COLLOQUIUM MATHEMATICUM

Online First version

WILD AND EVEN POINTS IN GLOBAL FUNCTION FIELDS

BY

ALFRED CZOGAŁA, PRZEMYSŁAW KOPROWSKI and
BEATA ROTHKEGEL (Katowice)

Abstract. We develop a criterion for a point of a global function field to be a unique wild point of some self-equivalence of this field. We show that this happens if and only if the class of the point in the Picard group of the field is 2-divisible. Moreover, given a finite set of points whose classes are 2-divisible in the Picard group, we show that there is always a self-equivalence of the field for which this is precisely the set of wild points. Unfortunately, for more than one point this condition is no longer necessary.

1. Introduction and related works. Hilbert-symbol equivalence (formerly known under the name *reciprocity equivalence*) appeared for the first time in the early 90's in papers by J. Carpenter, P. E. Conner, R. Litherland, R. Perlis, K. Szymiczek and the first author (see e.g. [PSCL94]). It was originally introduced as a tool for investigating Witt equivalence of global fields (two fields are said to be *Witt equivalent* when their Witt rings of similarity classes of non-degenerate quadratic forms are isomorphic—roughly speaking, Witt equivalent fields admit "equivalent" classes of orthogonal geometries). Nowadays, it is known that Witt equivalence of fields is closely related to étale cohomology. For fields of rational functions $K = k(X)$, the relevant groups are: $H^1(K, \mathbb{Z}/2) \cong K^\times/K^{\times 2}$, the group of square classes of K, and $H^2(K, \mathbb{Z}/2) \cong \operatorname{Br}_2(K)$, the group of 2-torsion elements in the Brauer group of K. When one passes to a finite extension of the field of rational functions, i.e. to the function field of an algebraic curve X, the group $\operatorname{Pic} X/2 \operatorname{Pic} X$ becomes relevant, too.

Recently, the theory of Hilbert-symbol equivalence developed into a research subject by itself. It was generalized to higher-degree symbols (see e.g. [CS97], [CS98]), to quaternion-symbol equivalence of real function fields (see e.g. [Kop02]), as well to a ring setting (see e.g. [RC07]). One of the problems considered in this theory is to describe self-equivalences of a given field.

2010 *Mathematics Subject Classification*: Primary 11E12; Secondary 11E81, 11G20, 14H05.

Key words and phrases: self-equivalence, small equivalence, wild prime.

Received 4 May 2016; revised 18 January 2018.

Published online *.

DOI: 10.4064/cm6979-1-2018

Let K be a global field of characteristic $\neq 2$ and let X denote the set of all primes of K (i.e. classes of non-trivial places on K). A *self-equivalence* of K is a pair (T, t), consisting of a bijection $T : X \xrightarrow{\sim} X$ and an automorphism $t : K^\times/K^{\times 2} \xrightarrow{\sim} K^\times/K^{\times 2}$ of the square-class group of K satisfying the condition

$$(\lambda, \mu)_\mathfrak{p} = (t\lambda, t\mu)_{T\mathfrak{p}} \quad \text{for all } \mathfrak{p} \in X \text{ and } \lambda, \mu \in K^\times/K^{\times 2}.$$

Here, $(\cdot, \cdot)_\mathfrak{p}$ denotes the Hilbert symbol

$$K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2} \times K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2} \to \{\pm 1\}.$$

Every self-equivalence of a global field induces an automorphism of its Witt ring. Given a self-equivalence of a global field K, a prime $\mathfrak{p}$ of K is called *tame* if $\operatorname{ord}_\mathfrak{p} \lambda \equiv \operatorname{ord}_{T\mathfrak{p}} t\lambda \pmod 2$ for all $\lambda \in K$. Otherwise $\mathfrak{p}$ is called *wild.* A few years ago, M. Somodi gave a full characterization of all finite sets of wild primes in $\mathbb{Q}$ (see [Som06]) and in $\mathbb{Q}(i)$ (see [Som08]). His results were recently generalized to a broad class of number fields by two of the present authors [CR14]).

In this paper, we consider the same question for global function fields, i.e. algebraic function fields in one variable over finite fields. Hence from now on, K is a global function field of characteristic $\neq 2$ and a (finite) field $\mathbb{F}_q$ is the full field of constants of K. We may think of K as a field of rational functions on some smooth, irreducible complete curve X. The closed points of X are identified with non-trivial places of K. We shall never explicitly refer to the generic point of X. Thus, in what follows, we use the word "point" to mean "closed point". We denote the set of closed points again by X. We show (Theorem 4.7) that a point $\mathfrak{p} \in X$ is a unique wild point for some self-equivalence of K if and only if its class in the Picard group of X is 2-divisible (i.e. belongs to the subgroup $2 \operatorname{Pic} X$). One implication of this theorem still holds even when we increase the number of points; this way we obtain a complete counterpart (Theorem 4.8) for function fields of the results from [Som06, Som08, CR14]. These two results establish a direct link between the property of being wild (for some self-equivalence) and 2-divisibility in the Picard group of K. For this reason, we develop in Section 3 some criteria for the class of a point $\mathfrak{p} \in X$ to be 2-divisible in $\operatorname{Pic} X$. In particular, we show (Theorem 3.7) that a point of a hyperelliptic curve (of odd degree) is 2-divisible in $\operatorname{Pic} X$ (hence is a unique wild point of some self-equivalence) if and only if its norm over the rational function field is represented by the norm of the field extension $K/\mathbb{F}_q(x)$. This in turn implies that for such curves, wild points always exist (Proposition 3.11).

We use the following notation. Given a function field K and a point $\mathfrak{p} \in X$, we denote by $\mathcal{O}_\mathfrak{p}$ the associated valuation ring, by $K_\mathfrak{p}$ the completion of K and by $K(\mathfrak{p})$ the residue field. The degree $[K(\mathfrak{p}) : \mathbb{F}_q]$ of the residue field of $\mathfrak{p}$ over the full field of constants is called the *degree* of $\mathfrak{p}$ and denoted $\deg \mathfrak{p}$. Given a non-empty, open subset $Y \subseteq X$, we write $\mathcal{O}_Y := \bigcap_{\mathfrak{p}\in Y} \mathcal{O}_\mathfrak{p}$ and

$$E_Y := \{\lambda \in K^\times \mid \forall_{\mathfrak{p}\in Y} \operatorname{ord}_\mathfrak{p} \lambda \equiv 0 \pmod 2\}$$

This set is a union of cosets of $K^{\times 2}$ and we denote its image in the square-class group of K by $\mathbf{E}_Y := E_Y/K^{\times 2}$. Further, when Y is a proper subset, we consider the subset of E_Y consisting of all those functions that are local squares everywhere *outside* Y, namely

$$\varDelta_Y := E_Y \cap \bigcap_{\mathfrak{p}\notin Y} K_\mathfrak{p}^{\times 2} = E_X \cap \bigcap_{\mathfrak{p}\notin Y} K_\mathfrak{p}^{\times 2}.$$

This set again contains full square classes of K and so we write $\boldsymbol{\Delta}_Y := \varDelta_Y/K^{\times 2}$. In the special case when Y is of the form $X \setminus \{\mathfrak{p}\}$, we abbreviate the notation by writing $E_\mathfrak{p}$, $\mathbf{E}_\mathfrak{p}$, $\varDelta_\mathfrak{p}$ and $\boldsymbol{\Delta}_\mathfrak{p}$ for $E_{X\setminus\{\mathfrak{p}\}}$, $\mathbf{E}_{X\setminus\{\mathfrak{p}\}}$, $\varDelta_{X\setminus\{\mathfrak{p}\}}$ and $\boldsymbol{\Delta}_{X\setminus\{\mathfrak{p}\}}$, respectively.

The square-class group $\mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$ has order 2. We write $\zeta \in \mathbb{F}_q \subset K$ for a fixed generator of this group, with the convention that $\zeta = -1$ whenever -1 is not a square in K (i.e. $\operatorname{card}(\mathbb{F}_q) \equiv 3 \pmod 4$). Abusing notation slightly, we tend to use the same symbols $\lambda, \mu, \ldots$ to denote elements of the field and their classes in the square-class group of this field. Likewise, the fraktur letters $\mathfrak{p}, \mathfrak{q}, \ldots$ denote, depending on the context, either points of K or their classes in $\operatorname{Pic} X$ or $\operatorname{Pic} \mathcal{O}_Y$. Divisors, as well as their classes in the Picard group, are always written additively.

2. Preliminaries. Recall that if $K_\mathfrak{p}$ is a local field, then the square-class group of $K_\mathfrak{p}$ consists of four elements: $1, u_\mathfrak{p}, \pi_\mathfrak{p}$ and $u_\mathfrak{p}\pi_\mathfrak{p}$, where $\pi_\mathfrak{p}$ is the class of a uniformizer and $u_\mathfrak{p}$ is the class of a unit which is not a square (see e.g. [Lam05, Theorem VI.2.2]). We call $u_\mathfrak{p}$ the $\mathfrak{p}$-*primary unit.* If (T, t) is a self-equivalence of K, then t factors over all the local square-class groups by [PSCL94, Lemma 4]. In particular, it maps $1 \in K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$ to $1 \in K_{T\mathfrak{p}}^\times/K_{T\mathfrak{p}}^{\times 2}$. If it also maps $u_\mathfrak{p}$ to $u_{T\mathfrak{p}}$, then it is necessarily tame by the pigeonhole principle. Thus we have proved:

Observation 2.1. *A self-equivalence (T, t) is wild at a point $\mathfrak{p} \in X$ if and only if* $\operatorname{ord}_{T\mathfrak{p}} tu_\mathfrak{p} \equiv 1 \pmod 2$.

The primary unit $u_\mathfrak{p}$ may also be characterized by using Hilbert symbols as follows:

$$(u_\mathfrak{p}, \lambda)_\mathfrak{p} = (-1)^{\operatorname{ord}_\mathfrak{p} \lambda} \quad \text{for every } \lambda \in K_\mathfrak{p}^\times.$$

The Hilbert symbol $(\cdot, \cdot)_\mathfrak{p}$ can be viewed as a non-degenerate $\mathbb{F}_2$-inner product on $K_\mathfrak{p}^\times/K_\mathfrak{p}^{\times 2}$, provided the additive group $\mathbb{F}_2$ is identified with the multiplicative group $\{\pm 1\}$. The following observation is now immediate:

Observation 2.2. *Let* $\mathfrak{p}, \mathfrak{q} \in X$ *be two points of* K *such that* $-1 \in K_{\mathfrak{p}}^2 \cap K_{\mathfrak{q}}^2$. *Then the isomorphism* $\tau : K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2} \to K_{\mathfrak{q}}^{\times}/K_{\mathfrak{q}}^{\times 2}$ *defined by*

$$\tau(u_{\mathfrak{p}}) = u_{\mathfrak{q}}\pi_{\mathfrak{q}}, \qquad \tau(\pi_{\mathfrak{p}}) = \pi_{\mathfrak{q}}$$

is an isometry of the inner product spaces

$$(K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2}, (\cdot,\cdot)_{\mathfrak{p}}) \quad \textit{and} \quad (K_{\mathfrak{q}}^{\times}/K_{\mathfrak{q}}^{\times 2}, (\cdot,\cdot)_{\mathfrak{q}}).$$

Below we gather some results concerning 2-ranks of the class groups: either the Picard group $\operatorname{Pic} X$ of a complete curve X or the Picard group $\operatorname{Pic} \mathcal{O}_Y$ for some fixed open subset $\emptyset \neq Y \subsetneq X$. Recall that the latter group can be identified with the ideal class group $\operatorname{Cl} \mathcal{O}_Y$ of the coordinate ring $\mathcal{O}_Y$ of Y, as $\mathcal{O}_Y$ is a Dedekind domain.

We begin with a proposition that is not new: the first assertion was proved in [Czo01, p. 607] and the second in [Czo01, Lemma 2.1]. The third assertion is a simple consequence of the previous two. We state the result explicitly only for ease of reference.

Proposition 2.3. *Let* $\emptyset \neq Y \subsetneq X$ *be a proper open subset of* X. *Then*

(1) $\operatorname{rk}_2 \mathbf{E}_Y = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Y + \operatorname{card}(X \setminus Y)$;
(2) $\operatorname{rk}_2 \mathbf{\Delta}_Y = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Y$;
(3) $\operatorname{rk}_2(\mathbf{E}_Y/\mathbf{\Delta}_Y) = \operatorname{card}(X \setminus Y)$;

An identity similar to (1) above can also be proved for a complete curve.

Lemma 2.4. $\operatorname{rk}_2 \mathbf{E}_X = 1 + \operatorname{rk}_2 \operatorname{Pic}^0 X$.

Proof. Let H be the subgroup of $\operatorname{Pic}^0 X$ consisting of elements of order 2. The map

$$E_X \to H, \qquad \lambda \mapsto \tfrac{1}{2} \operatorname{div}_K \lambda = \sum_{\mathfrak{p} \in X} \tfrac{1}{2} \operatorname{ord}_{\mathfrak{p}} \lambda \cdot \mathfrak{p},$$

is a surjective homomorphism with kernel $\mathbb{F}_q^{\times} \cdot K^{\times 2}$. Thus, $\operatorname{rk}_2(E_X/\mathbb{F}_q^{\times} K^{\times 2}) = \operatorname{rk}_2 \operatorname{Pic}^0 X$. The groups $\mathbb{F}_q^{\times} K^{\times 2}/K^{\times 2}$ and $\mathbb{F}_q^{\times}/\mathbb{F}_q^{\times 2}$ are isomorphic and the 2-rank of $\mathbb{F}_q^{\times}/\mathbb{F}_q^{\times 2}$ equals 1. This proves the lemma. ∎

Now, we consider the case when we have two open subsets $Z \subset Y \subset X$.

Lemma 2.5. *If* $\emptyset \neq Z \subset Y \subsetneq X$ *are two proper open subsets of* X, *then*

(1) $\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Z = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Y - \operatorname{rk}_2\langle\{\mathfrak{p} + 2 \operatorname{Pic} \mathcal{O}_Y \mid \mathfrak{p} \in Y \setminus Z\}\rangle$;
(2) $\operatorname{rk}_2 \mathbf{E}_Z = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Y - \operatorname{rk}_2\langle\{\mathfrak{p} + 2 \operatorname{Pic} \mathcal{O}_Y \mid \mathfrak{p} \in Y \setminus Z\}\rangle + \operatorname{card}(X \setminus Z)$.

Proof. Since $Z \subset Y$, we have $\mathcal{O}_Z \supset \mathcal{O}_Y$, and by functoriality there is a natural morphism $\operatorname{Pic} \mathcal{O}_Y \to \operatorname{Pic} \mathcal{O}_Z$. It is clearly an epimorphism, since the class of a divisor $\sum_{\mathfrak{p} \in Z} n_{\mathfrak{p}} \mathfrak{p}$ is the image of the class of any divisor of the form $\sum_{\mathfrak{p} \in Z} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\mathfrak{q} \in Y \setminus Z} n_{\mathfrak{q}} \mathfrak{q}$. This epimorphism induces an epimorphism of the quotient groups $\operatorname{Pic} \mathcal{O}_Y/2 \operatorname{Pic} \mathcal{O}_Y \twoheadrightarrow \operatorname{Pic} \mathcal{O}_Z/2 \operatorname{Pic} \mathcal{O}_Z$, whose kernel is generated by the set $\{\mathfrak{p} + 2 \operatorname{Pic} \mathcal{O}_Y \mid \mathfrak{p} \in Y \setminus Z\}$. This proves the first assertion of the lemma; the second follows immediately from the first one and Proposition 2.3. ■

It is natural to compare the 2-rank of $\operatorname{Pic}^0 X$ with the 2-rank of the class group $\operatorname{Pic} \mathcal{O}_Y$ of a proper open subset $Y \subsetneq X$. Below we formulate two relevant results for the case $Y = X \setminus \{\mathfrak{p}\}$.

LEMMA 2.6. *Let $\zeta \in \mathbb{F}_q$ be a fixed generator of the square-class group $\mathbb{F}_q^\times/\mathbb{F}_q^{\times 2}$ of the full field of constants of K. If $\mathfrak{p} \in X$ is a point of odd degree, then*

(1) $\mathbf{E}_X = \mathbf{E}_\mathfrak{p} = \langle\zeta\rangle \oplus \mathbf{\Delta}_\mathfrak{p}$;
(2) $\operatorname{rk}_2 \operatorname{Pic}^0 X = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_\mathfrak{p}$.

Proof. Let $\lambda \in E_\mathfrak{p}$. Since the degree of the principal divisor $\operatorname{div}_K \lambda$ is 0, we have

$$\operatorname{ord}_\mathfrak{p} \lambda \cdot \deg \mathfrak{p} = -\sum_{\mathfrak{q} \neq \mathfrak{p}} \operatorname{ord}_\mathfrak{q} \lambda \cdot \deg \mathfrak{q}.$$

Now, $\operatorname{ord}_\mathfrak{q} \lambda$ is even for every $\mathfrak{q} \neq \mathfrak{p}$, since $\lambda \in E_\mathfrak{p}$. On the other hand, $\deg \mathfrak{p}$ is odd by assumption. It follows that $\operatorname{ord}_\mathfrak{p} \lambda$ is even, too. Hence $\lambda \in E_X$ and so we have proved that $\mathbf{E}_\mathfrak{p} \subseteq \mathbf{E}_X$. The other inclusion is trivial and the equality $\mathbf{E}_\mathfrak{p} = \langle\zeta\rangle \oplus \mathbf{\Delta}_\mathfrak{p}$ follows from Proposition 2.3 and the fact that ζ is not a local square at a given point if and only if this point has an odd degree. This proves (1); and (2) follows immediately from Lemma 2.4 and Proposition 2.3(1). ■

PROPOSITION 2.7. *If $\mathfrak{p} \in X$ is any point, then*

$$\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_\mathfrak{p} = \begin{cases} \operatorname{rk}_2 \operatorname{Pic}^0 X & \text{if } \mathfrak{p} \notin 2 \operatorname{Pic} X, \\ 1 + \operatorname{rk}_2 \operatorname{Pic}^0 X & \text{if } \mathfrak{p} \in 2 \operatorname{Pic} X. \end{cases}$$

The proof is postponed to the next section.

3. 2-divisibility of classes of prime divisors. This section is devoted to the following problem: If $\mathfrak{p} \in X$ is a point, when is the class of $\mathfrak{p}$ in $\operatorname{Pic} X$ divisible by 2 (i.e. lying in $2 \operatorname{Pic} X$)? Points having this property will be called 2-*divisible* or briefly, albeit less formally, *even*. The results of this section not only have direct applications in the rest of this paper, but (at least some of them) are of independent interest. Let us begin with the following basic observation.

OBSERVATION 3.1. *If $\mathfrak{p} \in X$ is an even point, then $\deg \mathfrak{p}$ is an even integer.*

This follows immediately from the fact (see e.g. [Lor96, Corollary VII.7.10]) that the epimorphism $\deg : \operatorname{Div} K \twoheadrightarrow \mathbb{Z}$ factors through the subgroup of principal divisors, inducing a well defined group epimorphism $\deg : \operatorname{Pic} X \twoheadrightarrow \mathbb{Z}$.

It is well known (see e.g. [Lor96, Proposition VII.7.12]) that for a field of rational functions this map is actually an isomorphism. Hence, in such a field, even points are precisely the points of even degrees. Of course, this is not so in general. For example, if K is the function field of an elliptic curve over $\mathbb{F}_3$ given in Weierstrass normal form by the polynomial $y^2 - x^3 + x$, then there are exactly six points of degree 2 and twelve points of degree 4 in K but none (!) of them is 2-divisible in $\operatorname{Pic} X$ (verified ([1]) using Magma [BCP97]). Thus, we have to search for some other criteria of 2-divisibility.

PROPOSITION 3.2. *A point $\mathfrak{p} \in X$ is 2-divisible in* $\operatorname{Pic} X$ *if and only if there exists an element $\lambda \in E_{\mathfrak{p}}$ such that* $\operatorname{ord}_{\mathfrak{p}} \lambda \equiv 1 \pmod 2$.

Proof. Assume that $\mathfrak{p}$ is an even point; this means that

$$\mathfrak{p} + \operatorname{div}_K \lambda = \sum_{\mathfrak{q} \in X} 2n_{\mathfrak{q}} \cdot \mathfrak{q}$$

for some $n_{\mathfrak{q}} \in \mathbb{Z}$ almost all zero and some $\lambda \in K$. It is clear that λ satisfies the assertion.

Conversely, assume the existence of $\lambda \in E_{\mathfrak{p}}$ of odd order at $\mathfrak{p}$, say $\operatorname{ord}_{\mathfrak{p}} \lambda = 2k + 1$. Write the divisor of λ as

$$\operatorname{div}_K \lambda = (2k+1)\mathfrak{p} + \sum_{\substack{\mathfrak{q} \in X \\ \mathfrak{q} \neq \mathfrak{p}}} 2n_{\mathfrak{q}}\mathfrak{q}$$

for some $k \in \mathbb{Z}$ and $n_{\mathfrak{q}} \in \mathbb{Z}$ almost all zero. Therefore, in the Picard group of K,

$$\mathfrak{p} = \operatorname{div}_K \lambda - 2\Big(k\mathfrak{p} + \sum_{\substack{\mathfrak{q} \in X \\ \mathfrak{q} \neq \mathfrak{p}}} n_{\mathfrak{q}}\mathfrak{q}\Big).$$

In particular $\mathfrak{p} \in 2 \operatorname{Pic} X$, as claimed. ∎

We will need the following, rather basic, fact from group theory, which we believe is well known to experts but we are not aware of any convenient reference.

LEMMA 3.3. *Let G be a finite abelian group. If H is a subgroup of G, then*

$$\operatorname{rk}_2 G/H \geq \operatorname{rk}_2 G - \operatorname{rk}_2 H.$$

Proof. The 2-rank of a finite abelian group A is just the dimension of the $\mathbb{F}_2$-vector space $A \otimes_{\mathbb{Z}} \mathbb{F}_2$. Take a short exact sequence

$$0 \to H \to G \to G/H \to 0$$

([1]) The source codes for Magma of all the counterexamples are available at the second author's web page http://z2.math.us.edu.pl/perry/papers.

and tensor it with $\mathbb{F}_2$. We obtain the exact sequence of $\mathbb{F}_2$-vector spaces

$$H \otimes_{\mathbb{Z}} \mathbb{F}_2 \to G \otimes_{\mathbb{Z}} \mathbb{F}_2 \to G/H \otimes_{\mathbb{Z}} \mathbb{F}_2 \to 0.$$

Let I be the image of the first homomorphism in the above sequence. Clearly $\dim_{\mathbb{F}_2}(H \otimes_{\mathbb{Z}} \mathbb{F}_2) \geq \dim_{\mathbb{F}_2} I$ and we have

$$\begin{aligned}\dim_{\mathbb{F}_2}(G \otimes_{\mathbb{Z}} \mathbb{F}_2) - \dim_{\mathbb{F}_2}(H \otimes_{\mathbb{Z}} \mathbb{F}_2) &\leq \dim_{\mathbb{F}_2}(G \otimes_{\mathbb{Z}} \mathbb{F}_2) - \dim_{\mathbb{F}_2} I \\ &= \dim_{\mathbb{F}_2}((G/H) \otimes_{\mathbb{Z}} \mathbb{F}_2). \quad \blacksquare\end{aligned}$$

Proof of Proposition 2.7. Let $d := \deg \mathfrak{p}$. It follows from [Ros02, Proposition 14.1] that the following sequence is exact:

$$0 \to \operatorname{Pic}^0 X \to \operatorname{Pic} \mathcal{O}_{\mathfrak{p}} \to \mathbb{Z}_d \to 0.$$

Therefore $\operatorname{Pic} \mathcal{O}_{\mathfrak{p}}/\operatorname{Pic}^0 X$ is isomorphic to $\mathbb{Z}_d$ and so their 2-ranks are equal. Lemma 3.3 asserts that

$$1 \geq \operatorname{rk}_2 \mathbb{Z}_d \geq \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{p}} - \operatorname{rk}_2 \operatorname{Pic}^0 X.$$

Consequently,

$$\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{p}} \leq 1 + \operatorname{rk}_2 \operatorname{Pic}^0 X. \tag{1}$$

Lemma 2.4 asserts that $\operatorname{rk}_2 \mathbf{E}_X = 1 + \operatorname{rk}_2 \operatorname{Pic}^0 X$, while Proposition 2.3 states that $\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{p}} = \operatorname{rk}_2 \mathbf{E}_{\mathfrak{p}} - 1$. Clearly $\mathbf{E}_X \subseteq \mathbf{E}_{\mathfrak{p}}$. If $\mathfrak{p} \notin 2 \operatorname{Pic} X$, then $\mathbf{E}_X = \mathbf{E}_{\mathfrak{p}}$ by Proposition 3.2, hence

$$\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{p}} = \operatorname{rk}_2 \operatorname{Pic}^0 X.$$

On the other hand, if $\mathfrak{p} \in 2 \operatorname{Pic} X$, then $\mathbf{E}_X \subsetneq \mathbf{E}_{\mathfrak{p}}$, again by Proposition 3.2. Thus

$$\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{p}} > \operatorname{rk}_2 \operatorname{Pic}^0 X,$$

and the assertion follows from (1). ∎

One immediate consequence of Proposition 2.7 is the following criterion for 2-divisibility.

PROPOSITION 3.4. *Let $\mathfrak{p} \in X$ be any point. Then $\mathfrak{p}$ is 2-divisible in* $\operatorname{Pic} X$ *if and only if every function having even order everywhere on X is a local square at $\mathfrak{p}$ (i.e. if $\mathbf{E}_X = \mathbf{\Delta}_{\mathfrak{p}}$).*

Proof. Think of $\mathbf{\Delta}_{\mathfrak{p}}$ as a subspace of the $\mathbb{F}_2$-linear space $\mathbf{E}_X$. Lemma 2.4 asserts that $\operatorname{rk}_2 \mathbf{E}_X = 1 + \operatorname{rk}_2 \operatorname{Pic}^0 X$, while $\operatorname{rk}_2 \mathbf{\Delta}_{\mathfrak{p}} = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{p}}$ by Proposition 2.3. Now, it follows from Proposition 2.7 that $\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{p}} = 1 + \operatorname{rk}_2 \operatorname{Pic}^0 X = \operatorname{rk}_2 \mathbf{E}_X$ if and only if $\mathfrak{p} \in 2 \operatorname{Pic} X$. Consequently, $\dim_{\mathbb{F}_2} \mathbf{\Delta}_{\mathfrak{p}} = \dim_{\mathbb{F}_2} \mathbf{E}_X$, and so $\mathbf{\Delta}_{\mathfrak{p}}$ is the full space $\mathbf{E}_X$, if and only if $\mathfrak{p}$ is even. ∎

So far we have been considering 2-divisibility in the Picard group of the complete curve. The next proposition deals with 2-divisibility in $\operatorname{Pic} \mathcal{O}_Y$ (or equivalently in $\operatorname{Cl} \mathcal{O}_Y$), that is, over some proper open subset Y of X.

Proposition 3.5. *Let $\emptyset \neq Y \subsetneq X$ be a proper open subset and $\mathfrak{p} \in Y$. Then $\mathfrak{p}$ is 2-divisible in $\operatorname{Pic}\mathcal{O}_Y$ if and only if $\mathit{\Delta}_Y \subset K_{\mathfrak{p}}^{\times 2}$.*

Proof. By assumption there exists $\lambda \in K^\times$ such that $\operatorname{div}_{\mathcal{O}_Y}\lambda = \mathfrak{p} + 2\mathfrak{D}$ for some $\mathcal{O}_Y$-divisor $\mathfrak{D} \in \operatorname{Div}\mathcal{O}_Y$. Fix $\mu \in \mathit{\Delta}_Y$. Then, for every $\mathfrak{q} \in X\setminus Y$, the element μ is a local square at $\mathfrak{q}$, hence the quaternion algebra $\left(\frac{\lambda,\mu}{K_{\mathfrak{q}}}\right)$ splits. On the other hand, if $\mathfrak{q} \in Y\setminus\{\mathfrak{p}\}$, then both μ and λ are $\mathfrak{q}$-adic units modulo $K_{\mathfrak{q}}^{\times 2}$ and so again $\left(\frac{\lambda,\mu}{K_{\mathfrak{q}}}\right)$ splits. Consequently, the quaternion algebras $\left(\frac{\lambda,\mu}{K_{\mathfrak{q}}}\right)$ split for all $\mathfrak{q} \in X$, except possibly $\mathfrak{p}$. It follows from Hilbert's reciprocity formula that in that case also $\left(\frac{\lambda,\mu}{K_{\mathfrak{p}}}\right)$ splits. But μ is arbitrary, which implies that λ must be a local square at $\mathfrak{p}$.

Conversely, let $Z = Y \setminus \{\mathfrak{p}\}$. Since $\mu \in K_{\mathfrak{p}}^{\times 2}$ for every $\mu \in \mathit{\Delta}_Y$ by assumption, we have $\mathbf{\Delta}_Y = \mathbf{\Delta}_Z$ and it follows from Proposition 2.3(2) that

$$\operatorname{rk}_2\operatorname{Pic}\mathcal{O}_Y = \operatorname{rk}_2\operatorname{Pic}\mathcal{O}_Z.$$

Consequently, $\mathfrak{p} \in 2\operatorname{Pic}\mathcal{O}_Y$, by Lemma 2.5. ∎

Finally, we present a proposition connecting 2-divisibility in the Picard group of a complete curve with 2-divisibility over its open subset.

Proposition 3.6. *Let $\mathfrak{p}$, $\mathfrak{q}$ be points of X with $\deg\mathfrak{p}$ even and $\deg\mathfrak{q}$ odd. Then*

$$\mathfrak{p} \in 2\operatorname{Pic}X \iff \mathfrak{p} \in 2\operatorname{Pic}\mathcal{O}_{X\setminus\{\mathfrak{q}\}}.$$

Proof. Let $Y := X\setminus\{\mathfrak{q}\}$. If $\mathfrak{p}$ is 2-divisible in $\operatorname{Pic}X$, then $p = \operatorname{div}_K\lambda + 2\mathfrak{D}$ for some $\lambda \in K$ and $\mathfrak{D} \in \operatorname{Div}K$. Drop any occurrences of $\mathfrak{q}$ in $\mathfrak{D}$ and the principal divisor $\operatorname{div}_K\lambda$, to get $\mathcal{O}_Y$-divisors $\mathfrak{D}'$ and $\operatorname{div}_{\mathcal{O}_Y}\lambda$. Therefore, over $\mathcal{O}_Y$, we have

$$\mathfrak{p} = \operatorname{div}_{\mathcal{O}_Y}\lambda + 2\mathfrak{D}' \in \operatorname{Div}\mathcal{O}_Y,$$

and so $\mathfrak{p} \in 2\operatorname{Pic}\mathcal{O}_Y$.

Conversely, assume that $\mathfrak{p} \in 2\operatorname{Pic}\mathcal{O}_Y$; this means that there are $\lambda \in K$ and $\mathcal{O}_Y$-divisor $\mathfrak{D} \in \operatorname{Div}\mathcal{O}_Y$ such that

$$\operatorname{div}_{\mathcal{O}_Y}\lambda = \mathfrak{p} + 2\mathfrak{D} \in \operatorname{Div}\mathcal{O}_Y.$$

Passing from Y to the complete curve X, write

$$\operatorname{div}_K\lambda = \mathfrak{p} + 2\mathfrak{D} + \operatorname{ord}_{\mathfrak{q}}\lambda\cdot\mathfrak{q}.$$

Compute the degrees of both sides to get

$$0 = \deg\mathfrak{p} + 2\deg\mathfrak{D} + \operatorname{ord}_{\mathfrak{q}}\lambda\cdot\deg\mathfrak{q}.$$

We have assumed that $\deg\mathfrak{q}$ is odd, while $\deg\mathfrak{p}$ is even, hence $\operatorname{ord}_{\mathfrak{q}}\lambda$ must be even too, say $\operatorname{ord}_{\mathfrak{q}}\lambda = 2k$ for some $k \in \mathbb{Z}$. Thus, $\operatorname{div}_K\lambda = \mathfrak{p} + 2(\mathfrak{D} + k\mathfrak{q})$, which means that $\mathfrak{p}$ is even, as desired. ∎

All the above results are of rather general nature and are valid for *any* global function field. It should not come as a big surprise that if we concentrate on function fields of a special type, more can be proved. Recall that a smooth curve X whose affine part X^{aff} is defined by a polynomial $y^2 - f(x)$ is called *hyperelliptic* when $\deg f \geq 4$, *elliptic* when $\deg f = 3$ and *conic* when $\deg f \leq 2$. In what follows, we will deal with elliptic and hyperelliptic curves in a uniform fashion, and we shall call all curves of this form "hyperelliptic", treating elliptic curves as a special case of hyperelliptic ones. We warn the reader, however, that this is not standard terminology.

Let K/F be an extension of function fields and $\pi : X \twoheadrightarrow Y$ be the corresponding morphism of their associated (smooth) curves. Recall (cf. [Lor96, Ch. VII, §7]) that a *norm* is a function $\operatorname{Norm}_{K/F} : \operatorname{Div} K \to \operatorname{Div} F$ given by

$$\operatorname{Norm}_{K/F}\Bigl(\sum_i a_i \mathfrak{p}_i\Bigr) := \sum_i a_i f(\mathfrak{p}_i/\pi(\mathfrak{p}_i))\pi(\mathfrak{p}_i), \tag{2}$$

where $f(\mathfrak{p}/\pi(\mathfrak{p}))$ is the inertia degree of $\mathfrak{p}$ over $\pi(\mathfrak{p})$. If Y^{aff} is the affine part of Y, $\mathcal{O}_F = \mathbb{F}_q[Y^{\mathrm{aff}}]$ is the ring of functions regular on Y^{aff} and $\mathcal{O}_K = \operatorname{int.cl}_K \mathcal{O}_F$ is the integral closure of $\mathcal{O}_F$ in K, then $\operatorname{Norm}_{K/F}|_{\operatorname{Div}\mathcal{O}_K}$ restricted to $\operatorname{Div}\mathcal{O}_K$ is a morphism $\operatorname{Div}\mathcal{O}_K \to \operatorname{Div}\mathcal{O}_F$. If additionally $F = \mathbb{F}_q(x)$ is a field of rational functions, then to every point $\mathfrak{p}$ of $Y = \mathbb{P}^1\mathbb{F}_q$ one may unambiguously assign either a monic polynomial $p \in \mathbb{F}_q[x]$ with a single zero at $\mathfrak{p}$ and no other zeros, or a function $1/x$ when $\mathfrak{p}$ is the point at infinity. This constitutes a morphism $\operatorname{Div} F \to F^\times$ from the group of divisors to the multiplicative group of the field F. Composing it over $\operatorname{Norm}_{K/F}$, we arrive at the map $\operatorname{norm}_{K/F} : \operatorname{Div} K \to F^\times$, which (harmlessly abusing notation) we shall again call a *norm*. In what follows, we shall prefer $\operatorname{norm}_{K/F}$ to $\operatorname{Norm}_{K/F}$ since the former allows us to compare the norm of a divisor with values of the standard norm of the field extension $\operatorname{norm}_{K/F} : K^\times \to F^\times$.

THEOREM 3.7. *Let K be a function field of a smooth hyperelliptic curve X of odd degree and $\mathfrak{p} \in X$ be a point of even degree. Then $\mathfrak{p}$ is 2-divisible in $\operatorname{Pic} X$ if and only if $\operatorname{norm}_{K/F}\mathfrak{p}$ is representable by $\operatorname{norm}_{K/F} : K^\times \to F^\times$, where F is a field of rational functions. In other words,*

$$\mathfrak{p} \in 2\operatorname{Pic} X \iff \exists_{\lambda\in K}\ \operatorname{norm}_{K/F}\mathfrak{p} = \operatorname{norm}_{K/F}\lambda.$$

The proof of this theorem will be divided into Lemmas 3.8–3.10, in which $K = \operatorname{qf}(\mathbb{F}_q[x,y]/(y^2 - f(x)))$ is always a function field of a hyperelliptic curve X with its affine part defined by the polynomial $y^2 - f(x)$; further $F = \mathbb{F}_q(x)$ is a field of rational functions in x and $\mathcal{O}_K = \operatorname{int.cl}\mathbb{F}_q[x]$. We denote by $\bar{\ } : K \to K$ the unique non-trivial F-automorphism of K. The ring $\mathcal{O}_K$ is a Dedekind domain, hence its Picard group can be identified with its ideal class group $\operatorname{Cl}\mathcal{O}_K$.

The first lemma is basically a recap of [BS66, Theorem III.8.7]. Unfortunately, in [BS66] it is proved only for number fields, hence for completeness we explicitly state and prove its function field counterpart.

LEMMA 3.8. *If the* $\operatorname{norm}_{K/F}\mathfrak{D}$ *of a divisor* $\mathfrak{D} \in \operatorname{Div}\mathcal{O}_K$ *equals* 1*, then the class of* $\mathfrak{D}$ *lies in* $2\operatorname{Pic}\mathcal{O}_K$*.*

Proof. We closely follow [BS66, proof of Theorem III.8.7]. Write the divisor $\mathfrak{D}$ in the form

$$\mathfrak{D} = \sum_{i=1}^{m}(a_i\mathfrak{p}_i + b_i\overline{\mathfrak{p}}_i) + \sum_{j=1}^{n} c_j\mathfrak{q}_j,$$

where the points $\mathfrak{q}_j = \overline{\mathfrak{q}}_j$ are fixed under the action of $\bar{}$ and the $\mathfrak{p}_i \neq \overline{\mathfrak{p}}_i$ are not. Then $\operatorname{norm}_{K/F}\mathfrak{p}_i = \operatorname{norm}_{K/F}\overline{\mathfrak{p}}_i = p_i$ and $\operatorname{norm}_{K/F}\mathfrak{q}_j = q_j^{f_j}$ for some monic polynomials $p_i, q_j \in \mathbb{F}_q[x]$, $f_j \in \{1,2\}$, $i \leq m$, $j \leq n$. Therefore

$$1 = \operatorname{norm}_{K/F}\mathfrak{D} = \prod_{i=1}^{m} p_i^{a_i+b_i} \cdot \prod_{j=1}^{n} q_j^{c_j}.$$

Now, all the polynomials are irreducible and pairwise distinct and $\mathbb{F}_q[x]$ is a UFD, hence all the exponents must vanish. In particular $c_j = 0$ for every j and $a_i = -b_i$ for every i. Consequently,

$$\mathfrak{D} = \sum_{i=1}^{m} a_i(\mathfrak{p}_i - \overline{\mathfrak{p}}_i),$$

but $\mathfrak{p}_i + \overline{\mathfrak{p}}_i = \operatorname{div}_{\mathcal{O}_K} p$, hence $\mathfrak{p}_i = -\overline{\mathfrak{p}}_i$ in $\operatorname{Pic}\mathcal{O}_K$. All in all, we write the class of $\mathfrak{D}$ as

$$\sum_{i=1}^{m} 2a_i\mathfrak{p}_i \in 2\operatorname{Pic}\mathcal{O}_K. \ ■$$

We are now in a position to prove the direct implication of Theorem 3.7.

LEMMA 3.9. *If* $\deg\mathfrak{p} \in 2\mathbb{Z}$ *and* $\operatorname{norm}_{K/F}\mathfrak{p} \in \operatorname{norm}_{K/F}K^\times$*, then* $\mathfrak{p}$ *is even.*

Proof. By the assumption of the theorem, the degree of X is odd, and it follows from [Lor96, Lemma V.10.15] that X has a unique point at infinity (denote it ∞_K) and this point is ramified. In particular, $\deg\infty_K = 1 \notin 2\mathbb{Z}$ and so $\mathfrak{p}$ and ∞_K are distinct. If the inertia degree of $\mathfrak{p}$ (in K/F) equals 2, then $\operatorname{norm}_{K/F}\mathfrak{p} = p^2$ for some monic $p \in \mathbb{F}_q[x]$. This means that $\operatorname{div}_K p = \mathfrak{p} - 2\infty_K$. Therefore $\mathfrak{p} = \operatorname{div}_K p + 2\infty_K \in 2\operatorname{Pic}X$.

From now on, we assume that $\mathfrak{p} \neq \infty_K$ and the inertia degree of $\mathfrak{p}$ equals 1. Hence, $\operatorname{norm}_{K/F}\mathfrak{p} = p$ and by assumption there exists $\lambda \in K$ such that $p = \operatorname{norm}_{K/F}\lambda = \lambda\overline{\lambda}$. Take a divisor $\mathfrak{D} := \mathfrak{p} - \operatorname{div}_{\mathcal{O}_K}\lambda \in \operatorname{Div}\mathcal{O}_K$.

Clearly

$$\operatorname{norm}_{K/F} \mathfrak{D} = \frac{\operatorname{norm}_{K/F} \mathfrak{p}}{\operatorname{norm}_{K/F} \lambda} = 1,$$

and so the previous lemma asserts that $\mathfrak{D} \in 2 \operatorname{Pic} \mathcal{O}_K$. Since ∞_K is the unique point at infinity and $\deg \infty_K = 1$, therefore [Lor96, Proposition VIII.9.2] implies that $\operatorname{Pic} \mathcal{O}_K$ is isomorphic to $\operatorname{Pic}^0 K$. Hence, passing with $\mathfrak{D}$ to $\operatorname{Pic} X$, we have $\mathfrak{p} - \operatorname{div}_K \lambda + 2k\infty_K \in 2 \operatorname{Pic} X$ for some $k \in \mathbb{Z}$. In particular $\mathfrak{p} \in 2 \operatorname{Pic} X$, as desired. ■

We now prove the opposite implication of Theorem 3.7.

LEMMA 3.10. *The norm* $\operatorname{norm}_{K/F} \mathfrak{p}$ *of every even point lies in* $\operatorname{norm}_{K/F} K^\times$.

Proof. Take $\mathfrak{p} \in X$ and assume that it is 2-divisible in $\operatorname{Pic} X$. Thus, there are $\mathfrak{D} \in \operatorname{Div} K$ and $\lambda \in K$ such that

$$\mathfrak{p} = 2\mathfrak{D} + \operatorname{div}_K \lambda.$$

Compute the norms of both sides to get

$$\operatorname{norm}_{K/F} \mathfrak{p} = \operatorname{norm}_{K/F}(2\mathfrak{D} + \operatorname{div}_K \lambda) = (\operatorname{norm}_{K/F} \mathfrak{D})^2 \cdot \operatorname{norm}_{K/F} \lambda.$$

If $\lambda = a + by$ for some $a, b \in F$, then $\operatorname{norm}_{K/F} \lambda = a^2 - b^2 f$, therefore

$$\operatorname{norm}_{K/F} \mathfrak{p} = (ac)^2 - (bc)^2 f,$$

where $c = \operatorname{norm}_{K/F} \mathfrak{D} \in F$. In particular $\operatorname{norm}_{K/F} \mathfrak{p} \in \operatorname{norm}_{K/F} K^\times$. ■

The proof of Theorem 3.7 is now complete.

REMARK 1. Note that the condition $\deg f \notin 2\mathbb{Z}$ occurs only in the proof of Lemma 3.9. Therefore, the implication

$$\mathfrak{p} \in 2 \operatorname{Pic} X \Rightarrow \operatorname{norm}_{K/F} \mathfrak{p} \in \operatorname{norm}_{K/F} K^\times$$

holds even without this assumption. Nevertheless, for the other implication this condition is indispensable. Indeed, take

$$K = \operatorname{qf}\bigl(\mathbb{F}_5[x, y]/(y^2 - x^4 + x + 1)\bigr).$$

Using Magma one checks that there are a total of eight points of K of degree 2 that are not 2-divisible in $\operatorname{Pic} X$, but their norms lie in $\operatorname{norm}_{K/F} K^\times$.

REMARK 2. The assumption that $\deg \mathfrak{p}$ is even is also essential. Take the field

$$K = \operatorname{qf}\bigl(\mathbb{F}_{13}[x, y]/(y^2 + 12x^3 + x^2 + 3x + 10)\bigr).$$

As mentioned in the proof of Lemma 3.9, the field K has the unique point at infinity ∞_K and $\deg \infty_K = 1$. On the other hand, $\operatorname{norm}_{K/F} \infty_K = 1/x \in \operatorname{norm}_{K/F} K^\times$. Again this example was checked using Magma.

The criterion in the above theorem lets us show that even points do exist.

Proposition 3.11. *Let K be a function field of a (smooth) hyperelliptic curve given by a polynomial $y^2 - f(x)$. If $f \in \mathbb{F}_q[x]$ is monic of odd degree, then there are infinitely many points of K that are 2-divisible in* $\operatorname{Pic} X$.

Proof. As observed in the proof of Lemma 3.9, K has unique point at infinity (denoted ∞_K). This point is ramified and the Picard group $\operatorname{Pic}\mathcal{O}_K$ of $\mathcal{O}_K = \operatorname{int.cl}_K \mathbb{F}_q[x]$ is isomorphic to $\operatorname{Pic}^0 X$. Let $f = f_1 \cdots f_n$ be the decomposition of f into irreducible monic factors. Fix a non-zero $M \in \mathbb{N}$ and take an irreducible polynomial $q_0 \in \mathbb{F}_q[x]$ of even degree strictly greater than M and prime to $\operatorname{char}\mathbb{F}_q$. Take an extension $\mathbb{F}_q(\alpha_0)$ of $\mathbb{F}_q$, where α_0 is a root of q_0. Clearly, $\mathbb{F}_q(\alpha_0) \neq \mathbb{F}_q$ since the degree of q_0 is even and greater than $M \neq 0$. Denote

$$\lambda_1 := f_1(\alpha_0), \quad \ldots, \quad \lambda_n := f_n(\alpha_0)$$

and consider the field $\mathbb{F}_q(\beta) := \mathbb{F}_q(\alpha_0, \sqrt{\lambda_1}, \ldots, \sqrt{\lambda_n})$. Further, let $p \in \mathbb{F}_q[x]$ be the minimal polynomial of β. Take $\mathfrak{p} \in X$ to be a point of K dominating p. Clearly the degree of $\mathfrak{p}$ is even and we have

$$\left(\frac{f_1}{p}\right) = \cdots = \left(\frac{f_n}{p}\right) = 1. \tag{3}$$

If the inertia degree of $\mathfrak{p}$ equals 2, then $\mathfrak{p} = \operatorname{div}_{\mathcal{O}_K} p$ in $\operatorname{Div}\mathcal{O}_K$, hence $\mathfrak{p} = 0$ in $\operatorname{Pic}\mathcal{O}_K \cong \operatorname{Pic}^0 X$. It follows that the class of $\mathfrak{p}$ in $\operatorname{Pic} X \cong \operatorname{Pic}^0 X \oplus \mathbb{Z}$ can be written as $(0, \deg\mathfrak{p})$, and so clearly belongs to $2\operatorname{Pic} X$. Thus, assume that the inertia degree $f(\mathfrak{p}/p)$ of $\mathfrak{p}$ is 1.

We claim that $\operatorname{norm}_{K/F}\mathfrak{p} \in \operatorname{norm}_{K/F} K$, in other words, $p = \operatorname{norm}_{K/F}\mathfrak{p}$ is represented over $F = \mathbb{F}_q(x)$ by the quadratic form $\langle 1, -f\rangle$. This is equivalent to saying that the form $\varphi := \langle 1, -f, -p\rangle$ is isotropic over $\mathbb{F}_q(x)$. By the local-global principle, it suffices to show that the form is locally isotropic in every completion of $\mathbb{F}_q(x)$.

First, take the completion at infinity, F_∞. By the assumption, $-\operatorname{ord}_\infty f = \deg f \notin 2\mathbb{Z}$, while $-\operatorname{ord}_\infty p = \deg p \in 2\mathbb{Z}$. Decompose the form $\varphi \otimes F_\infty$ into the sum $\langle 1, -p\rangle \otimes F_\infty \perp \langle -f\rangle \otimes F_\infty$, where the first summand has cooefficients of even order and the second of odd order. A well known consequence of Springer's theorem (see e.g. [Lam05, Proposition VI.1.9]) asserts that $\varphi \otimes F_\infty$ is isotropic if and only if the residue form of $\langle 1, -p\rangle$ is isotropic. But the latter is just $\langle 1, -1\rangle$, hence trivially isotropic, since p is monic.

Take now a completion F_s of F at the place associated to some irreducible polynomial s different from p and not dividing f. Using [Lam05, Proposition VI.1.9], we see that $\varphi \otimes F_s$ is again isotropic, because its residue form has dimension 3 (over a finite field) and therefore is isotropic.

Next, consider the completion F_p of F at the place associated to p. We know that all f_i's are squares modulo p, and so is f itself. Consequently, $\langle 1, -f\rangle \otimes F_p$ is isotropic, hence $\varphi \otimes F_p$ is isotropic, too. Finally, take the

f_i-adic completion F_{f_i} for some monic irreducible factor f_i of f. We have $\left(\frac{f_i}{p}\right) = 1$ by 3, and Dedekind's quadratic reciprocity law says that

$$\left(\frac{p}{f_i}\right) \cdot \left(\frac{f_i}{p}\right) = (-1)^{(\operatorname{card}(\mathbb{F}_q)-1)(\deg f_i \cdot \deg p)/2},$$

but $\deg p$ is even and it follows that $\left(\frac{p}{f_i}\right) = 1$. Thus, $\varphi \otimes F_{f_i}$ is again isotropic. All in all, φ is isotropic over F, which proves our claim. Theorem 3.7 asserts now that $\mathfrak{p}$ is even. It is immediate that taking $M := \deg p$ and repeating the above construction, we ultimately produce an infinite sequence of 2-divisible points in K. ∎

4. Main results. In this section, we prove our two main results: Theorem 4.7, showing that a point is even if and only if it is a unique wild point for some self-equivalence, and its partial generalization, Theorem 4.8. First, however, we need the following lemma, generalizing Proposition 3.5.

LEMMA 4.1. *Let $\emptyset \neq Y \subsetneq X$ be a proper open subset and $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in Y$. Then $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are linearly independent (over $\mathbb{F}_2$) in $\operatorname{Pic} \mathcal{O}_Y / 2 \operatorname{Pic} \mathcal{O}_Y$ if and only if there are $\lambda_1, \ldots, \lambda_n \in \Delta_Y$ linearly independent in $\mathbf{\Delta}_Y$ and such that for every $1 \leq i \leq n$,*

$$\lambda_i \notin K_{\mathfrak{p}_i}^2 \quad \textit{and} \quad \lambda_i \in \bigcap_{j \neq i} K_{\mathfrak{p}_j}^2.$$

Proof. We proceed by induction on n. For $n = 1$ the assertion follows from Proposition 3.5. Suppose that $n > 1$ and the assertion holds true for $n-1$. Classes of $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are linearly independent in $\operatorname{Pic} \mathcal{O}_Y / 2 \operatorname{Pic} \mathcal{O}_Y$, and so in particular $\mathfrak{p}_1$ is not 2-divisible in $\operatorname{Pic} \mathcal{O}_Y$. Proposition 3.5 asserts that there exists $\mu \in \Delta_Y$ such that $\mu \notin K_{\mathfrak{p}_1}^2$. Take a subset $Z := Y \setminus \{\mathfrak{p}_1\}$ of Y. By Lemma 2.5, we have $\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Z = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Y - 1$. Clearly, $\mathbf{\Delta}_Z \subset \mathbf{\Delta}_Y$ with $\mu \in \mathbf{\Delta}_Y \setminus \mathbf{\Delta}_Z$. Moreover, $\mathfrak{p}_2, \ldots, \mathfrak{p}_n$ remain linearly independent in $\operatorname{Pic} \mathcal{O}_Z / 2 \operatorname{Pic} \mathcal{O}_Z$.

It follows from the inductive hypothesis that there are $\lambda_2, \ldots, \lambda_n \in \Delta_Z$ linearly independent in $\mathbf{\Delta}_Z$ and such that for every $2 \leq i \leq n$,

$$\lambda_i \notin K_{\mathfrak{p}_i}^2 \quad \text{and} \quad \lambda_i \in \bigcap_{\substack{j \neq i \\ j \geq 2}} K_{\mathfrak{p}_j}^2.$$

By the very definition of Δ_Z, all λ_i's for $i \geq 2$ lie in $K_{\mathfrak{p}_1}^2$. Let

$$\lambda_1 := \mu \cdot \prod_{i>1} \lambda_i^{\varepsilon_i}, \quad \text{where} \quad \varepsilon_i = \begin{cases} 0 & \text{if } \mu \in K_{\mathfrak{p}_i}^2, \\ 1 & \text{if } \mu \notin K_{\mathfrak{p}_i}^2. \end{cases}$$

It is now immediate that $\lambda_1 \in \bigcap_{j \neq 1} K_{\mathfrak{p}_j}^2$ while $\lambda_1 \notin K_{\mathfrak{p}_1}^2$. This proves one implication. The other one follows from [Czo01, Lemma 2.1]. ∎

LEMMA 4.2. *Let $\mathfrak{p} \in 2\operatorname{Pic} X$ be an even point. Then for any other even point $\mathfrak{q} \in 2\operatorname{Pic} X$, the set $\mathbf{E}_{\mathfrak{p}} \setminus \mathbf{E}_X$ is contained in a square class of the completion $K_{\mathfrak{q}}$.*

Proof. Since $\mathbf{\Delta}_{\mathfrak{p}} = \mathbf{E}_X$ by Proposition 3.4, $\mathbf{E}_X$ is a subgroup of $\mathbf{E}_{\mathfrak{p}}$ of index $(\mathbf{E}_{\mathfrak{p}} : \mathbf{E}_X) = 2$ by Proposition 2.3. Take any $\lambda, \mu \in \mathbf{E}_{\mathfrak{p}} \setminus \mathbf{E}_X$; then $\lambda \cdot \mathbf{E}_X = \mu \cdot \mathbf{E}_X$ and so $\lambda \cdot \mu \in \mathbf{E}_X = \mathbf{\Delta}_{\mathfrak{q}} \subset K_{\mathfrak{q}}^{\times 2}$. ■

We define a relation on the set of 2-divisible points: $\mathfrak{p} \in 2\operatorname{Pic} X$ is related to $\mathfrak{q} \in 2\operatorname{Pic} X$, written $\mathfrak{p} \smile \mathfrak{q}$, when $\mathbf{E}_{\mathfrak{p}} \setminus \mathbf{E}_X \subset K_{\mathfrak{q}}^{\times 2}$. Unfortunately this relation—although symmetric—is neither reflexive nor transitive (see Remark 3 below).

LEMMA 4.3. *The relation $\smile$ is symmetric.*

Proof. Take $\lambda \in \mathbf{E}_{\mathfrak{p}} \setminus \mathbf{E}_X$ and $\mu \in \mathbf{E}_{\mathfrak{q}} \setminus \mathbf{E}_X$. Assume that $\mathfrak{p} \smile \mathfrak{q}$, so that $\lambda \in K_{\mathfrak{q}}^{\times 2}$. Take any point $\mathfrak{r}$ distinct from both $\mathfrak{p}$ and $\mathfrak{q}$; then a local quaternion algebra $\left(\frac{\lambda,\mu}{K_{\mathfrak{r}}}\right)$ splits, since $\operatorname{ord}_{\mathfrak{r}} \lambda \equiv \operatorname{ord}_{\mathfrak{r}} \mu \equiv 0 \pmod 2$. Next, also $\left(\frac{\lambda,\mu}{K_{\mathfrak{q}}}\right)$ splits, because λ is a square in $K_{\mathfrak{q}}$. It follows from Hilbert's reciprocity law that $\left(\frac{\lambda,\mu}{K_{\mathfrak{p}}}\right)$ splits as well. But $\operatorname{ord}_{\mathfrak{p}} \lambda \equiv 1 \pmod 2$, hence μ must be a local square at $\mathfrak{p}$. Consequently, $\mathbf{E}_{\mathfrak{q}} \setminus \mathbf{E}_X$ is contained in $K_{\mathfrak{p}}^{\times 2}$ and so $\mathfrak{q}$ is related to $\mathfrak{p}$. ■

REMARK 3. While it is obvious (and harmless) that $\smile$ is not reflexive, it is less obvious that in general it is not transitive. Take the function field of an elliptic curve X over $\mathbb{F}_3$ given by the equation $y^2 = x^3 + x - 1$. Consider the points $\mathfrak{p}, \mathfrak{q}, \mathfrak{r} \in X$, where $\mathfrak{p}$ is the common zero of x and $x^3 + x$; $\mathfrak{q}$ is the common zero of $x^4 + x^2 + 2x + 1$ and $y + x^2 + 2x$; and $\mathfrak{r}$ is the common zero of $x^4 + x^2 + 2x + 1$ and $y + 2x^2 + x$. Then, using Magma one can check that $\mathfrak{p} \smile \mathfrak{q}$ and $\mathfrak{p} \smile \mathfrak{r}$, but $\mathfrak{q}$ and $\mathfrak{r}$ are not related.

Let us now recall the notion of *small equivalence*. Let $\emptyset \neq \mathcal{S} \subset X$ be a finite (hence closed) subset of X. We say that $\mathcal{S}$ is *sufficiently large* if $\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{X\setminus\mathcal{S}} = 0$. If $\mathcal{S} \subset X$ is a sufficiently large set of points of K, then a triple $(T_{\mathcal{S}}, t_{\mathcal{S}}, (t_{\mathfrak{p}} \mid \mathfrak{p} \in \mathcal{S}))$ is called (cf. [PSCL94, §6]) a *small $\mathcal{S}$-equivalence* of the field K if

(SE1) $T_{\mathcal{S}} : \mathcal{S} \to X$ is injective,

(SE2) $t_{\mathcal{S}} : \mathbf{E}_{X\setminus\mathcal{S}} \to \mathbf{E}_{X\setminus T_{\mathcal{S}}\mathcal{S}}$ is a group isomorphism,

(SE3) for every $\mathfrak{p} \in \mathcal{S}$ the map $t_{\mathfrak{p}} : K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2} \to K_{T_{\mathcal{S}}\mathfrak{p}}^{\times}/K_{T_{\mathcal{S}}\mathfrak{p}}^{\times 2}$ is an isomorphism of local square-class groups preserving Hilbert symbols, in the sense that

$$(x, y)_{\mathfrak{p}} = (t_{\mathfrak{p}} x, t_{\mathfrak{p}} y)_{T_{\mathcal{S}}\mathfrak{p}} \quad \text{for all } x, y \in K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2};$$

(SE4) the following diagram commutes:

$$\begin{array}{ccc} \mathbf{E}_{X\setminus\mathcal{S}} & \xrightarrow{i_{\mathcal{S}}} & \prod_{\mathfrak{p}\in\mathcal{S}} K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2} \\ \Big\downarrow t_{\mathcal{S}} & & \Big\downarrow \prod_{\mathfrak{p}\in\mathcal{S}} t_{\mathfrak{p}} \\ \mathbf{E}_{X\setminus T_{\mathcal{S}}\mathcal{S}} & \xrightarrow{i_{T_{\mathcal{S}}\mathcal{S}}} & \prod_{\mathfrak{p}\in\mathcal{S}} K_{T_{\mathcal{S}}\mathfrak{p}}^{\times}/K_{T_{\mathcal{S}}\mathfrak{p}}^{\times 2} \end{array} \tag{4}$$

where the maps $i_{\mathcal{S}} = \prod_{\mathfrak{p}\in\mathcal{S}} i_{\mathfrak{p}}$ and $i_{T_{\mathcal{S}}\mathcal{S}} = \prod_{\mathfrak{q}\in T_{\mathcal{S}}\mathcal{S}} i_{\mathfrak{q}}$ are the diagonal homomorphisms with

$$i_{\mathfrak{p}} : \mathbf{E}_{X\setminus\mathcal{S}} \to K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2}, \qquad i_{\mathfrak{q}} : \mathbf{E}_{X\setminus T_{\mathcal{S}}\mathcal{S}} \to K_{\mathfrak{q}}^{\times}/K_{\mathfrak{q}}^{\times 2}.$$

We say that the local isomorphism $t_{\mathfrak{p}} : K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2} \to K_{T_{\mathcal{S}}\mathfrak{p}}^{\times}/K_{T_{\mathcal{S}}\mathfrak{p}}^{\times 2}$ is *tame* when

$$\operatorname{ord}_{\mathfrak{p}} \lambda \equiv \operatorname{ord}_{T_{\mathcal{S}}\mathfrak{p}} t_{\mathfrak{p}}\lambda \pmod 2 \quad \text{for every } \lambda \in K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2}.$$

The next result follows from [PSCL94, Theorem 2 and Lemma 4]:

THEOREM 4.4. *Every small $\mathcal{S}$-equivalence $(T_{\mathcal{S}}, t_{\mathcal{S}}, (t_{\mathfrak{p}} \mid \mathfrak{p} \in \mathcal{S}))$ of the field K can be extended to a self-equivalence (T, t) of K tame on $X \setminus \mathcal{S}$. Moreover, the self-equivalence (T, t) is tame at $\mathfrak{p} \in \mathcal{S}$ if and only if the local isomorphism $t_{\mathfrak{p}}$ is tame.*

REMARK 4. In the case considered in this paper (that is, over global function fields) any local square-class group $K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2}$ consists of just four elements $\{1, u_{\mathfrak{p}}, \pi_{\mathfrak{p}}, u_{\mathfrak{p}}\pi_{\mathfrak{p}}\}$, with $\operatorname{ord}_{\mathfrak{p}} u_{\mathfrak{p}} \equiv 0 \pmod 2$ and $\operatorname{ord}_{\mathfrak{p}} \pi_{\mathfrak{p}} \equiv 1 \pmod 2$. For two square classes $\lambda, \mu \in K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2}$, $\lambda, \mu \neq 1$, the Hilbert symbol can be computed with the formula

$$(\lambda, \mu)_{\mathfrak{p}} = 1 \iff \lambda = \mu.$$

Therefore, *every* bijection of the local square-class groups mapping squares to squares is an isomorphism and preserves the Hilbert symbols. Consequently, the condition (SE3) is always satisfied for this type of fields.

PROPOSITION 4.5. *Let K be a global function field and X an associated smooth curve. Let $\mathfrak{p}, \mathfrak{p}_1, \dots, \mathfrak{p}_l$ be 2-divisible points such that $\mathfrak{p}_i \smile \mathfrak{p}_j$ for every $i \neq j$. Then there is a self-equivalence (T, t) of K such that:*

- *$\mathfrak{p}$ is the unique wild point of (T, t), i.e. $\mathcal{W}(T, t) = \{\mathfrak{p}\}$;*
- *T preserves the selected points in the sense that*

$$T\mathfrak{p} = \mathfrak{p} \quad \text{and} \quad T\mathfrak{p}_i = \mathfrak{p}_i \text{ for } i = 1, \dots, l;$$

- *for every $\mathfrak{p}_i \smile \mathfrak{p}$, the isomorphism t restricted to the local square-class group $K_{\mathfrak{p}_i}^{\times}/K_{\mathfrak{p}_i}^{\times 2}$ is the identity;*
- *for every $\mathfrak{p}_i \not\smile \mathfrak{p}$, the isomorphism t restricted to the local square-class group $K_{\mathfrak{p}_i}^{\times}/K_{\mathfrak{p}_i}^{\times 2}$ is a transposition of the square classes of odd orders.*

Proof. Take an open subset $Y := X \setminus \{\mathfrak{p}, \mathfrak{p}_1, \dots, \mathfrak{p}_l\}$ of X and let $m := \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Y$. Observe that

$$\begin{aligned}\operatorname{rk}_2 \mathbf{\Delta}_Y &= \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Y = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_\mathfrak{p} - \operatorname{rk}_2 \langle \mathfrak{p}_1 + 2 \operatorname{Pic} \mathcal{O}_\mathfrak{p}, \dots, \mathfrak{p}_l + 2 \operatorname{Pic} \mathcal{O}_\mathfrak{p} \rangle \\ &= \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_\mathfrak{p} = \operatorname{rk}_2 \mathbf{\Delta}_\mathfrak{p},\end{aligned}$$

where the first and the last equalities follow from Proposition 2.3, the second follows from Lemma 2.5, while the third one is due to the fact that every $\mathfrak{p}_i$ is 2-divisible in $\operatorname{Pic} X$, and consequently also in $\operatorname{Pic} \mathcal{O}_\mathfrak{p}$. Therefore, the $\mathbb{F}_2$-linear spaces $\mathbf{\Delta}_\mathfrak{p}$ and $\mathbf{\Delta}_Y$ are equal, but the former is just $\mathbf{E}_X$ by Proposition 3.4. All in all, $\mathbf{\Delta}_Y = \mathbf{E}_X$.

Take a basis $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ of $\operatorname{Pic} \mathcal{O}_Y / 2 \operatorname{Pic} \mathcal{O}_Y$. Lemma 4.1 asserts that there are elements $\mu_1, \dots, \mu_m \in \Delta_Y$ linearly independent in $\mathbf{\Delta}_Y$ and such that $\mu_i \in K_{\mathfrak{q}_j}^{\times 2}$ if and only if $i \neq j$. Clearly, they form a basis of $\mathbf{\Delta}_Y = \mathbf{E}_X$. Now, $\operatorname{rk}_2(\mathbf{E}_\mathfrak{p}/\mathbf{E}_X) = 1$ by Propositions 3.4 and 2.3. Likewise, $\operatorname{rk}_2(\mathbf{E}_{\mathfrak{p}_i}/\mathbf{E}_X) = 1$ for every $i = 1, \dots, l$. Therefore, there are square-classes

$$\lambda \in \mathbf{E}_\mathfrak{p} \setminus \mathbf{E}_X, \quad \lambda_1 \in \mathbf{E}_{\mathfrak{p}_1} \setminus \mathbf{E}_X,\ \dots,\ \lambda_l \in \mathbf{E}_{\mathfrak{p}_l} \setminus \mathbf{E}_X.$$

By assumption $\mathfrak{p}_i \smile \mathfrak{p}_j$ for all $1 \leq i \neq j \leq l$, hence every λ_i is a local square at every $\mathfrak{p}_j$ for $j \neq i$. Multiplying by appropriate μ_j's if necessary, we may assume without loss of generality that $\lambda, \lambda_1, \dots, \lambda_l$ are local squares at $\mathfrak{q}_j$ for every $j = 1, \dots, m$.

Denote

$$\mathcal{S} := \{\mathfrak{p}, \mathfrak{p}_1, \dots, \mathfrak{p}_l, \mathfrak{q}_1, \dots, \mathfrak{q}_m\}$$

and let $Z := X \setminus \mathcal{S} \subset Y$. It follows from Lemma 2.5 that $\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Z = 0$ and so $\mathcal{S}$ is a sufficiently large set. We claim that the set

$$\mathscr{B} := \{\lambda, \lambda_1, \dots, \lambda_l, \mu_1, \dots, \mu_m\}$$

forms a basis of the $\mathbb{F}_2$-linear space $\mathbf{E}_Z$. First, we show that it is linearly independent. Suppose it is not. Thus

$$\nu := \lambda^a \cdot \prod_{i=1}^{l} \lambda_i^{b_i} \cdot \prod_{j=1}^{m} \mu_j^{c_j}$$

is a square in K for some $a, b_1, \dots, b_l, c_1, \dots, c_m \in \mathbb{F}_2$. This means that $0 \equiv \operatorname{ord}_\mathfrak{p} \nu \equiv a \pmod 2$, since all the other elements have even order at $\mathfrak{p}$, consequently $a = 0$. Similarly, for every $1 \leq i \leq l$, $0 \equiv \operatorname{ord}_{\mathfrak{p}_i} \nu \equiv b_i \pmod 2$ so also $b_1 = \dots = b_l = 0$. Finally, $c_1 = \dots = c_m = 0$, because $\mu_1, \dots, \mu_m$ are linearly independent in $\mathbf{\Delta}_Y$, a subspace of $\mathbf{E}_X$. Further, Proposition 2.3 asserts that

$$\dim_{\mathbb{F}_2} \mathbf{E}_Z = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_Z + \operatorname{card}(\mathcal{S}) = \operatorname{card}(\mathscr{B}),$$

proving that $\mathscr{B}$ is a basis of $\mathbf{E}_Z$.

Observe that if $\mathfrak{p}$ is related to *every* point $\mathfrak{p}_i$, $i = 1, \dots, l$, then a $\mathfrak{p}$-primary unit u does not belong to $\mathbf{E}_Z$. On the other hand, if $\mathfrak{p} \not\smile \mathfrak{p}_i$ for some $i \in \{1, \dots, l\}$, then the element λ_i obtained above is a $\mathfrak{p}$-primary unit (and symmetrically λ is a $\mathfrak{p}_i$-primary unit).

Construct a triple $(T_{\mathcal{S}}, t_{\mathcal{S}}, (t_{\mathfrak{r}} \mid \mathfrak{r} \in \mathcal{S}))$ in the following way:

- let $T_{\mathcal{S}} : \mathcal{S} \to \mathcal{S}$ be the identity;
- define the automorphism $t_{\mathcal{S}} : \mathbf{E}_Z \to \mathbf{E}_Z$ by fixing its values on the basis $\mathscr{B}$:
  - $t_{\mathcal{S}}(\lambda) := \lambda$,
  - $t_{\mathcal{S}}(\lambda_i) := \begin{cases} \lambda_i & \text{if } \mathfrak{p} \smile \mathfrak{p}_i, \\ \lambda\lambda_i & \text{if } \mathfrak{p} \not\smile \mathfrak{p}_i, \end{cases}$
  - $t_{\mathcal{S}}(\mu_j) := \mu_j$ for $j = 1, \dots, m$;
- finally, the automorphisms of the local square-class groups are given as follows:
  - $t_{\mathfrak{p}}$ is the transposition $(u, u\lambda)$ on $K_{\mathfrak{p}}^{\times}/K_{\mathfrak{p}}^{\times 2} = \{1, u, \lambda, u\lambda\}$ (recall that $u = \lambda_i \pmod{K_{\mathfrak{p}}^{\times 2}}$ whenever $\mathfrak{p} \not\smile \mathfrak{p}_i$),
  - for a point $\mathfrak{p}_i$ related to $\mathfrak{p}$, take $t_{\mathfrak{p}_i}$ to be the identity on $K_{\mathfrak{p}_i}^{\times}/K_{\mathfrak{p}_i}^{\times 2}$,
  - for a point $\mathfrak{p}_i$ not related to $\mathfrak{p}$, let $t_{\mathfrak{p}_i}$ be a "tame transposition" $(\lambda_i, \lambda\lambda_i)$ on the group $K_{\mathfrak{p}_i}^{\times}/K_{\mathfrak{p}_i}^{\times 2} = \{1, \lambda, \lambda_i, \lambda\lambda_i\}$,
  - for the remaining points $\mathfrak{q}_1, \dots, \mathfrak{q}_m$, let $t_{\mathfrak{q}_j}$ be the identity on the corresponding square-class group.

The commutativity of the diagram (4) is now immediate. It follows that the triple $(T_{\mathcal{S}}, t_{\mathcal{S}}, (t_{\mathfrak{r}} \mid \mathfrak{r} \in \mathcal{S}))$ is a small equivalence and Theorem 4.4 asserts that it can be extended to a self-equivalence (T, t) of K tame on Z. Since only $t_{\mathfrak{p}}$ is wild, $\mathfrak{p}$ is the unique wild point of (T, t). ∎

LEMMA 4.6. *Let K be a global function field and X an associated smooth curve, and let (T, t) be a self-equivalence of K. If (T, t) has a unique wild point $\mathfrak{p}$, then $\mathfrak{p} \in 2 \operatorname{Pic} X$.*

Proof. By the assumption $\mathcal{W}(T, t) = \{\mathfrak{p}\}$. Denote $\mathfrak{q} := T\mathfrak{p}$. Suppose that $\mathfrak{p}$ is not 2-divisible. Thus, Proposition 3.2 shows that every element of $E_{\mathfrak{p}}$ has even order at $\mathfrak{p}$, in particular $\mathbf{E}_{\mathfrak{p}} = \mathbf{E}_X$. Now, it follows from Proposition 2.3(3) that there is an element $\lambda \in K$ such that $\mathbf{E}_X = \mathbf{E}_{\mathfrak{p}} = \langle\lambda\rangle \oplus \mathbf{\Delta}_{\mathfrak{p}}$. Clearly, $\operatorname{ord}_{\mathfrak{p}} \lambda \equiv 0 \pmod 2$ and λ is not a local square at $\mathfrak{p}$, that is, λ is a $\mathfrak{p}$-primary unit.

As $\mathfrak{p}$ is a wild point of (T, t), we have $\operatorname{ord}_{\mathfrak{q}} t\lambda \equiv 1 \pmod 2$ by Observation 2.1. It follows from Proposition 3.2 that $\mathfrak{q}$ is an even point of K. It is straightforward to show that $t\mathbf{E}_{\mathfrak{p}} = \mathbf{E}_{T\mathfrak{p}} = \mathbf{E}_{\mathfrak{q}}$. In particular, the 2-ranks must agree:

$$\operatorname{rk}_2 \mathbf{E}_{\mathfrak{p}} = \operatorname{rk}_2 \mathbf{E}_{\mathfrak{q}}.$$

Use Proposition 2.3 to express these 2-ranks as

$$\operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{p}} + 1 = \operatorname{rk}_2 \operatorname{Pic} \mathcal{O}_{\mathfrak{q}} + 1.$$

Now, $\mathfrak{q}$ is 2-divisible in $\operatorname{Pic} X$, while $\mathfrak{p}$ is not. Proposition 2.7 asserts that the left-hand side equals $\operatorname{rk}_2 \operatorname{Pic}^0 X+1$, while the right-hand side is $\operatorname{rk}_2 \operatorname{Pic}^0 X+2$. This is clearly a contradiction. ∎

Combining Proposition 4.5 with the above lemma, we arrive at our first main result.

THEOREM 4.7. *Let K be a global function field and X an associated smooth curve. Given a point $\mathfrak{p} \in X$, the following two conditions are equivalent:*

- $\mathfrak{p}$ *is* 2*-divisible in* $\operatorname{Pic} X$*;*
- $\mathfrak{p}$ *is the unique wild point of some self-equivalence of* K*.*

Looking at Proposition 4.5 obviously shows that if we have a set of even points and each of them is related to all the others, then we can build a number of self-equivalences, each wild at precisely one of these points and preserving the rest. Then the wild set of the composition of all these self-equivalences consists of all our (related) even points. It turns out that this is still true even when not all the points are related. Theorem 4.8 below not only generalizes one implication of Theorem 4.7, but also constitutes a direct counterpart of [CR14, Theorem 1.1] for the case of global function fields.

THEOREM 4.8. *Let K be a global function field and X be its associated smooth curve. Given finitely many points $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in X$ that are* 2*-divisible in* $\operatorname{Pic} X$*, there is a self-equivalence (T, t) of K such that $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are precisely its wild points, i.e. $\mathcal{W}(T, t) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.*

Proof. We proceed by induction on n. The case $n = 1$ simply boils down to Theorem 4.7. Hence, suppose that the assertion holds for all sets of cardinality $n - 1$ and consider a set of n even points $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \subset X$. Since $\mathfrak{p}_1$ is even, Proposition 4.5 asserts that there exists a self-equivalence (T_1, t_1) of K such that $\mathfrak{p}_1$ is the unique wild point of (T_1, t_1) and $T_1\mathfrak{p}_1 = \mathfrak{p}_1$. Denote the images of the remaining points by $\mathfrak{q}_2 := T_1\mathfrak{p}_2$, …, $\mathfrak{q}_n := T_1\mathfrak{p}_n$. We claim that $\mathfrak{q}_2, \ldots, \mathfrak{q}_n$ are all 2-divisible in $\operatorname{Pic} X$.

In order to prove the claim, observe first that since $\mathfrak{p}_1$ is even, $\mathbf{\Delta}_{\mathfrak{p}_1} = \mathbf{E}_X$ by Proposition 3.4. Moreover (T_1, t_1) is tame on $X \setminus \{\mathfrak{p}_1\}$, therefore $t_1\mathbf{E}_{\mathfrak{p}_1} = \mathbf{E}_{T_1\mathfrak{p}_1} = \mathbf{E}_{\mathfrak{p}_1}$. It follows that also $t_1\mathbf{\Delta}_{\mathfrak{p}_1} = t_1(\mathbf{E}_{\mathfrak{p}_1} \cap K_{\mathfrak{p}_1}^{\times 2}) = \mathbf{E}_{\mathfrak{p}_1} \cap K_{\mathfrak{p}_1}^{\times 2} = \mathbf{\Delta}_{\mathfrak{p}_1}$, as every self-equivalence preserves local squares. Consequently,

$$t\mathbf{E}_X = t_1\mathbf{\Delta}_{\mathfrak{p}_1} = \mathbf{\Delta}_{\mathfrak{p}_1} = \mathbf{E}_X.$$

Take now any point $\mathfrak{p}_i$ with $i > 1$ and write

$$\mathbf{E}_X = t_1\mathbf{E}_X = t_1\mathbf{\Delta}_{\mathfrak{p}_i} = t_1(\mathbf{E}_X \cap K_{\mathfrak{p}_i}^{\times 2}) = t_1\mathbf{E}_X \cap t_1K_{\mathfrak{p}_i}^{\times 2} = \mathbf{E}_X \cap K_{\mathfrak{q}_i}^{\times 2} = \mathbf{\Delta}_{\mathfrak{q}_i}.$$

It follows from Proposition 3.4 that $\mathfrak{q}_i \in 2 \operatorname{Pic} X$, as claimed.

By the inductive hypothesis, there exists a self-equivalence (T_2, t_2) of K with wild set $\mathcal{W}(T_2, t_2) = \{\mathfrak{q}_2, \ldots, \mathfrak{q}_n\}$. The composition

$$(T, t) = (T_2 \circ T_1, t_2 \circ t_1)$$

is now the desired self-equivalence of K with wild set $\mathcal{W}(T, t) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. ■

REMARK 5. The above theorem generalizes only one of the implications of Theorem 4.7 to sets having more than one point. This is all we can do, since the opposite implication no longer holds for larger sets. The simplest counterexample we are aware of is probably the following: Let K be the function field of the elliptic curve over $\mathbb{F}_5$ given in Weierstrass normal form by the polynomial $y^2 + x^3 + x + 2$. Take two points: $\mathfrak{p} \sim (1, 1)$ and $\mathfrak{q} \sim (1, 4)$. Then neither of them is even, since both are rational. Nevertheless, there exists a self-equivalence of K that is wild precisely at these two points. We will discuss the structure of bigger wild sets in another paper.

Acknowledgments. We wish to thank the anonymous reviewer for providing a corrected proof of Lemma 3.3 and for useful comments that improved the overall exposition of the paper.

REFERENCES

[BS66] A. I. Borevich and I. R. Shafarevich, *Number Theory*, Pure Appl. Math. 20, Academic Press, New York, 1966.

[BCP97] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), 235–265.

[Czo01] A. Czogała, *Witt rings of Hasse domains of global fields*, J. Algebra 244 (2001), 604–630.

[CR14] A. Czogała and B. Rothkegel, *Wild primes of a self-equivalence of a number field*, Acta Arith. 166 (2014), 335–348.

[CS97] A. Czogała and A. Sładek, *Higher degree Hilbert-symbol equivalence of number fields*, Tatra Mt. Math. Publ. 11 (1997), 77–88.

[CS98] A. Czogała and A. Sładek, *Higher degree Hilbert symbol equivalence of algebraic number fields. II*, J. Number Theory 72 (1998), 363–376.

[Kop02] P. Koprowski, *Witt equivalence of algebraic function fields over real closed fields*, Math. Z. 242 (2002), 323–345.

[Lam05] T. Y. Lam, *Introduction to Quadratic Forms over Fields*, Grad. Stud. Math. 67, Amer. Math. Soc., Providence, RI, 2005.

[Lor96] D. Lorenzini, *An Invitation to Arithmetic Geometry*, Grad. Stud. Math. 9, Amer. Math. Soc., Providence, RI, 1996.

[PSCL94] R. Perlis, K. Szymiczek, P. E. Conner, and R. Litherland, *Matching Witts with global fields*, in: Recent Advances in Real Algebraic Geometry and Quadratic Forms (Berkeley, CA, 1990/1991; San Francisco, CA, 1991), Contemp. Math. 155, Amer. Math. Soc., Providence, RI, 1994, 365–387.

[Ros02] M. Rosen, *Number Theory in Function Fields*, Grad Texts in Math. 210, Springer, New York, 2002.

[RC07] B. Rothkegel and A. Czogała, *Witt equivalence of semilocal Dedekind domains in global fields*, Abh. Math. Sem. Univ. Hamburg 77 (2007), 1–24.

[Som06] M. Somodi, *A characterization of the finite wild sets of rational self-equivalences*, Acta Arith. 121 (2006), 327–334.

[Som08] M. Somodi, *Self-equivalences of the Gaussian field*, Rocky Mountain J. Math. 38 (2008), 2077–2089.

Alfred Czogała, Przemysław Koprowski, Beata Rothkegel
Institute of Mathematics
University of Silesia
Bankowa 14
40-007 Katowice, Poland
E-mail: alfred.czogala@us.edu.pl
przemyslaw.koprowski@us.edu.pl
brothkegel@math.us.edu.pl