x}{k(E)_{f(x)}}\right) = \left(\frac{\pi\,,\,\theta}{k(E)_{f(x)}}\right) = \left(\frac{\pi\,,\,\alpha}{k(E) <f(x)>}\right) \otimes_{k<f(x)>} k(\theta) <f(x)>.$$

and by the last remark about $[k(E)_{f(x)} : k <f(x)>]$ the last algebra is non-trivial if and only if $((\pi\,,\,\alpha\,)|\,k(E) <f(x)>)$ is non-trivial over $k < f(x) >$. But we know that the algebra $((\pi\,,\,\alpha\,)|\,k < f(x) >)$ are non-trivial and the same is true for $((\pi\,,\,x\,)|\,k(E)_{f(x)})$. Therefore $((\pi\,,\,x\,)|\,k(E))$ is non-trivial. If one set $z = x - \pi^m a$, then the algebra $((\pi\,,\,x - \pi^m a\,)|\,k(E))$ will be of the form $((\pi\,,\,z\,)|\,k(E))$, where E will be given by the equation $y^2 = z(z+\pi^m a)(x+(b+\pi^m a))$ and this is the case which was considered before, so $((\pi\,,\,x-\pi^m a\,)|\,k(E))$ is also non-trivial. Since $((\pi\,,\,\alpha\,)|\,k(E)) \ncong ((\pi\,,\,x\,)|\,k(E))$ by corollary to lemma 17, then $((\pi\,,\,\alpha x\,)|\,k(E))$ is non-trivial. The same argument shows that $((\pi\ ,\ \alpha(x-\pi^m a)\ )|\ k(E))$ and $((\pi\ ,\ \alpha(x+b)\ )|\ k(E))$ are also non-trivial. To prove that $((\pi\ ,\ x+b\ )|\ k(E))$ if $b\notin(k^*)^2$ let us consider the algebra $((\pi\ ,\ x+b\ )|\ k(E)_x)$:

$$\left(\frac{\pi\ ,\ x+b}{k(E)_x}\right)=\left(\frac{\pi\ ,\ x+b}{k<x>(\sqrt{-ab\pi^m x})}\right)\cong\left(\frac{\pi\ ,\ b+(-ab\pi^m x)/(-ab\pi^m)}{k<x>(\sqrt{-ab\pi^m x})}\right)\cong$$

$$\cong\left(\frac{\pi\ ,\ b}{k<\sqrt{-ab\pi^m x}>}\right).$$

The last algebra is non-trivial by $b\notin(k^*)^2$ and the same is true for $((\pi\ ,\ x+b\ )|\ k(E)_x)$. Now it is easy to see that all quaternion algebras from I_1 are pairwise not isomorphic over $k(E)$ and hence the corresponding elements of ${}_2Br\ E$ are different. To finish proof in the case I_1 one need to observe that the number of these algebras is equal to the order of ${}_2Br\ E$. As in the case I_2 we need to prove non-triviality of

$$\left(\frac{\alpha\ ,\ x}{k(E)}\right),\left(\frac{\alpha\ ,\ \pi x}{k(E)}\right),\left(\frac{\pi\alpha\ ,\ x}{k(E)}\right),\left(\frac{\pi\alpha\ ,\ \alpha x}{k(E)}\right)\ \text{provided}\ b\in(O_k^*)^2.$$

For the algebra $((\alpha\ ,\ x\ )|\ k(E))$ let us consider two cases: $m=1$ and $m>1$. If $m=1$

$$\left(\frac{\alpha\ ,\ x}{k(E)_x}\right)=\left(\frac{\alpha\ ,\ -\pi ab}{k<x>(\sqrt{-\pi abx})}\right)=\left(\frac{\pi\ ,\ \alpha}{k<\sqrt{-\pi abx}>}\right).$$

and it is clear that the last algebra is non-trivial. In case $m>1$ one has

$$\left(\frac{\alpha\ ,\ x}{k(E)_{x-\pi}}\right)=\left(\frac{\alpha\ ,\ \pi}{k<x-\pi>(\sqrt{\pi(\pi-\pi^m a)(\pi+b)})}\right)=$$

$$=\left(\frac{\alpha\ ,\ \pi}{k<x-\pi>(\sqrt{b})}\right)=\left(\frac{\alpha\ ,\ \pi}{k<x-\pi>}\right),$$

and the last algebra is again non-trivial. Therefore $((\alpha\ ,\ x\ )|\ k(E))\not\sim 1$ for any $m\geq 1$.

The algebra $((\alpha\ ,\ \pi x\ )|\ k(E))$ is non-trivial by corollary 6.

For the algebra $((\pi\alpha\ ,\ x\ )|\ k(E))$ one can pass to another prime element $\nu=\pi\alpha$ of k and we have the case which was considered before. Furthermore,

$$\left(\frac{\pi\alpha\ ,\ \alpha x}{k(E)}\right)\sim\left(\frac{\nu\ ,\ x}{k(E)}\right)\otimes\left(\frac{\nu\ ,\ \alpha}{k(E)}\right),$$

and the last algebra is non-trivial by corrolary 6.

Let us consider finally the cases II and III. In these cases E is given by the equation $y^2=x(x-\pi a)(x-\pi^m b)$, where either $m>1$ or $\bar{a}\neq\bar{b}$.

To prove that all quaternions algebras from the cases II and III are unramified over $k(E)$ it is enough to prove that algebras $((\alpha\ ,\ x\ )|\ k(E))$ and $((\alpha\ ,\ x-\pi a\ )|\ k(E))$ are unramified (since

$$\left(\frac{\alpha\ ,\ x-\pi^m b}{k(E)}\right)\sim\left(\frac{\alpha\ ,\ x}{k(E)}\right)\otimes\left(\frac{\alpha\ ,\ x-\pi a}{k(E)}\right),$$

and tensor product of uramified algebras is also unramified). The algebras $((\alpha, x)|k(E)_\infty)$ and $((\alpha\, ,\ x - \pi a\,)|\,k(E)_\infty)$ are unramified by lemma 17. Furthermore,

$$\left(\frac{\alpha\ ,\ x}{k(E)_x}\right) \cong \left(\frac{\alpha\ ,\ x}{k<x>(\sqrt{ab\pi^{m+1}x})}\right) \cong \left(\frac{\alpha\ ,\ ab\pi^{m+1}}{k<x>(\sqrt{ab\pi^{m+1}x})}\right),$$

and the last algebra is obtained by an extension of scalars from $((\alpha\, ,\ ab\pi^{m+1}\,)|\,k)$, so it is unramified over $k(E)_x$.

$$\left(\frac{\alpha\ ,\ x-\pi a}{k(E)_{x-\pi a}}\right) \cong \left(\frac{\alpha\ ,\ x-\pi a}{k<x-\pi a>(\sqrt{\pi a(\pi a-\pi^m b)(x-\pi a)})}\right) \cong$$

$$\cong \left(\frac{\alpha\ ,\ 1-\pi^{m-1}b/a}{k<x-\pi a>(\sqrt{(x-\pi a)(1-\pi^{m-1}b/a)})}\right),$$

and again the similar arguments shows that the last algebra is unramified.

To finish proof of the theorem it is enough to prove that algebras

$$\left(\frac{\alpha\ ,\ x}{k(E)}\right),\ \left(\frac{\alpha\ ,\ x-\pi a}{k(E)}\right) \text{ and } \left(\frac{\alpha\ ,\ x-\pi^m b}{k(E)}\right)$$

are non-trivial. (Since

$$\left(\frac{\alpha\ ,\ \pi(x-\pi a)}{k(E)}\right) \not\sim 1,\ \left(\frac{\alpha\ ,\ \pi x}{k(E)}\right) \not\sim 1 \text{ and } \left(\frac{\alpha\ ,\ \pi(x-\pi^m b)}{k(E)}\right) \not\sim 1$$

by corrolary 6.) This by the last assertion can be proved as follows:

$$\left(\frac{\alpha\ ,\ x}{k(E)_{x-\pi a}}\right) \cong \left(\frac{\alpha\ ,\ \pi a}{k<x-\pi a>(\sqrt{(x-\pi a)(1-\pi^{m-1}b/a)})}\right) \not\sim 1,$$

$$\left(\frac{\alpha\ ,\ x-\pi a}{k(E)_x}\right) \cong \left(\frac{\alpha\ ,\ -\pi a}{k<x>(\sqrt{ab\pi^{m+1}x})}\right) \not\sim 1,$$

$$\left(\frac{\alpha\ ,\ x-\pi^m b}{k(E)_{x-\pi a}}\right) \cong \left(\frac{\alpha\ ,\ \pi(a-\pi^{m-1}b)}{k<x-\pi a>(\sqrt{(x-\pi a)(1-\pi^{m-1}b/a)})}\right),$$

and since $a-\pi^{m-1}b \in O_k^*$, the last algebra is non-trivial.

Q.E.D.

10 The group ${}_2Br\ E$. The semi-split case of additive reduction

In case of additive reduction the group ${}_2Br\ E$ can be described as follows.

Theorem 12 *Let E be an elliptic curve over a non-dyadic local field k with additive reduction. Then in the semi-split case the group ${}_2Br\ E$ consists of the following elements:*

In case $A.a)$:

$$\left[\left(\frac{\pi\,,\,1}{k(E)}\right)\right],\left[\left(\frac{\pi\,,\,\alpha}{k(E)}\right)\right],\left[\left(\frac{\alpha\,,\,x}{k(E)}\right)\right],\left[\left(\frac{\alpha\,,\,\pi x}{k(E)}\right)\right].$$

In case $A.b)$:

$$\left[\left(\frac{\pi\,,\,1}{k(E)}\right)\right],\left[\left(\frac{\pi\,,\,\alpha}{k(E)}\right)\right],\left[\left(\frac{\pi\,,\,x}{k(E)}\right)\right],\left[\left(\frac{\pi\,,\,\alpha x}{k(E)}\right)\right].$$

In case $A.c)$:

$$\left[\left(\frac{\pi\,,\,1}{k(E)}\right)\right],\left[\left(\frac{\pi\,,\,\alpha}{k(E)}\right)\right],$$

$$\left[\left(\frac{\pi\sqrt{b}g(u)u\,,\,x-\pi\sqrt{b}u}{k(E)}\right)\right],\left[\left(\frac{\pi\sqrt{b}g(u)u\,,\,\alpha(x-\pi\sqrt{b}u)}{k(E)}\right)\right],$$

where $g(x)\in k[x]$ *and*

$$g(x)=\begin{cases} x^2+1 & \textit{in cases } A.c)1-A.c)2,\\ x^2+(a/\sqrt{b})x+1 & \textit{in cases } A.c)3-A.c)4,\end{cases}$$

and

$$u\in O_k^*,\ g(u)\in O_k^*\setminus(O_k^*)^2\ \textit{ in cases } A.c)1-A.c)3,\ \textit{ and}$$
$$u=-1+\pi^r w,\ w\in O_k^*,\ w^2-c\in O_k^*\setminus(O_k^*)^2\ \textit{ in case } A.c)4.$$

In case $A.d)$:

$$\left[\left(\frac{\pi\,,\,1}{k(E)}\right)\right],\left[\left(\frac{\pi\,,\,\alpha}{k(E)}\right)\right],\left[\left(\frac{\alpha\,,\,x+\pi\sqrt{b}}{k(E)}\right)\right],\left[\left(\frac{\alpha\,,\,\alpha\pi(x+\pi\sqrt{b})}{k(E)}\right)\right].$$

In case $A.e)$:

$$\left[\left(\frac{\pi\,,\,1}{k(E)}\right)\right],\left[\left(\frac{\pi\,,\,\alpha}{k(E)}\right)\right],\left[\left(\frac{\alpha\,,\,x}{k(E)}\right)\right],\left[\left(\frac{\alpha\,,\,\pi x}{k(E)}\right)\right].$$

Proof. To present all elements of ${}_2Br\ E$ it is enough to have a quaternion algebra, which is unramified and non-trivial over $k(E)$ and non-isomorphic to $((\pi\,,\,\alpha)|\,k(E))$ (because the order of ${}_2Br\ E$ is 4 and $[((\pi\,,\,1)|\,k(E))]$, $[((\pi\,,\,\alpha)|\,k(E))]$ are different elements of ${}_2Br\ E$). To do this, let us firstly assume that E is given by the equation $y^2=x(x^2+\pi^m ax+\pi^t b)$, where $a\in O_k^*\bigcup\{0\},\ b\in O_k^*,\ m>0,\ t=1,2,3$. In the case of odd t let us consider the algebra $((\alpha\,,\,x)|\,k(E))$. Then

$$\left(\frac{\alpha\,,\,x}{k(E)_x}\right)\cong\left(\frac{\alpha\,,\,\pi^t b}{k<\sqrt{\pi^t bx}>}\right)\cong\left(\frac{\alpha\,,\,\pi}{k<\sqrt{\pi^t bx}>}\right),$$

Hence the algebra $((\alpha\,,\,x)|\,k(E))$ is non-trivial and unramified over $k(E)$ and it is not isomorphic to $((\pi\,,\,\alpha)|\,k(E))$ by corrolary to lemma 17. In case $t=2,\ b\notin(k^*)^2$ let us consider the algebra $((\pi\,,\,x)|\,k(E))$. Then

$$\left(\frac{\pi\,,\,x}{k(E)_x}\right)\cong\left(\frac{\pi\,,\,b}{k<\sqrt{bx}>}\right),$$

and therefore $((\pi\ ,\ x\ )|\, k(E))$ is non-trivial and unramified over $k(E)$. Again by corrolary to lemma 17 it is non-isomorphic to $((\pi\ ,\ \alpha\ )|\, k(E))$.

If E cannot be given by an equation of the above form, then it can be given by the equation $y^2 = x(x^2 + \pi^m ax + \pi^2 b)$, where $a \in O_k^* \bigcup\{0\},\ b \in (O_k^*)^2,\ m > 0$.

Passing to another prime element $\nu = \pi\sqrt{b}$ of k we shall transform the above equations for E to the following ones

$$y^2 = x(x^2 + \nu^2)$$

$$y^2 = x(x^2 + \nu^m \tilde{a}x + \nu^2),\ \text{where}\ \tilde{a} = a/(\sqrt{b})^m.$$

According to the list of minimal Weierstrass equations for E we shall have the following possibilities.

$A.c)1\ \ y^2 = x(x^2 + \nu^2),\ -1 \notin (k^*)^2;$

$A.c)2\ \ y^2 = x(x^2 + \nu^m \tilde{a}x + \nu^2),\ m > 1,\ -1 \notin (k^*)^2;$

$A.c)3\ \ y^2 = x(x^2 + \nu\tilde{a}x + \nu^2),\ \overline{\tilde{a}^2} - 4 \notin (\bar{k}^*)^2 \bigcup\{0\};$

$A.c)4\ \ y^2 = x(x^2 + \nu\tilde{a}x + \nu^2),\ \tilde{a} = 2 + \nu^{2r}c/b^r,\ c \in O_k^* \setminus (O_k^*)^2;$

$A.d)\ \ y^2 = x(x^2 + \nu\tilde{a}x + \nu^2),\ \tilde{a} = 2 + \nu^{2r+1}c/(b^r\sqrt{b}),\ c\sqrt{b} \in O_k^* \setminus (O_k^*)^2.$

$A.e)\ \ y^2 = x(x^2 + \nu\tilde{a}x + \nu^2),\ \tilde{a} = 2 + \nu^{2r+1}c/(b^r\sqrt{b}),\ c\sqrt{b} \in (O_k^*)^2.$

Let us show that in the first four cases there exists an element $u \in O_k^*$ such that the algebra $((\nu ug(u)\ ,\ x - \nu u)|\, k(E))$ is non-trivial, unramified over $k(E)$ and non-isomorphic to $((\pi\ ,\ \alpha\ )|\, k(E))$. To prove this let us begin with cases $A.c)1 - A.c)3$. In these cases there exists an element $\tilde{u} \in \bar{k}^*$ such that $\bar{g}(\tilde{u}) \in O_k^* \setminus (O_k^*)^2$. If $|\bar{k}| \geq 7$, then it is true by proposition 1, and moreover, $\tilde{u} \neq 0$, since $\bar{g}(0) \in (\bar{k}^*)^2$.

Let $|\bar{k}| < 7$. Then in the cases $A.c)1, A.c)2$ $\bar{k} = \boldsymbol{F}_3$ (Since $-1 \in (\boldsymbol{F}_5^*)^2$) and by corollary 1 there exists an element $\tilde{u} \in \boldsymbol{F}_3^*$ such that $\bar{g}(\tilde{u}) \in \boldsymbol{F}_3^* \setminus (\boldsymbol{F}_3^*)^2$. In the case $A.c)3$ we have

$$\bar{g}(x) = x^2 + \bar{\tilde{a}}x + 1 = \left(x + \frac{\bar{\tilde{a}}}{2}\right)^2 + \left(-\frac{\bar{\tilde{a}}^2 - 4}{4}\right),\quad \frac{\bar{\tilde{a}}^2 - 4}{4} \notin (\bar{k}^*)^2 \bigcup\{0\}.$$

If $\bar{k} = \boldsymbol{F}_3$, then $(\bar{\tilde{a}}^2 - 4)/4 \in (\boldsymbol{F}_3^*)^2$ and therefore again by corollary 1 there exists such an element $\tilde{u}$ and $\tilde{u} \neq 0$ since $\bar{g}(0) = 1 \in (\boldsymbol{F}_3^*)^2$. For the remaining case $A.c)3$, $\bar{k} = \boldsymbol{F}_5$ and we can use again corollary 1.

Let now u is a preimage of $\tilde{u}$ in k. Then $u \in O_k^*$ and $g(u) \in O_k^* \setminus (O_k^*)^2$. Hence

$$\left(\frac{\nu ug(u)\ ,\ x - \nu u}{k(E)_x}\right) \cong \left(\frac{\nu ug(u)\ ,\ -\nu u}{k < \sqrt{x} >}\right) \cong \left(\frac{g(u)\ ,\ -\nu u}{k < \sqrt{x} >}\right).$$

The last algebra is non-trivial and the same is true for $((\nu ug(u)\ ,\ x - \nu u\ )|\, k(E))$. In view of corollary to lemma 17 it is not isomorphic to $((\pi\ ,\ \alpha\ )|\, k(E))$. Let us check it is unramified.

$$\left(\frac{\nu ug(u)\ ,\ x - \nu u}{k(E)_{x-\nu u}}\right) \cong \left(\frac{\nu ug(u)\ ,\ x - \nu u}{k < x - \nu u > (\sqrt{\nu ug(u)})}\right).$$

The last algebra is trivial so it is unramified. Finishing consideration of the cases $A.c)1-$ $-A.c)3$ let us observe that the algebra $((\nu ug(u)\ ,\ x-\nu u\ )|\ k(E)_\infty)$ is unramified by lemma 17.

Let us consider the case $A.c)4$. The algebra $((\nu ug(u)\,,\ x-\nu u\ )|\ k(E))$, $u\in O_k^*$ is again non-isomorphic to $((\pi\ ,\ \alpha\ )|\ k(E))$. To prove that it is unramified over $k(E)$ one needs to repeat the previous arguments. Now let us choose $u\in O_k^*$ to satisfy the condition that the algebra $((\nu ug(u)\ ,\ x-\nu u\ )|\ k(E))$ is non-trivial. To do this let us show firstly that there is $\tilde v\in\bar k^*$ such that $\tilde v^2-\bar c/\bar b^r\in\bar k^*\setminus(\bar k^*)^2$, $\bar c\notin(\bar k^*)^2, \bar b\in(\bar k^*)^2$, i.e.

$$\tilde v^2+\left(-\frac{\bar c}{\bar b^r}\right)\notin(\bar k^*)^2 \text{ and } \frac{\bar c}{\bar b^r}\notin(\bar k^*)^2.$$

Now the existence of such $\tilde v$ follows from corollary 1. Let v be a preimage of $\tilde v$ in k, $u=-1+\nu^r v$, $w=(\sqrt{b})^r v$. Then $u=-1+\pi^r w$, $\bar w^2-\bar c=\bar b^r\bar v^2-\bar c=\bar b^r(\tilde v^2-\bar c/\bar b^r)\notin(\bar k^*)^2$ and therefore $w^2-c\in O_k^*\setminus(O_k^*)^2$. Furthermore, $g(u)=(-1+\nu^r v)^2+(2+\nu^{2r}c/b^r)(-1+\nu^r v)+1=\nu^{2r}(v^2-c/b^r+\nu^r cb/b^r)\in\alpha(k^*)^2$ since $\bar v^2-\bar c/\bar b^r\in\bar k^*\setminus(\bar k^*)^2$. Hence

$$\left(\frac{\nu ug(u)\ ,\ x-\nu u}{k(E)_x}\right)\cong\left(\frac{\nu ug(u)\ ,\ -\nu u}{k<x>}\right)\cong\left(\frac{g(u)\ ,\ -\nu u}{k<x>}\right).$$

The last algebra is non-trivial and so it is true for $((\nu ug(u)\ ,\ x-\nu u\ )|\ k(E))$.

Passing to consideration of the case $A.d)$ let us choose $u\in O_k^*$ in such a way that the algebra $((\alpha, x-u\nu)|k(E)_{x-u\nu})$ would be trivial. It will be done, if $\nu u((\nu u)^2+\nu\tilde a(\nu u)+\nu^2)\in\alpha(k^*)^2$. Really, in this case the field $k(E)_{x-u\nu}\cong k(\sqrt{\alpha})<x-u\nu>$ splits the last algebra. We have also

$$\nu u(\nu^2u^2+\nu^2u(2+\nu^{2r+1}\frac{c}{b^r\sqrt{b}}+\nu^2))=\nu^3u((u+1)^2+\nu^{2r+1}\frac{cu}{b^r\sqrt{b}})\in\alpha(k^*)^2.$$

If one set $u=-1$, then the last expression is equal to $c\sqrt{b}$ up to a square, and therefore satisfies to our requirement. So the algebra $((\nu ug(u)\,,\ x-\nu u\ )|\ k(E))$ is unramified and it is not isomorphic to $((\pi\ ,\ \alpha\ )|\ k(E))$. To prove its non-triviality let us consider the algebra $((\alpha\ ,\ x-u\nu\ )|\ k(E)_x)$. Then

$$\left(\frac{\alpha\ ,\ x-u\nu}{k(E)_x}\right)\cong\left(\frac{\alpha\ ,\ -u\nu}{k<x>(\sqrt{x})}\right)$$

and the last algebra is non-trivial.

In the case $A.e)$ let us consider the algebra $((\alpha\ ,\ x\ )|\ k(E))$ which is not isomorphic to $((\pi\ ,\ \alpha\ )|\ k(E))$. Moreover, the algebra

$$\left(\frac{\alpha\ ,\ x}{k(E)_x}\right)\cong\left(\frac{\alpha\ ,\ x}{k<\sqrt{x}>}\right)$$

is trivial, and therefore is uramified, so it is true for $\left(\frac{\alpha\ ,\ x}{k(E)}\right)$. The last algebra is also non-trivial because

$$k(E)_{x+\nu}\cong k<x+\nu>(\sqrt{-\nu(\nu^2-\tilde a\nu^2+\nu^2)})=k<x+\nu>(\sqrt{\frac{c}{b^r\sqrt{b}}})=k<x+\nu>.$$

So

$$\left(\frac{\alpha\ ,\ x}{k(E)_{x+\nu}}\right)\cong\left(\frac{\alpha\ ,\ -\nu}{k<x+\nu>}\right)$$

is a non-trivial algebra. Thus the theorem is proved.

11 The group ${}_2Br\ E$. The semi-split case of multiplicative reduction

The presentation of elements of ${}_2Br\ E$ by quaternion algebras in semi-split case of multiplicative reduction of E is as follows.

Theorem 13 *Let E be elliptic curve over a non-dyadic local field k with multiplicative reduction. In the semi-split case the group ${}_2Br\ E$ consists of the following elements:*

In case $M.a)$

$$\left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right], \left[\left(\frac{\pi b\ ,\ x+a}{k(E)}\right)\right], \left[\left(\frac{\pi b\ ,\ \alpha(x+a)}{k(E)}\right)\right];$$

In case $M.b)$

$$\left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ x}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha x}{k(E)}\right)\right];$$

In case $M.c)$

$$\left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ x+a}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ \pi(x+a)}{k(E)}\right)\right];$$

In case $M.d)$

$$\left[\left(\frac{\pi\ ,\ 1}{k(E)}\right)\right], \left[\left(\frac{\pi\ ,\ \alpha}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ x+a-v\pi^m}{k(E)}\right)\right], \left[\left(\frac{\alpha\ ,\ \pi(x+a-v\pi^m)}{k(E)}\right)\right],$$

where $v \in O_k^*$, $v^2 - ab \in O_k^* \setminus (O_k^*)^2$ and a, b, m are just the same as in the corresponding list of minimal Weierstrass equations.

Proof. Similar to proof of the previous theorem we only need to indicate in every of possible case a non-trivial unramified quaternion algebra which is not isomorphic to $((\pi\ ,\ \alpha\ )|\ k(E))$. A curve E may be given by the equation $y^2 = x((x+a)^2 + \pi^s bx)$, where $a, b \in O_k^*$, $s > 0$.

Let s be odd. Then the algebra $((\pi b,\ x+a\ )|k(E))$ is non-isomorphic to $((\pi,\ \alpha\ )|k(E))$ and unramified in view of

$$\left(\frac{\pi b\ ,\ x+a}{k(E)_{x+a}}\right) \cong \left(\frac{\pi b\ ,\ x+a}{k<x+a>(\sqrt{\pi^s b})}\right) \cong \left(\frac{\pi\ ,\ 1}{k<x+a>(\sqrt{\pi^s b})}\right).$$

Furthermore, if L is the unramified cubic extention of k then by corollary to lemma 1 there exists an element $\tilde{w} \in (\bar{L}^*)^2$ such that $\bar{a} + \tilde{w} \in \bar{L}^* \setminus (\bar{L}^*)^2$. Let w be a preimage of $\tilde{w}$ in L and $f(x)$ its minimal polynomial over k. Then

$$\left(\frac{\pi b\ ,\ x+a}{k(E)_f}\right) \cong \left(\frac{\pi b\ ,\ a+w}{k(w)<f>(\sqrt{w((w+a)^2+\pi^s bw)})}\right) \cong \left(\frac{\pi b\ ,\ a+w}{k(w)<f>}\right).$$

The last algebra obviously is non-trivial so this is true for $((\pi b\,,\ x+a\,)|\,k(E))$.

Let now $s=2m$. If $-a\notin (k^*)^2$, then the algebra $((\pi\,,\ x\,)|\,k(E))$ satisfies our requirements. Really, in view of corollary to lemma 17 it is not isomorphic to $((\pi\,,\ \alpha\,)|\,k(E))$. Moreover,

$$\left(\frac{\pi\,,\ x}{k(E)_x}\right)\cong\left(\frac{\pi\,,\ x}{k<x>(\sqrt{x((x+a)^2+\pi^s bx)})}\right)\cong\left(\frac{\pi\,,\ x}{k<\sqrt{x}>}\right)\cong\left(\frac{\pi\,,1}{k<\sqrt{x}>}\right).$$

Finally, $((\pi\,,\ x\,)|\,k(E))$ is non-trivial. To see this one can choose an element $\tilde{v}\in k^*$ such that $\tilde{v}^2+(-\overline{ab})\in\bar{k}^*\setminus(\bar{k}^*)^2$. The irreducibility of the polynomial $(x+a)^2+\pi^s bx$ over k implies $ab\notin(k^*)^2$. In case $\bar{k}=\mathbb{F}_3$ it follows from the last condition that $(-\overline{ab})\in(\bar{k}^*)^2$, and then by corollary to lemma 1 one concludes that needed $\tilde{v}$ exists. If $|\bar{k}|\geq 5$, then existence of needed $\tilde{v}$ follows in view of the same corollary.

Let us denote by v a preimage $\tilde{v}$ in k. Then

$$\left(\frac{\pi\,,\ x}{k(E)_{x+a-\pi^m v}}\right)\cong\left(\frac{\pi\,,\ -a}{k<x+a-\pi^m v>(\sqrt{(-a)(\pi^{2m}v^2+(-a+\pi^m v)\pi^{2m}b)})}\right)=$$

$$\left(\frac{\pi\,,\ -a}{k<x+a-\pi^m v>(\sqrt{-a(v^2-ab)})}\right)=\left(\frac{\pi\,,\ -a}{k<x+a-\pi^m v>(\sqrt{-a(v^2-ab)})}\right)=$$

$$\left(\frac{\pi\,,\ -a}{k<\,x+a-\pi^m v\,>}\right),$$

and the last algebra is non-trivial.

Finally, let $s=2m$, and $(-a)\in(k^*)^2$. If $-1\in(k^*)^2$, then $a\in(k^*)^2$, $b\notin(k^*)^2$ and one can take the algebra $((\alpha\,,\ x+a\,)|\,k(E))$. As before to prove this algebra is unramified it is enough to prove that $((\alpha\,,\ x+a\,)|\,k(E)_{x+a})$ is unramified. Since $k(E)_{x+a}\cong k<x+a>(\sqrt{(-a)\pi^s b(-a)})=k<x+a>(\sqrt{b})$ one has

$$\left(\frac{\alpha\,,\ x+a}{k(E)_{x+a}}\right)\cong\left(\frac{\alpha\,,\ x+a}{k<x+a>(\sqrt{b})}\right)\cong\left(\frac{\pi\,,\ 1}{k<x+a>(\sqrt{b})}\right).$$

Thus the algebra $((\alpha,\ x+a\,)|\,k(E))$ is unramified. Let us prove that it is also non-trivial. If $f(x)$ is the minimal polynomial of $(-a+\sqrt[3]{\pi})$ over k and $\Pi=\sqrt[3]{\pi}$. Then

$$\left(\frac{\alpha\,,\ x+a}{k(E)_f}\right)\cong\left(\frac{\alpha\,,\ \Pi}{k<f>(\Pi)(\sqrt{(-a+\Pi)(\Pi^2+\Pi^{3s}b(-a+\Pi))})}\right)\cong\left(\frac{\alpha\,,\ \Pi}{k<f>(\Pi)}\right)$$

and the last algebra obviously is non-trivial. Hence $((\alpha\,,\ x+a\,)|\,k(E))$ is also non-trivial. Moreover, it is not isomorphic to $((\pi\,,\ \alpha\,)|\,k(E))$.

Let $s=2m$, $-1,a\notin(k^*)^2 u=a-v\pi^m$ and $v\in O_k^*$ such that $\bar{v}^2-\bar{a}\bar{b}\in\bar{k}^*\setminus(\bar{k}^*)^2$ (such an element exists in view of corollary to lemma 1). Let us consider the algebra $((\alpha\,,\ x+u\,)|\,k(E))$. Then

$$\left(\frac{\alpha\,,\ x+u}{k(E)_{x+u}}\right)\cong\left(\frac{\alpha\,,\ x+u}{k<x+u>(\sqrt{(-a)(v^2\pi^{2m}+\pi^{2m}b(-a+v\pi^m))})}\right)$$

$$\cong \left(\frac{\alpha\, ,\, x+u}{k<x+u>(\sqrt{v^2-ab})}\right) \cong \left(\frac{\pi\, ,\, 1}{k<x+u>(\sqrt{v^2-ab})}\right).$$

Since by lemma 17 the algebra $((\alpha\, ,\, x+u\,)|\, k(E)_\infty)$ is trivial, then $((\alpha\, ,\, x+u\,)|\, k(E))$ is unramified. If $\Pi = \sqrt[3]{\pi}$ and $f(x)$ is the minimal polynomial of $-u+\Pi$ over k, then

$$\left(\frac{\alpha\, ,\, x+u}{k(E)_f}\right) \cong \left(\frac{\alpha\, ,\, x+u}{k<f>(\Pi)(\sqrt{(-u+\Pi)((\Pi+v\pi^m)^2+\pi^{2m}b(-a+v\pi^m+\Pi))}}\right) =$$

$$\left(\frac{\alpha\, ,\, \Pi}{k(\Pi)<f>(\sqrt{\Pi^2+\Pi^r\delta})}\right),$$

where $r>2$ and $\delta \in O_k^*$. The last algebra is of the form $((\alpha\, ,\, \Pi\,)|\, k(\Pi)<f>)$ and hence is non-trivial, so one can conclude that $((\alpha\, ,\, x+u\,)|\, k(E))$ is also non-trivial. Since it is not isomorphic to $((\pi\, ,\, \alpha\,)|\, k(E))$, the theorem is proved.

Q.E.D.

28.12.94

BELARUS 220073
Minsk, Surganov str. 11
Institute of Mathematics
Vyacheslav Yanchevskii
imanb%imanb.belpak.by@demos.su

BELARUS 220012
Minsk, Surganov str. 6
Institute of Engineering Cybernetics
Gennady Margolin
mahaniok%bas10.basnet.minsk.by@demos.su

References

[1] Demeyer F.R., Knus M.A.: *The Brauer group of a real curve.* Proc. Amer. Math. Soc., vol.57, n.2, 1976, p.233-270.

[2] Gross B.H., Harris J.: *Real algebraic curves.* Ann. Scient. Norm. Sup., 1981, t.14, p.157-182.

[3] Witt E.: *Zerlegung reeller algebraischer Funktionen in Quadrate. Schiefkőrper űber reellem Functionkőrper.* J. Reine Angew. Math., 1934, b.171, s.4-11.

[4] Scharlau W.: *Über die Brauer-Gruppe eines algebraischen Funktionenkőrpers in einer Variablen.* J. fűr die reine und angew. Math., 1969, bd.239-240, p.1-6.

[5] Lichtenbaum S.: *Duality theorems for curves over p-adic fields.* Invent. Math., vol 7, p.120-136 (1969).

[6] Colliot-Thélène J.-P.(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.

[7] Tate J.: *Algorithm for determining the type of a singular fiber in an elliptic pencil.* Modular functions in One Variable IV, Lecture Notes in Math.476, Springer-Verlag, 1975, p.33-52.

[8] Serre J.-P.: *Cohomologie Galoisienne.* Lecture Notes in Math.5. Springer-Verlag. 1973.

[9] Tate J.: *WC-groups over p-adic fields.* Seminaire Bourbaki, Décembre 1957, n.1556.

[10] Bashmakov M.I.: *Cohomologies of abelian varieties over number field.* Uspehi mat. nauk, 1972, v.27, N.6(168), p.25-66. (In russian).

[11] Schoof R.: *Nonsingular plane curves over finite fields.* J. Combin. Theory, ser.A, vol.46, 1987, n.2, p.183-211.

[12] Voloh J.F.: *A note on elliptic curves over finite fields.* Bull. Soc. Math. France., 1988, vol.116, p.455-458.

[13] Waterhouse W.C.: *Abelian varieties over finite fields.* Ann. Sci. E.N.S., ser.4, 1969, vol.2, p.521-560.

[14] Silverman J.: *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1985.

[15] Husemőller D.: *Elliptic Curves.* Graduate Texts in Math.111, Springer-Verlag, 1986..

[16] Lang S.: *Abelian Varieties.* New-York: Interscience, 1959.

[17] Knebusch M.: *On algebraic curves over real closed fields II.* Mathematische Zeitschrift, Springer-Verlag, 1976, bd.151, p.189-205.

[18] Parshin A.N.: *Abelian coverings of arithmetic schemes.* Doklady Akad. Nauk SSSR, v.243, n.4, 1978, p.855-858. (In russian).

[19] Shuji Saito : *Arithmetic on Two-dimensional Local Rings.* Invent. math. 85, p.379-414 (1986).

[20] P. Swinnerton-Dyer : *The Brauer group of cubic surfaces.* Math. Paroc. of the Cambridge Philosophical Society. Vol.113, May 1993, part 3, p.449-460.

[21] J.-L. Colliot-Thélène and P. Swinnerton-Dyer *Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties.* Preprint Universitè de Paris-SUD N14, 1993.

[22] Merkurjev A.S.: *On the norm residue symbol of degree 2.* Dokl. Akad. Nauk SSSR 261, 542-547 (1981); (English Translation) Sov. Math. Dokl. 24, 546-551 (1981).

[23] C. Chevalley : *Introduction to the theory of algebraic functions of one variable.* AMS, Math. Surv., v.1 N.-Y. 1951.

[24] Tsfasman M. and Vlăduţ S.: *Algebraic-geometric Codes.* Kluwer Academic Publishers, 1991.