ACTA ARITHMETICA
166.4 (2014)

Wild primes of a self-equivalence of a number field

by

Alfred Czogała and Beata Rothkegel (Katowice)

1. Introduction. Let K be a number field. By a *self-equivalence* of K we understand a pair of maps (T,t), where $T\colon \Omega(K)\to\Omega(K)$ is a bijection of the set $\Omega(K)$ of all primes of K and $t\colon \dot K/\dot K^2\to \dot K/\dot K^2$ is an automorphism of the square class group $\dot K/\dot K^2$ that preserves the Hilbert symbols:

$$(x,y)_{\mathfrak p}=(tx,ty)_{T\mathfrak p}\quad \text{for all } \mathfrak p\in\Omega(K),\ x,y\in \dot K/\dot K^2.$$

A finite prime $\mathfrak p\in\Omega(K)$ of the field K is said to be a *tame* prime of (T,t) if

$$\operatorname{ord}_{\mathfrak p} x\equiv \operatorname{ord}_{T\mathfrak p} tx \pmod 2\quad \text{for all } x\in \dot K/\dot K^2.$$

A prime $\mathfrak p\in\Omega(K)$ is said to be *wild* if it is not a tame prime of (T,t). The set $\mathcal W=\mathcal W(T,t)$ of all wild primes of (T,t) is called the *wild set* of (T,t).

In [S1] and [S3] Somodi has examined wild primes in the case of the rational number field $\mathbb Q$ and the Gaussian field $\mathbb Q(i)$, respectively. In [S1] it was shown that a finite set $\mathcal W$ of primes of $\mathbb Q$ is the wild set of some self-equivalence (T,t) of $\mathbb Q$ if and only if any nondyadic prime in $\mathcal W$ is generated by a prime number $p\equiv 1 \pmod 4$. In [S3] it was proven that any set of primes of the field $\mathbb Q(i)$ is the wild set of some self-equivalence (T,t) of $\mathbb Q(i)$.

In this paper we examine the wild sets of self-equivalences of algebraic number fields K which satisfy the following two conditions:

(c1) *The* 2*-rank of the ideal class group C_K of K is equal to the* 2*-rank of the narrow ideal class group C_K^+ of K.*
(c2) *The field K has a unique dyadic prime $\mathfrak d$ and the class $\mathsf{cl}\,\mathfrak d$ of $\mathfrak d$ is a square in the ideal class group C_K.*

We prove the following result.

Theorem 1.1 (Main result). *Let K be a number field which satisfies* (c1) *and* (c2). *Let $\{\mathfrak p_1,\dots,\mathfrak p_n\}$ be a set of finite primes of K which satisfy the following conditions:*

2010 *Mathematics Subject Classification*: Primary 11E12; Secondary 11E81.
Key words and phrases: self-equivalence, small $\mathcal S$-equivalence, wild prime.

DOI: 10.4064/aa166-4-2 © Instytut Matematyczny PAN, 2014

(w1) $\left(\frac{-1}{\mathfrak{p}_i}\right) = 1$ *for every nondyadic prime* $\mathfrak{p}_i \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.
(w2) $\mathsf{cl}\,\mathfrak{p}_i \in C_K^2$ *for every* $i \in \{1, \ldots, n\}$.

Then there exists a self-equivalence (T,t) *of* K *such that* $\mathcal{W}(T,t) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

Theorem 1.1 will be proven in three steps. In the first step (Subsection 3.1) we shall construct a self-equivalence of K with a unique wild prime $\mathfrak{d}$. Similarly, in the second step (Subsection 3.2) we shall construct a self-equivalence of K with a unique wild prime $\mathfrak{p}$ which is nondyadic and satisfies (w1) and (w2). Using these results, in the third step (Section 4) we shall use induction, as in [S1] and [S3].

It is clear that the rational number field $\mathbb{Q}$ and the Gaussian field $\mathbb{Q}(i)$ satisfy (c1) and (c2), and thus the above theorem generalizes the results of [S1] and [S3]. In Section 4 we shall describe all quadratic number fields which satisfy (c1) and (c2).

In the construction of self-equivalences we shall use the methods developed in [PSCL] and [C]. In Section 2 we adjust these methods to the present situation. In general, we follow the standard terminology and notation of [S2] but we shall slightly simplify them.

Now we introduce some notation.

Throughout the paper, $\Omega(K)$ denotes the set of all primes of a number field K. We write $l = l_K$ for the 2-rank of the ideal class group C_K and $r = r(K)$ for the number of infinite real primes of K.

A finite nonempty set $\mathcal{S} \subset \Omega(K)$ of primes of K will be called a *Hasse set* if it contains all infinite (archimedean) primes of K. For every Hasse set $\mathcal{S}$ of K the set

$$\mathcal{O}_{\mathcal{S}} = \mathcal{O}_{\mathcal{S}}(K) = \{x \in K : \operatorname{ord}_{\mathfrak{p}} x \geq 0 \text{ for all } \mathfrak{p} \text{ outside } \mathcal{S}\}$$

is called the ring of $\mathcal{S}$-*integers* of K. The ideal class group and the class number of $\mathcal{O}_{\mathcal{S}}(K)$ will be denoted by $C_{\mathcal{S}} = C_{\mathcal{S}}(K)$ and $h_{\mathcal{S}} = h_{\mathcal{S}}(K)$, respectively. The narrow ideal class group $C_{\mathcal{S}}^+ = C_{\mathcal{S}}^+(K)$ of $\mathcal{O}_{\mathcal{S}}(K)$ is called the *narrow* $\mathcal{S}$-*class group* of K.

For $\mathfrak{p} \in \Omega(K)$ we write $K_{\mathfrak{p}}$ for the completion of K at $\mathfrak{p}$. If $\mathfrak{p}$ is a nondyadic finite prime, then we denote the quadratic residue symbol modulo $\mathfrak{p}$ by $\left(\frac{\cdot}{\mathfrak{p}}\right)$.

If G is an abelian group and H is a subgroup of G such that $G^2 \subset H$, then G/H is an elementary abelian 2-group and can be equipped with the structure of an $\mathbb{F}_2$-vector space. We shall then frequently use the vector space terminology. In particular, the 2-rank of G is the dimension of G/G^2 as an $\mathbb{F}_2$-vector space. Where it is not misleading, we shall simply denote the square class aG^2 by a. We shall use this notation mainly for the local square $a\dot{K}_{\mathfrak{p}}^2$ and the global square class $a\dot{K}^2$.

We write $\langle a_1, \ldots, a_n \rangle$ for the $\mathbb{F}_2$-vector subspace of G/G^2 generated by $a_1, \ldots, a_n \in G$.

2. Preliminary results. From now on, K denotes an algebraic number field.

Assume that S is a Hasse set of primes of K containing all dyadic primes of K. We denote

$$E_{\mathcal{S}} = E_{\mathcal{S}}(K) = \{x \in \dot{K} : \operatorname{ord}_{\mathfrak{p}} x \equiv 0 \pmod 2 \text{ for all } \mathfrak{p} \text{ outside } \mathcal{S}\},$$
$$\Delta_{\mathcal{S}} = \Delta_{\mathcal{S}}(K) = \{x \in E_{\mathcal{S}} : x \in \dot{K}_{\mathfrak{p}}^2 \text{ for all } \mathfrak{p} \in \mathcal{S}\}.$$

It is easy to check that $E_{\mathcal{S}}$ is a subgroup of the multiplicative group $\dot{K}$ and $\dot{K}^2 \subseteq \Delta_{\mathcal{S}} \subseteq E_{\mathcal{S}}$. Elements that belong to $E_{\mathcal{S}}$ are said to be *S-singular*.

From [C2, p. 607] it follows that

$$\mathsf{rk}_2\, E_{\mathcal{S}}/\dot{K}^2 = \#\,\mathcal{S} + \mathsf{rk}_2\, C_{\mathcal{S}}.$$

By [C2, Lemma 2.1],

$$\mathsf{rk}_2\, \Delta_{\mathcal{S}}/\dot{K}^2 = \mathsf{rk}_2\, C_{\mathcal{S}}.$$

Therefore

$$\mathsf{rk}_2\, E_{\mathcal{S}}/\Delta_{\mathcal{S}} = \#\,\mathcal{S}.$$

Remark 2.1. Assume that $S \subset S'$ are Hasse sets of K. Then $E_{\mathcal{S}} \subseteq E_{\mathcal{S}'}$ and $\Delta_{\mathcal{S}'} \subseteq \Delta_{\mathcal{S}}$. Moreover, there is a natural group epimorphism $C_{\mathcal{S}} \to C_{\mathcal{S}'}$. This epimorphism induces an epimorphism $C_{\mathcal{S}}/C_{\mathcal{S}}^2 \to C_{\mathcal{S}'}/C_{\mathcal{S}'}^2$, whose kernel is the subgroup of $C_{\mathcal{S}}/C_{\mathcal{S}}^2$ generated by the set $\{\mathsf{cl}\,\mathfrak{p}\, C_{\mathcal{S}}^2 : \mathfrak{p} \in \mathcal{S}' \setminus \mathcal{S}\}$. Thus

$$\mathsf{rk}_2\, C_{\mathcal{S}'} = \mathsf{rk}_2\, C_{\mathcal{S}} - \mathsf{rk}_2 \langle \{\mathsf{cl}\,\mathfrak{p}\, C_{\mathcal{S}}^2 : \mathfrak{p} \in \mathcal{S}' \setminus \mathcal{S}\}\rangle$$

and

$$\mathsf{rk}_2\, E_{\mathcal{S}'}/\dot{K}^2 = \#\,\mathcal{S}' + (\mathsf{rk}_2\, C_{\mathcal{S}} - \mathsf{rk}_2 \langle \{\mathsf{cl}\,\mathfrak{p}\, C_{\mathcal{S}}^2 : \mathfrak{p} \in \mathcal{S}' \setminus \mathcal{S}\}\rangle).$$

Lemma 2.2. *Let $\mathcal{S}$ be a Hasse set of primes of K containing all dyadic primes and $\mathfrak{p} \in \Omega(K) \setminus \mathcal{S}$. Then*

$$\mathsf{cl}\,\mathfrak{p} \in C_{\mathcal{S}}^2 \iff \left(\frac{b}{\mathfrak{p}}\right) = 1 \text{ for every } b \in \Delta_{\mathcal{S}}.$$

Proof. ($\Rightarrow$) By assumption there exists $x_{\mathfrak{p}} \in \dot{K}$ such that $(x_{\mathfrak{p}}) = \mathfrak{p} \cdot J^2$ for some fractional $\mathcal{S}$-ideal J of K. Fix $b \in \Delta_{\mathcal{S}}$. Since for every prime $\mathfrak{q} \notin \mathcal{S} \cup \{\mathfrak{p}\}$ the elements $b, x_{\mathfrak{p}}$ are $\mathfrak{q}$-adic units modulo $\dot{K}_{\mathfrak{q}}^2$,

$$(b, x_{\mathfrak{p}})_{\mathfrak{q}} = 1 \quad \text{for every } \mathfrak{q} \notin \mathcal{S} \cup \{\mathfrak{p}\}.$$

As $b \in \dot{K}_{\mathfrak{q}}^2$ for every $\mathfrak{q} \in \mathcal{S}$, we have

$$(b, x_{\mathfrak{p}})_{\mathfrak{q}} = 1 \quad \text{for every } \mathfrak{q} \in \mathcal{S}.$$

From Hilbert reciprocity, $(b, x_{\mathfrak{p}})_{\mathfrak{p}} = 1$, i.e. $\left(\frac{b}{\mathfrak{p}}\right) = 1$.

($\Leftarrow$) Let $\mathcal{S}_1 = \mathcal{S} \cup \{\mathfrak{p}\}$. Since $b \in \dot{K}_{\mathfrak{p}}^2$ for every $b \in \Delta_{\mathcal{S}}$ (by assumption), $\Delta_{\mathcal{S}_1} = \Delta_{\mathcal{S}}$. Thus

$$\mathsf{rk}_2\, C_{\mathcal{S}} = \mathsf{rk}_2\, C_{\mathcal{S}_1},$$

so $\mathsf{cl}\,\mathfrak{p} \in C_{\mathcal{S}}^2$. ∎

Proposition 2.3. *Let $\mathcal{S}$ be a Hasse set of primes of K containing all dyadic primes and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \Omega(K) \setminus \mathcal{S}$ be nondyadic primes of K. The classes $\mathsf{cl}\,\mathfrak{p}_1, \ldots, \mathsf{cl}\,\mathfrak{p}_n$ in K are linearly independent in the group $C_{\mathcal{S}}/C_{\mathcal{S}}^2$ if and only if there exist $b_1, \ldots, b_n \in \Delta_{\mathcal{S}}$ linearly independent in the group $\Delta_{\mathcal{S}}/\dot{K}^2$ such that*

$$\left(\frac{b_i}{\mathfrak{p}_i}\right) = -1, \quad \left(\frac{b_i}{\mathfrak{p}_j}\right) = 1 \quad \textit{for all } i, j \in \{1, \ldots, n\},\ i \neq j.$$

Proof. The implication "⇐" follows from [C2, Lemma 2.1].

(⇒) Induction on n. If $n = 1$, then this follows from Lemma 2.2.

Now assume $n > 1$. By Lemma 2.2 there exists $b_1 \in \Delta_{\mathcal{S}}$ such that $\left(\frac{b_1}{\mathfrak{p}_1}\right) = -1$. Let $\mathcal{S}_1 = \mathcal{S} \cup \{\mathfrak{p}_1\}$. Then $\mathsf{rk}_2\, C_{\mathcal{S}_1} = \mathsf{rk}_2\, C_{\mathcal{S}} - 1$, $\Delta_{\mathcal{S}_1} \subseteq \Delta_{\mathcal{S}}$ and $b_1 \notin \Delta_{\mathcal{S}_1}$. Moreover, $\mathsf{cl}\,\mathfrak{p}_2, \ldots, \mathsf{cl}\,\mathfrak{p}_n$ are linearly independent in $C_{\mathcal{S}_1}/C_{\mathcal{S}_1}^2$.

The induction hypothesis shows that there exist $b_2, \ldots, b_n \in \Delta_{\mathcal{S}_1}$ linearly independent in $\Delta_{\mathcal{S}_1}/\dot{K}^2$ such that

$$\left(\frac{b_i}{\mathfrak{p}_i}\right) = -1, \quad \left(\frac{b_i}{\mathfrak{p}_j}\right) = 1 \quad \text{for all } i, j \in \{2, \ldots, n\},\ i \neq j.$$

Obviously $\left(\frac{b_i}{\mathfrak{p}_1}\right) = 1$ for $i = 2, \ldots, n$. If necessary, we multiply b_1 by a product of appropriate elements b_i, $i \in \{2, \ldots, n\}$, to get $\left(\frac{b_1}{\mathfrak{p}_i}\right) = 1$ for $i = 2, \ldots, n$. ■

Let $\mathcal{S}$ be a Hasse set of K. We say that $\mathcal{S}$ is *sufficiently large* if it contains all infinite primes and all dyadic primes of K and $\mathsf{rk}_2\, C_{\mathcal{S}} = 0$.

Let $\mathcal{S}$ and $\mathcal{S}'$ be sufficiently large sets of primes of the field K. A triple $(T_{\mathcal{S}}, t_{\mathcal{S}}, \prod_{\mathfrak{p}\in\mathcal{S}} t_{\mathfrak{p}})$ is said to be a *small $\mathcal{S}$-equivalence* of K if

- $T_{\mathcal{S}} \colon \mathcal{S} \to \mathcal{S}'$ is a bijection,
- $t_{\mathcal{S}} \colon E_{\mathcal{S}}/\dot{K}^2 \to E_{\mathcal{S}'}/\dot{K}^2$ is an isomorphism of groups,
- for every $\mathfrak{p} \in \mathcal{S}$ the map $t_{\mathfrak{p}} \colon \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \to \dot{K}_{T\mathfrak{p}}/\dot{K}_{T\mathfrak{p}}^2$ is a Hilbert-symbol-preserving local isomorphism:

$$(x, y)_{\mathfrak{p}} = (t_{\mathfrak{p}}x, t_{\mathfrak{p}}y)_{T\mathfrak{p}} \quad \text{for all } x, y \in \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2,$$

- the diagram

$$\begin{array}{ccc} E_{\mathcal{S}}/\dot{K}^2 & \xrightarrow{\ i_{\mathcal{S}}\ } & \prod_{\mathfrak{p}\in\mathcal{S}} \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \\ \Big\downarrow t_{\mathcal{S}} & & \Big\downarrow \prod_{\mathfrak{p}\in\mathcal{S}} t_{\mathfrak{p}} \\ E_{\mathcal{S}'}/\dot{K}^2 & \xrightarrow{\ i_{\mathcal{S}'}\ } & \prod_{\mathfrak{p}\in\mathcal{S}} \dot{K}_{T\mathfrak{p}}/\dot{K}_{T\mathfrak{p}}^2 \end{array} \tag{2.1}$$

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

$$i_{\mathfrak{p}} \colon E_{\mathcal{S}}/\dot{K}^2 \to \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \quad \text{and} \quad i_{\mathfrak{q}} \colon E_{\mathcal{S}'}/\dot{K}^2 \to \dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2.$$

We say that the local isomorphism $t_{\mathfrak{p}}\colon \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \to \dot{K}_{T\mathfrak{p}}/\dot{K}_{T\mathfrak{p}}^2$ is *tame* when

$$\operatorname{ord}_{\mathfrak{p}} a \equiv \operatorname{ord}_{T\mathfrak{p}} t_{\mathfrak{p}}(a) \pmod 2 \quad \text{for every } a \in \dot{K}_{\mathfrak{p}}.$$

The following theorem follows from [PSCL, Theorem 2 and Lemma 4].

THEOREM 2.4. *Every small $\mathcal{S}$-equivalence $(T_{\mathcal{S}}, t_{\mathcal{S}}, \prod_{\mathfrak{p}\in\mathcal{S}} t_{\mathfrak{p}})$ of K can be extended to a self-equivalence (T, t) of K that is tame outside $\mathcal{S}$:*

$$\mathfrak{p} \notin \mathcal{W}(T,t) \quad \textit{for every } \mathfrak{p} \in \Omega(K) \setminus \mathcal{S}.$$

The self-equivalence (T,t) is tame at a finite prime $\mathfrak{p} \in \mathcal{S}$ if and only if the local isomorphism $t_{\mathfrak{p}}$ is tame.

Assume that $\mathfrak{p}$ is a finite prime of K. We write $\pi_{\mathfrak{p}}$ for a fixed local uniformizer at $\mathfrak{p}$, and $u_{\mathfrak{p}}$ for a unique square class in $K_{\mathfrak{p}}$ which has the property that the extension $K_{\mathfrak{p}}(\sqrt{u_{\mathfrak{p}}})/K_{\mathfrak{p}}$ is quadratic unramified. We call $u_{\mathfrak{p}}$ the $\mathfrak{p}$-*primary unit.* It is also characterized by the property

$$(u_{\mathfrak{p}}, y)_{\mathfrak{p}} = (-1)^{\operatorname{ord}_{\mathfrak{p}} y} \quad \text{for every } y \in \dot{K}_{\mathfrak{p}}.$$

The local square group $\dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2$ has the structure of a nondegenerate $\mathbb{F}_2$-inner product space given by the Hilbert symbol $(\ ,\ )_{\mathfrak{p}}$ provided we identify the additive group $\mathbb{F}_2$ with the multiplicative group $\{\pm 1\}$. Using the properties of Hilbert symbols, it is easy to check that the $\mathbb{F}_2$-subspace $\langle u_{\mathfrak{p}},\, \pi_{\mathfrak{p}}\rangle$ of $\dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2$ is nonsingular, so by the orthogonal complement theorem (cf. [S, Theorem 5.2.2]) we obtain the orthogonal direct sum decomposition

$$\dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 = \langle u_{\mathfrak{p}}, \pi_{\mathfrak{p}}\rangle \oplus \langle u_{\mathfrak{p}}, \pi_{\mathfrak{p}}\rangle^{\perp}.$$

Note that when $\mathfrak{p}$ is a nondyadic prime, the orthogonal complement $\langle u_{\mathfrak{p}}, \pi_{\mathfrak{p}}\rangle^{\perp}$ is the zero subspace (i.e. $\dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 = \langle u_{\mathfrak{p}}, \pi_{\mathfrak{p}}\rangle$).

LEMMA 2.5. *If $\mathfrak{p}$ is a dyadic prime such that $u_{\mathfrak{p}} \neq -1 \bmod \dot{K}_{\mathfrak{p}}^2$, then the isomorphism $\tau\colon \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \to \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2$ defined by*

$$\tau(u_{\mathfrak{p}}) = u_{\mathfrak{p}}\pi_{\mathfrak{p}}, \quad \tau(\pi_{\mathfrak{p}}) = \pi_{\mathfrak{p}}, \quad \tau(v) = v \quad \textit{for every } v \in \langle u_{\mathfrak{p}}, \pi_{\mathfrak{p}}\rangle^{\perp}$$

is an isometry of the inner product space $(\dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2,\, (\ ,\ )_{\mathfrak{p}})$ into itself (*i.e. τ preserves the Hilbert symbol*).

Proof. First we observe that the assumption $u_{\mathfrak{p}} \neq -1 \bmod \dot{K}_{\mathfrak{p}}^2$ implies that $(\pi_{\mathfrak{p}}, \pi_{\mathfrak{p}})_{\mathfrak{p}} = (-1, \pi_{\mathfrak{p}})_{\mathfrak{p}} = 1$. Now it suffices to observe that

$$(u_{\mathfrak{p}}\pi_{\mathfrak{p}}, u_{\mathfrak{p}}\pi_{\mathfrak{p}})_{\mathfrak{p}} = (-1, u_{\mathfrak{p}}\pi_{\mathfrak{p}})_{\mathfrak{p}} = (-1, u_{\mathfrak{p}})_{\mathfrak{p}}(-1, \pi_{\mathfrak{p}})_{\mathfrak{p}} = 1 = (u_{\mathfrak{p}}, u_{\mathfrak{p}})_{\mathfrak{p}},$$
$$(u_{\mathfrak{p}}\pi_{\mathfrak{p}}, \pi_{\mathfrak{p}})_{\mathfrak{p}} = (u_{\mathfrak{p}}, \pi_{\mathfrak{p}})_{\mathfrak{p}}(-1, \pi_{\mathfrak{p}})_{\mathfrak{p}} = -1 = (u_{\mathfrak{p}}, \pi_{\mathfrak{p}})_{\mathfrak{p}},$$
$$(u_{\mathfrak{p}}\pi_{\mathfrak{p}}, v)_{\mathfrak{p}} = 1 = (u_{\mathfrak{p}}, v)_{\mathfrak{p}} \quad \text{for every } v \in \langle u_{\mathfrak{p}}, \pi_{\mathfrak{p}}\rangle^{\perp}. \ \blacksquare$$

Analogously, we can prove the following lemma.

Lemma 2.6. *If* $\mathfrak{p}$ *and* $\mathfrak{q}$ *are nondyadic primes such that* $\left(\frac{-1}{\mathfrak{p}}\right)=\left(\frac{-1}{\mathfrak{q}}\right)=1$, *then the isomorphism* $\tau\colon \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \to \dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2$ *defined by*

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

is an isometry of inner product spaces.

3. Self-equivalence with one wild prime. Assume K is a number field which satisfies (c1) and (c2).

Let $\mathcal{R} = \{\infty_1, \ldots, \infty_r\}$ ($r \ge 0$) be the set of all infinite real primes of K. We set $E_K = E_{\mathcal{R}}$. Of course, the $\mathcal{R}$-ideal class group $C_{\mathcal{R}}$ and the narrow $\mathcal{R}$-ideal class group $C_{\mathcal{R}}^+$ are equal to C_K and C_K^+, respectively.

Let $\mathfrak{d} \in \Omega(K)$ be a unique dyadic prime of K. Then, by assumption, $\mathsf{cl}\,\mathfrak{d} \in C_K^2$, so $\mathsf{cl}\,\mathfrak{d} \in C_K^{+2}$. There exists a totally positive element $x_{\mathfrak{d}} \in \dot{K}^+$ such that $(x_{\mathfrak{d}}) = \mathfrak{d} \cdot J^2$ for some fractional ideal J of the field K. We can take $x_{\mathfrak{d}}$ as the $\mathfrak{d}$-adic uniformizer (i.e. $\pi_{\mathfrak{d}} = x_{\mathfrak{d}} \bmod \dot{K}_{\mathfrak{d}}^2$).

Denote $\mathcal{D} = \mathcal{R} \cup \{\mathfrak{d}\}$. Then $C_{\mathcal{D}}/C_{\mathcal{D}}^2 = C_K/C_K^2$ and

$$E_{\mathcal{D}}/\dot{K}^2 = E_K/\dot{K}^2 \oplus \langle x_{\mathfrak{d}} \rangle.$$

Choose a basis $(\mathsf{cl}\,\mathfrak{p}_1, \ldots, \mathsf{cl}\,\mathfrak{p}_l)$ of the group C_K/C_K^2. Let $\mathcal{S} = \mathcal{D} \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\}$. Then $\mathsf{rk}_2\, C_{\mathcal{S}} = 0$ and

$$E_{\mathcal{S}}/\dot{K}^2 = E_{\mathcal{D}}/\dot{K}^2.$$

Of course $\mathcal{S}$ is a sufficiently large set of primes of K.

By Proposition 2.3 there exist $b_1, \ldots, b_l \in \Delta_{\mathcal{D}}$ such that

$$\left(\frac{b_i}{\mathfrak{p}_i}\right) = -1, \quad \left(\frac{b_i}{\mathfrak{p}_j}\right) = 1 \quad \text{for all } i, j \in \{1, \ldots, l\},\ i \neq j.$$

Multiplying $x_{\mathfrak{d}}$ by suitable elements b_i, $i \in \{1, \ldots, l\}$, we can assume that

$$\left(\frac{x_{\mathfrak{d}}}{\mathfrak{p}_i}\right) = 1 \quad \text{for all } i \in \{1, \ldots, l\},$$

i.e. $x_{\mathfrak{d}} \in \dot{K}_{\mathfrak{p}_i}^2$ for $i = 1, \ldots, l$.

3.1. Dyadic prime. We prove the following theorem.

Theorem 3.1. *If* K *is a number field which satisfies* (c1) *and* (c2), *then there exists a self-equivalence* (T, t) *of* K *such that* $\mathcal{W}(T, t) = \{\mathfrak{d}\}$.

Proof. We continue the consideration from the beginning of this section.

First we claim that

$$(a, x_{\mathfrak{d}})_{\mathfrak{d}} = 1 \quad \text{for every } a \in E_{\mathcal{S}}.$$

For every infinite prime ∞_i we have $(a, x_{\mathfrak{d}})_{\infty_i} = 1$, because $x_{\mathfrak{d}}$ is totally positive. If $\mathfrak{q}$ is a nondyadic finite prime, then $a, x_{\mathfrak{d}}$ are $\mathfrak{q}$-adic units modulo $\dot{K}_{\mathfrak{q}}^2$, so $(a, x_{\mathfrak{d}})_{\mathfrak{q}} = 1$. Thus, by Hilbert reciprocity, we obtain $(a, x_{\mathfrak{d}})_{\mathfrak{d}} = 1$, as claimed.

Consequently, $a \neq u_{\mathfrak{d}} \bmod \dot{K}_{\mathfrak{d}}^2$ for every element $a \in E_{\mathcal{S}}$. In particular $u_{\mathfrak{d}} \neq -1 \bmod \dot{K}_{\mathfrak{d}}^2$.

Now we proceed to the construction of a small $\mathcal{S}$-equivalence of K. Define

$$\begin{aligned} &T_{\mathcal{S}} \colon \mathcal{S} \to \mathcal{S}, && T_{\mathcal{S}} = \mathrm{id}_{\mathcal{S}}, \\ &t_{\mathcal{S}} \colon E_{\mathcal{S}}/\dot{K}^2 \to E_{\mathcal{S}}/\dot{K}^2, && t_{\mathcal{S}} = \mathrm{id}_{E_{\mathcal{S}}/\dot{K}^2}, \\ &t_{\mathfrak{q}} \colon \dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2 \to \dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2, && t_{\mathfrak{q}} = \mathrm{id}_{\dot{K}_{\mathfrak{q}}/\dot{K}_{\mathfrak{q}}^2} \quad \text{for every } \mathfrak{q} \in \mathcal{S} \setminus \{\mathfrak{d}\}. \end{aligned}$$

Define a local automorphism $t_{\mathfrak{d}} \colon \dot{K}_{\mathfrak{d}}/\dot{K}_{\mathfrak{d}}^2 \to \dot{K}_{\mathfrak{d}}/\dot{K}_{\mathfrak{d}}^2$ by

$$t_{\mathfrak{d}}(u_{\mathfrak{d}}) = u_{\mathfrak{d}}\pi_{\mathfrak{d}}, \quad t_{\mathfrak{d}}(\pi_{\mathfrak{d}}) = \pi_{\mathfrak{d}}, \quad t_{\mathfrak{d}}(v) = v \quad \text{for every } v \in \langle u_{\mathfrak{d}}, \pi_{\mathfrak{d}} \rangle^{\perp}.$$

Each isomorphism $t_{\mathfrak{q}}$ ($\mathfrak{q} \in \mathcal{S}$) preserves the Hilbert symbol. Indeed, for $\mathfrak{q} \neq \mathfrak{d}$ this is obvious, and for $\mathfrak{q} = \mathfrak{d}$ it follows from Lemma 2.5.

We prove that $(T_{\mathcal{S}}, t_{\mathcal{S}}, \prod_{\mathfrak{q} \in \mathcal{S}} t_{\mathfrak{q}})$ is a small $\mathcal{S}$-equivalence of K, i.e. diagram (2.1) commutes. The equality

$$t_{\mathcal{S}}(a) = t_{\mathfrak{q}}(a) \bmod \dot{K}_{\mathfrak{q}}^2 \quad \text{for every } a \in E_{\mathcal{S}}$$

is obvious for every $\mathfrak{q} \in \mathcal{S} \setminus \{\mathfrak{d}\}$. Finally, the case when $\mathfrak{q} = \mathfrak{d}$ must be examined.

As we have seen, $a \neq u_{\mathfrak{d}} \bmod \dot{K}_{\mathfrak{d}}^2$ for every $a \in E_{\mathcal{S}}$, hence

$$E_{\mathcal{S}} \dot{K}_{\mathfrak{d}}^2 / \dot{K}_{\mathfrak{d}}^2 \subseteq \langle \pi_{\mathfrak{d}} \rangle \oplus \langle u_{\mathfrak{d}}, \pi_{\mathfrak{d}} \rangle^{\perp}.$$

Thus $t_{\mathfrak{d}}(a) = a = t_{\mathcal{S}}(a)$ for every $a \in E_{\mathcal{S}}$.

We have shown that $(T_{\mathcal{S}}, t_{\mathcal{S}}, \prod_{\mathfrak{q} \in \mathcal{S}} t_{\mathfrak{q}})$ is a small $\mathcal{S}$-equivalence of K. By Theorem 2.4 it can be extended to a self-equivalence (T, t) that is tame outside $\mathcal{S}$. Of course (T, t) is also tame on $\mathcal{S} \setminus \mathcal{D}$, because the local isomorphisms $t_{\mathfrak{q}}$ for $\mathfrak{q} \in \mathcal{S} \setminus \mathcal{D}$ are tame. The local isomorphism $t_{\mathfrak{d}}$ is wild, so the dyadic prime $\mathfrak{d}$ is a unique wild prime of (T, t). ∎

3.2. Nondyadic prime. Now we prove the following theorem.

THEOREM 3.2. *If K is a number field which satisfies* (c1) *and* (c2) *and $\mathfrak{p}$ is a finite nondyadic prime such that $\left(\frac{-1}{\mathfrak{p}}\right) = 1$ and $\mathsf{cl}\,\mathfrak{p} \in C_K^2$, then there exists a self-equivalence (T, t) of K such that $\mathcal{W}(T, t) = \{\mathfrak{p}\}$.*

Proof. We continue the consideration from the beginning of this section.

Just as for the dyadic prime $\mathfrak{d}$, we deduce that there exists a totally positive element $x_{\mathfrak{p}} \in \dot{K}^+$ such that $(x_{\mathfrak{p}}) = \mathfrak{p} \cdot I^2$ for some fractional ideal I of K and we take $x_{\mathfrak{p}}$ as the $\mathfrak{p}$-adic uniformizer (i.e. $\pi_{\mathfrak{p}} = x_{\mathfrak{p}} \bmod \dot{K}_{\mathfrak{p}}^2$). Moreover, we can assume that $x_{\mathfrak{p}} \in \dot{K}_{\mathfrak{p}_i}^2$ for $i = 1, \ldots, l$.

Denote $\mathcal{S}_1 = \mathcal{S} \cup \{\mathfrak{p}\}$. Then $\mathsf{rk}_2\, C_{\mathcal{S}_1} = 0$, i.e. $\mathcal{S}_1$ is a sufficiently large set of primes of K. Moreover,

$$E_{\mathcal{S}_1}/\dot{K}^2 = E_{\mathcal{S}}/\dot{K}^2 \oplus \langle x_{\mathfrak{p}} \rangle.$$

We consider two cases.

(I) Assume that $\left(\frac{a}{\mathfrak{p}}\right) = 1$ for every $a \in E_{\mathcal{S}}$. Then we define a triple $(T_{\mathcal{S}_1}, t_{\mathcal{S}_1}, \prod_{\mathfrak{r}\in\mathcal{S}_1} t_{\mathfrak{r}})$ as follows:

$$\begin{aligned} &T_{\mathcal{S}_1}\colon \mathcal{S}_1 \to \mathcal{S}_1, && T_{\mathcal{S}_1} = \mathrm{id}_{\mathcal{S}_1}, \\ &t_{\mathcal{S}_1}\colon E_{\mathcal{S}_1}/\dot{K}^2 \to E_{\mathcal{S}_1}/\dot{K}^2, && t_{\mathcal{S}_1} = \mathrm{id}_{E_{\mathcal{S}_1}/\dot{K}^2}, \\ &t_{\mathfrak{r}}\colon \dot{K}_{\mathfrak{r}}/\dot{K}_{\mathfrak{r}}^2 \to \dot{K}_{\mathfrak{r}}/\dot{K}_{\mathfrak{r}}^2, && t_{\mathfrak{r}} = \mathrm{id}_{\dot{K}_{\mathfrak{r}}/\dot{K}_{\mathfrak{r}}^2} \quad \text{for every } \mathfrak{r} \in \mathcal{S}_1 \setminus \{\mathfrak{p}\}. \end{aligned}$$

Define a local automorphism $t_{\mathfrak{p}}\colon \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2 \to \dot{K}_{\mathfrak{p}}/\dot{K}_{\mathfrak{p}}^2$ by

$$t_{\mathfrak{p}}(u_{\mathfrak{p}}) = u_{\mathfrak{p}}\pi_{\mathfrak{p}}, \qquad t_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = \pi_{\mathfrak{p}}.$$

Each isomorphism $t_{\mathfrak{r}}$ ($\mathfrak{r} \in \mathcal{S}_1$) preserves the Hilbert symbol. Indeed, for $\mathfrak{r} \neq \mathfrak{p}$ this is obvious, and for $\mathfrak{r} = \mathfrak{p}$ it follows from Lemma 2.6.

Observe that diagram (2.1) commutes. Indeed, $t_{\mathcal{S}_1}(a) = t_{\mathfrak{r}}(a) \bmod \dot{K}_{\mathfrak{r}}^2$ for every $a \in E_{\mathcal{S}_1}$ and $\mathfrak{r} \in \mathcal{S}$, by the definitions of $t_{\mathfrak{r}}$ and $t_{\mathcal{S}_1}$.

The assumption $\left(\frac{a}{\mathfrak{p}}\right) = 1$ for every $a \in E_{\mathcal{S}}$ implies that

$$E_{\mathcal{S}}\dot{K}_{\mathfrak{p}}^2 \subseteq \dot{K}_{\mathfrak{p}}^2.$$

Therefore $t_{\mathfrak{p}}(a) = 1 = t_{\mathcal{S}_1}(a)$ for every $a \in E_{\mathcal{S}}$. Of course $t_{\mathfrak{p}}(x_{\mathfrak{p}}) = x_{\mathfrak{p}} = t_{\mathcal{S}_1}(x_{\mathfrak{p}})$, because $\pi_{\mathfrak{p}} = x_{\mathfrak{p}} \bmod \dot{K}_{\mathfrak{p}}^2$.

The triple $(T_{\mathcal{S}_1}, t_{\mathcal{S}_1}, \prod_{\mathfrak{r}\in\mathcal{S}_1} t_{\mathfrak{r}})$ is a small $\mathcal{S}_1$-equivalence of K. By Theorem 2.4 it extends to a self-equivalence (T, t) that is tame outside $\mathcal{S}_1$. Of course (T, t) is also tame on $\mathcal{S}$, because the local isomorphisms $t_{\mathfrak{r}}$ for $\mathfrak{r} \in \mathcal{S}$ are tame. The local isomorphism $t_{\mathfrak{p}}$ is wild, so $\mathfrak{p}$ is a unique wild prime of (T, t).

(II) Now assume that there exists $c \in E_{\mathcal{S}}$ such that $\left(\frac{c}{\mathfrak{p}}\right) = -1$. Then $c = u_{\mathfrak{p}} \bmod \dot{K}_{\mathfrak{p}}^2$ and $c \neq -1$, by assumption. We have the decomposition

$$E_{\mathcal{S}_1}/\dot{K}^2 = E_{\mathcal{S}}/\dot{K}^2 \oplus \langle x_{\mathfrak{p}} \rangle = V \oplus \langle c \rangle \oplus \langle x_{\mathfrak{p}} \rangle,$$

where $\left(\frac{a}{\mathfrak{p}}\right) = 1$ for every $a \in V$, that is, $V\dot{K}_{\mathfrak{p}}^2 \subseteq \dot{K}_{\mathfrak{p}}^2$.

From [LW, Lemma 2.1] it follows that there exist $x_{\mathfrak{q}} \in \dot{K}$ and a prime $\mathfrak{q} \notin \mathcal{S}$ such that

$$\begin{aligned} &x_{\mathfrak{q}} \in \dot{K}_{\mathfrak{r}}^2 && \text{for every } \mathfrak{r} \in \mathcal{S} \setminus \{\mathfrak{d}\}, \\ &x_{\mathfrak{q}} = x_{\mathfrak{p}} \bmod \dot{K}_{\mathfrak{d}}^2, \\ &\mathrm{ord}_{\mathfrak{q}}\, x_{\mathfrak{q}} = 1, \\ &\mathrm{ord}_{\mathfrak{r}}\, x_{\mathfrak{q}} \equiv 0 \pmod 2 && \text{for every } \mathfrak{r} \in \Omega(K) \setminus (\mathcal{S} \cup \{\mathfrak{q}\}). \end{aligned} \tag{3.1}$$

We fix a $\mathfrak{q}$-adic uniformizer $\pi_{\mathfrak{q}} = x_{\mathfrak{q}} \bmod \dot{K}_{\mathfrak{q}}^2$.

Set $\mathcal{S}_1' = \mathcal{S} \cup \{\mathfrak{q}\}$. Then

$$E_{\mathcal{S}_1'}/\dot{K}^2 = E_{\mathcal{S}}/\dot{K}^2 \oplus \langle x_{\mathfrak{q}} \rangle = V \oplus \langle c \rangle \oplus \langle x_{\mathfrak{q}} \rangle.$$

Define

$$(3.2)\qquad \begin{aligned} &T_{\mathcal{S}_1}:\mathcal{S}_1\to\mathcal{S}_1', && T_{\mathcal{S}_1}|_{\mathcal{S}}=\mathrm{id}_{\mathcal{S}},\ T_{\mathcal{S}_1}(\mathfrak{p})=\mathfrak{q},\\ &t_{\mathcal{S}_1}:E_{\mathcal{S}_1}/\dot K^2\to E_{\mathcal{S}_1'}/\dot K^2, && t_{\mathcal{S}_1}|_V=\mathrm{id}_V,\ t_{\mathcal{S}_1}(c)=cx_{\mathfrak{q}},\ t_{\mathcal{S}_1}(x_{\mathfrak{p}})=x_{\mathfrak{q}},\\ &t_{\mathfrak{r}}:\dot K_{\mathfrak{r}}/\dot K_{\mathfrak{r}}^2\to\dot K_{\mathfrak{r}}/\dot K_{\mathfrak{r}}^2, && t_{\mathfrak{r}}=\mathrm{id}_{\dot K_{\mathfrak{r}}/\dot K_{\mathfrak{r}}^2}\quad\text{for every }\mathfrak{r}\in\mathcal{S}\setminus\{\mathfrak{d}\}.\end{aligned}$$

Define a local isomorphism $t_{\mathfrak{p}}\colon \dot K_{\mathfrak{p}}/\dot K_{\mathfrak{p}}^2\to\dot K_{\mathfrak{q}}/\dot K_{\mathfrak{q}}^2$ by

$$t_{\mathfrak{p}}(u_{\mathfrak{p}})=u_{\mathfrak{q}}\pi_{\mathfrak{q}},\quad t_{\mathfrak{p}}(\pi_{\mathfrak{p}})=\pi_{\mathfrak{q}}.$$

Obviously each $t_{\mathfrak{r}}$ ($\mathfrak{r}\in\mathcal{S}\setminus\{\mathfrak{d}\}$) preserves Hilbert symbols. From the choice of $x_{\mathfrak{p}}$ it follows that $(-1,x_{\mathfrak{p}})_{\mathfrak{d}}=1$, so (3.1) gives $(-1,x_{\mathfrak{q}})_{\mathfrak{d}}=1$. Using (3.1) again and Hilbert reciprocity we obtain $(-1,x_{\mathfrak{q}})_{\mathfrak{q}}=1$, and therefore $\left(\frac{-1}{\mathfrak{q}}\right)=1$. From Lemma 2.6 it follows that $t_{\mathfrak{p}}$ also preserves Hilbert symbols.

Now we proceed to the definition of a local isomorphism $t_{\mathfrak{d}}$. For this purpose we use [C1, Lemma 2.9].

Consider the subgroups $H=E_{\mathcal{S}_1}\dot K_{\mathfrak{d}}^2/\dot K_{\mathfrak{d}}^2$ and $H'=E_{\mathcal{S}_1'}\dot K_{\mathfrak{d}}^2/\dot K_{\mathfrak{d}}^2$ of $\dot K_{\mathfrak{d}}/\dot K_{\mathfrak{d}}^2$.

We shall show that $t_{\mathcal{S}_1}$ induces an isomorphism $H\to H'$ that preserves the dyadic Hilbert symbol. Obviously $t_{\mathcal{S}_1}(-1)=-1$, because $-1\in V$.

First we shall show that

$$(3.3)\qquad (y,x_{\mathfrak{p}})_{\mathfrak{d}}=1\quad\text{for every }y\in V\oplus\langle x_{\mathfrak{p}}\rangle.$$

For this purpose, fix $y\in V\oplus\langle x_{\mathfrak{p}}\rangle$. For every finite prime $\mathfrak{r}\in\mathcal{S}\setminus\{\mathfrak{d}\}$ we have $(y,x_{\mathfrak{p}})_{\mathfrak{r}}=1$, because $x_{\mathfrak{p}}$ is an $\mathfrak{r}$-adic square, by the choice of $x_{\mathfrak{p}}$. Moreover, $x_{\mathfrak{p}}$ is totally positive, so $(y,x_{\mathfrak{p}})_{\infty_i}=1$ for $i=1,\dots,r$. If $y\in V\subset\dot K_{\mathfrak{p}}^2$, then $(y,x_{\mathfrak{p}})_{\mathfrak{p}}=1$. However, if $y=x_{\mathfrak{p}}$, then $(y,x_{\mathfrak{p}})_{\mathfrak{p}}=(x_{\mathfrak{p}},x_{\mathfrak{p}})_{\mathfrak{p}}=(-1,x_{\mathfrak{p}})_{\mathfrak{p}}=1$, because by assumption $-1\in\dot K_{\mathfrak{p}}^2$. Then from Hilbert reciprocity we obtain (3.3).

Hence it directly follows that $(y,x_{\mathfrak{q}})_{\mathfrak{d}}=1$ for every $y\in V$, because by the choice of $x_{\mathfrak{q}}$ we have $x_{\mathfrak{q}}=x_{\mathfrak{p}}\bmod\dot K_{\mathfrak{d}}^2$. Moreover, $(x_{\mathfrak{q}},x_{\mathfrak{q}})_{\mathfrak{d}}=(-1,x_{\mathfrak{q}})_{\mathfrak{d}}=(-1,x_{\mathfrak{p}})_{\mathfrak{d}}=1$. As a result we conclude that

$$(3.4)\qquad (y,x_{\mathfrak{q}})_{\mathfrak{d}}=1\quad\text{for every }y\in V\oplus\langle x_{\mathfrak{q}}\rangle.$$

For every $\mathfrak{r}\in\mathcal{S}\setminus\{\mathfrak{d}\}$ we have $(c,x_{\mathfrak{p}})_{\mathfrak{r}}=1$, because $x_{\mathfrak{p}}$ is totally positive and if $\mathfrak{r}$ is a finite prime, then $x_{\mathfrak{p}}$ is an $\mathfrak{r}$-adic square. Then Hilbert reciprocity and the choice of c yield $(c,x_{\mathfrak{p}})_{\mathfrak{d}}=(c,x_{\mathfrak{p}})_{\mathfrak{p}}=-1$. Since $x_{\mathfrak{q}}=x_{\mathfrak{p}}\bmod\dot K_{\mathfrak{d}}^2$, the above equality gives

$$(3.5)\qquad (c,x_{\mathfrak{q}})_{\mathfrak{d}}=(c,x_{\mathfrak{p}})_{\mathfrak{d}}=-1.$$

From the choice of $x_{\mathfrak{q}}$ we directly obtain

$$(V\oplus\langle x_{\mathfrak{p}}\rangle)\dot K_{\mathfrak{d}}^2=(V\oplus\langle x_{\mathfrak{q}}\rangle)\dot K_{\mathfrak{d}}^2.$$

From (3.3) and (3.5) we see that $c\notin(V\oplus\langle x_{\mathfrak{p}}\rangle)\,\dot K_{\mathfrak{d}}^2$, so $c\notin(V\oplus\langle x_{\mathfrak{q}}\rangle)\dot K_{\mathfrak{d}}^2$.

Since $(cx_{\mathfrak{q}}, x_{\mathfrak{q}})_{\mathfrak{d}} = (c, x_{\mathfrak{q}})_{\mathfrak{d}}(x_{\mathfrak{q}}, x_{\mathfrak{q}})_{\mathfrak{d}} = -1$, we have $cx_{\mathfrak{q}} \notin (V \oplus \langle x_{\mathfrak{q}} \rangle)\dot{K}_{\mathfrak{d}}^2$. This yields the decomposition

$$E_{\mathcal{S}_1}\dot{K}_{\mathfrak{d}}^2 = (V \oplus \langle x_{\mathfrak{p}} \rangle)\dot{K}_{\mathfrak{d}}^2 \oplus \langle c \rangle \dot{K}_{\mathfrak{d}}^2,$$

and similarly

$$E_{\mathcal{S}_1'}\dot{K}_{\mathfrak{d}}^2 = (V \oplus \langle x_{\mathfrak{q}} \rangle)\dot{K}_{\mathfrak{d}}^2 \oplus \langle cx_{\mathfrak{q}} \rangle \dot{K}_{\mathfrak{d}}^2.$$

Note that $x_{\mathfrak{p}} \in V\dot{K}_{\mathfrak{d}}^2$ if and only if $x_{\mathfrak{q}} \in V\dot{K}_{\mathfrak{d}}^2$, and in this case we have $t_{\mathcal{S}_1}(x_{\mathfrak{p}}) = x_{\mathfrak{q}} = x_{\mathfrak{p}} \bmod \dot{K}_{\mathfrak{d}}^2$.

Concluding the above discussion, we see that $t_{\mathcal{S}_1}$ induces an isomorphism of groups $H \to H'$. Moreover, (3.3)–(3.5) show that this isomorphism preserves the $\mathfrak{d}$-adic Hilbert symbol.

Now we show that the remaining assumptions of [C1, Lemma 2.9] hold. For this purpose, we first prove that

$$(y, x_{\mathfrak{d}})_{\mathfrak{d}} = 1 \quad \text{for every } y \in E_{\mathcal{S}}. \tag{3.6}$$

Indeed, $x_{\mathfrak{d}}$ is totally positive, so $(y, x_{\mathfrak{d}})_{\infty_i} = 1$ for every real prime ∞_i. For every finite prime $\mathfrak{r} \in \mathcal{S} \setminus \{\mathfrak{d}\}$ the equality $(y, x_{\mathfrak{d}})_{\mathfrak{r}} = 1$ follows from the fact that $x_{\mathfrak{d}}$ is an $\mathfrak{r}$-adic square. Therefore (3.6) follows by Hilbert reciprocity. This implies that $u_{\mathfrak{d}} \notin E_{\mathcal{S}}\dot{K}_{\mathfrak{d}}^2$.

Now observe that, for every $y \in V \oplus \langle x_{\mathfrak{p}} \rangle$, (3.3) and (3.5) imply that

$$(yc, x_{\mathfrak{p}})_{\mathfrak{d}} = (y, x_{\mathfrak{p}})_{\mathfrak{d}}(c, x_{\mathfrak{p}})_{\mathfrak{d}} = -1.$$

Hence, if $yc \in E_{\mathcal{S}_1}$ is a dyadic unit, then it cannot be a primary unit, i.e. $u_{\mathfrak{d}} \notin E_{\mathcal{S}_1}\dot{K}_{\mathfrak{d}}^2$.

Finally, all assumptions of [C1, Lemma 2.9] hold, so there exists a tame local isomorphism $t_{\mathfrak{d}} \colon \dot{K}_{\mathfrak{d}}/\dot{K}_{\mathfrak{d}}^2 \to \dot{K}_{\mathfrak{d}}/\dot{K}_{\mathfrak{d}}^2$ that preserves the $\mathfrak{d}$-adic Hilbert symbol and is an extension of $t_{\mathcal{S}_1}$.

We shall prove that $(T_{\mathcal{S}_1}, t_{\mathcal{S}_1}, \prod_{\mathfrak{q} \in \mathcal{S}_1} t_{\mathfrak{q}})$ is a small $\mathcal{S}_1$-equivalence.

It suffices to show that diagram (2.1) commutes. The equality $t_{\mathcal{S}_1}(a) = t_{\mathfrak{d}}(a) \bmod \dot{K}_{\mathfrak{d}}^2$ for every $a \in E_{\mathcal{S}_1}$ follows from the definition of $t_{\mathfrak{d}}$ as an extension of $t_{\mathcal{S}_1}$.

Fix $\mathfrak{r} \in \mathcal{S}_1 \setminus \{\mathfrak{d}\}$. The equality $t_{\mathcal{S}_1}(a) = t_{\mathfrak{r}}(a) \bmod \dot{K}_{\mathfrak{r}}^2$ for every $a \in V \oplus \langle x_{\mathfrak{p}} \rangle$ follows from the definitions of $t_{\mathcal{S}_1}$ and $t_{\mathfrak{r}}$, from the fact that $\left(\frac{a}{\mathfrak{p}}\right) = 1$ for $a \in V$, and from the fact that $x_{\mathfrak{p}}, x_{\mathfrak{q}} \in \dot{K}_{\mathfrak{r}}^2$ for $\mathfrak{r} \neq \mathfrak{p}$ and $x_{\mathfrak{p}} = \pi_{\mathfrak{p}} \bmod \dot{K}_{\mathfrak{p}}^2$, $x_{\mathfrak{q}} = \pi_{\mathfrak{q}} \bmod \dot{K}_{\mathfrak{q}}^2$. Moreover, $t_{\mathcal{S}_1}(c) = x_{\mathfrak{q}}c = c = t_{\mathfrak{r}}(c) \bmod \dot{K}_{\mathfrak{r}}^2$ for $\mathfrak{r} \in \mathcal{S}_1 \setminus \{\mathfrak{d}, \mathfrak{p}\}$ and $t_{\mathcal{S}_1}(c) = x_{\mathfrak{q}}c = t_{\mathfrak{p}}(c) \bmod \dot{K}_{\mathfrak{p}}^2$, because $c = u_{\mathfrak{p}} \bmod \dot{K}_{\mathfrak{p}}^2$ and $c = u_{\mathfrak{q}} \bmod \dot{K}_{\mathfrak{q}}^2$.

Using Theorem 2.4 as in (I) we show that there exists a self-equivalence (T, t) of K such that $\mathcal{W}(T, t) = \{\mathfrak{p}\}$. ∎

4. Summary. Now we use the results of the previous section to prove the main result.

Proof of Theorem 1.1. As in [S1] and [S3], we use induction on n.

For $n = 1$ the conclusion follows from Theorems 3.1 and 3.2.

Consider the prime $\mathfrak{p}_1$. If $\mathfrak{d} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, then we assume $\mathfrak{p}_1 = \mathfrak{d}$. Let (T_1, t_1) be a self-equivalence of K as in the proofs of Theorems 3.1, 3.2 and $\mathcal{W}(T_1, t_1) = \{\mathfrak{p}_1\}$.

Let

$$\mathfrak{r}_2 = T_1(\mathfrak{p}_2), \ \ldots, \ \mathfrak{r}_n = T_1(\mathfrak{p}_n).$$

Fix $i \in \{2, \ldots, n\}$. Observe that $\mathfrak{r}_i \notin \mathcal{D}$ (cf. [PSCL, Lemma 4]). Moreover, $\mathsf{cl}\,\mathfrak{r}_i \in C_K^2$. Indeed, from (w2) and Lemma 2.2 it follows that

$$\left(\frac{b}{\mathfrak{p}_i}\right) = 1 \quad \text{for every } b \in \Delta_{\mathcal{D}}.$$

By the proofs of Theorems 3.1 and 3.2,

$$t_1 b = b \quad \text{for every } b \in \Delta_{\mathcal{D}}.$$

Indeed, this is obvious for $t_1 = t$ from the proof of Theorem 3.1 and from the first part of the proof of Theorem 3.2. If $t_1 = t$ is the automorphism from the second part of Theorem 3.2 and $\mathfrak{p}_1 = \mathfrak{p}$, then it suffices to notice that

$$(b, x_{\mathfrak{p}})_{\mathfrak{p}} = (b, x_{\mathfrak{p}})_{\mathfrak{d}} = 1 \quad \text{for every } b \in \Delta_{\mathcal{D}}.$$

Hence $b \in \dot{K}_{\mathfrak{p}}^2$, i.e. $b \in V$. By (3.2), $t_1 b = tb = b$ for every $b \in \Delta_{\mathcal{D}}$.

Using [PSCL, Lemma 4] we get

$$\left(\frac{b}{\mathfrak{r}_i}\right) = 1 \quad \text{for every } b \in \Delta_{\mathcal{D}}.$$

Applying Lemma 2.2 again, we conclude that $\mathsf{cl}\,\mathfrak{r}_i \in C_K^2$.

By assumption $\left(\frac{-1}{\mathfrak{p}_i}\right) = 1$. Obviously $t_1(-1) = -1$, so $\left(\frac{-1}{\mathfrak{r}_i}\right) = 1$.

By inductive assumption there exists a self-equivalence (T_2, t_2) of K such that $\mathcal{W}(T_2, t_2) = \{\mathfrak{r}_2, \ldots, \mathfrak{r}_n\}$. Then $(T_2 \circ T_1, t_2 \circ t_1)$ is a self-equivalence of K such that $\mathcal{W}(T_2 \circ T_1, t_2 \circ t_1) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. ∎

Now assume that $K = \mathbb{Q}(\sqrt{D})$, where $D \neq 1$ is a square-free integer. Denote by γ the number of pairwise distinct prime divisors of the discriminant of K. The Gauss Genus Theorem yields $\mathsf{rk}_2\, C_K^+ = \gamma - 1$. From [RC, Theorem 2.1] it follows that

$$\mathsf{rk}_2\, C_K = \begin{cases} \gamma - 1 & \text{when either } D < 0 \text{ or } \ -1 \in N_{K/\mathbb{Q}}(\dot{K}), \\ \gamma - 2 & \text{when } D > 0 \text{ and } -1 \notin N_{K/\mathbb{Q}}(\dot{K}). \end{cases}$$

Hence K satisfies (c1) if and only if either $D < 0$ or $-1 \in N_{K/\mathbb{Q}}(\dot{K})$.

The field K has a unique dyadic ideal when either $D \equiv 5 \pmod 8$ or $D \equiv 2, 3 \pmod 4$. In the first case the dyadic ideal is the principal ideal generated by 2, so its class is a square in the ideal class group C_K. If $D \equiv 2, 3 \pmod 4$, the dyadic ideal ramifies in K. [C1, Proposition 3.3] implies that the class of this dyadic ideal is a square in C_K if and only if $2 \in |N_{K/\mathbb{Q}}(\dot{K})|$.

We have proven the following theorem.

THEOREM 4.1. *Assume that $K = \mathbb{Q}(\sqrt{D})$, where $D \neq 1$ is a square-free integer. Then*

- (c1) $\Leftrightarrow$ *either* $D < 0$ *or* $-1 \in N_{K/\mathbb{Q}}(\dot{K})$,
- (c2) $\Leftrightarrow$ *either* $D \equiv 5 \pmod 8$ *or* ($D \equiv 2, 3 \pmod 4$ *and* $2 \in |N_{K/\mathbb{Q}}(\dot{K})|$).

The conditions $-1 \in N_{K/\mathbb{Q}}(\dot{K})$ and $2 \in |N_{K/\mathbb{Q}}(\dot{K})|$ can be easily formulated in terms of arithmetical properties of prime divisors of D:

(1) $-1 \in N_{K/\mathbb{Q}}(\dot{K}) \Leftrightarrow D > 0$ and $p \equiv 1, 2 \pmod 4$ for every prime $p \mid D$.
(2) $2 \in N_{K/\mathbb{Q}}(\dot{K}) \Leftrightarrow p \equiv 1, 2, 7 \pmod 8$ for every prime $p \mid D$.
(3) $-2 \in N_{K/\mathbb{Q}}(\dot{K}) \Leftrightarrow D > 0$ and $p \equiv 1, 2, 3 \pmod 8$ for every prime $p \mid D$.

We now show how to verify conditions (w1) and (w2) for a given nondyadic finite prime $\mathfrak{p}$ of K. If $\mathfrak{p}$ lies over a prime number p, then

$$\left(\frac{-1}{\mathfrak{p}}\right) = 1 \;\Leftrightarrow\; \text{either } \left(\frac{-1}{p}\right) = 1 \text{ or } \left(\frac{-D}{p}\right) = 1.$$

From [C1, Proposition 3.3] it follows that

$$\mathsf{cl}\,\mathfrak{p} \in C_K^2 \;\Leftrightarrow\; N_{K/\mathbb{Q}}(\mathfrak{p}) \in |N_{K/\mathbb{Q}}(\dot{K})|.$$

5. Final remark. It is an interesting problem to find sufficient conditions for a finite set of finite primes of K to be a wild set of some self-equivalence of K. A partial answer is provided by the following two theorems. However, in general the problem remains open.

THEOREM 5.1. *Let K be a number field. If (T, t) is a self-equivalence of K, then $\left(\frac{-1}{\mathfrak{p}}\right) = 1$ for every nondyadic prime $\mathfrak{p} \in \mathcal{W}(T, t)$.*

Proof. The argument is due to [S3, p. 2079]. Suppose $\left(\frac{-1}{\mathfrak{p}}\right) = -1$. Then $-1 = u_{\mathfrak{p}}$ is a $\mathfrak{p}$-primary unit and we have

$$(-1, y)_{\mathfrak{p}} = (y, y)_{\mathfrak{p}} = (ty, ty)_{T\mathfrak{p}} = (-1, ty)_{T\mathfrak{p}} \qquad \text{for every } y \in \dot{K}.$$

Hence $\left(\frac{-1}{T\mathfrak{p}}\right) = -1$, so $-1 = u_{T\mathfrak{p}}$ is a $T\mathfrak{p}$-primary unit and

$$(-1)^{\operatorname{ord}_{\mathfrak{p}} y} = (-1, y)_{\mathfrak{p}} = (-1, ty)_{T\mathfrak{p}} = (-1)^{\operatorname{ord}_{T\mathfrak{p}} ty} \quad \text{for every } y \in \dot{K}.$$

Therefore

$$\operatorname{ord}_{\mathfrak{p}} y \equiv \operatorname{ord}_{T\mathfrak{p}} ty \pmod 2 \quad \text{for every } y \in \dot{K},$$

which is impossible. ∎

THEOREM 5.2. *Let K be a number field which satisfies conditions* (c1) *and* (c2). *Let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ be a set of finite nondyadic primes of K. If there exists a self-equivalence (T,t) of K such that $\mathcal{W}(T,t) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$, then the classes $\mathsf{cl}\,\mathfrak{p}_1, \ldots, \mathsf{cl}\,\mathfrak{p}_k$ in K are linearly dependent in the group C_K/C_K^2.*

Proof. Suppose that $\mathsf{cl}\,\mathfrak{p}_1, \ldots, \mathsf{cl}\,\mathfrak{p}_k$ are linearly independent in C_K/C_K^2.

We extend $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$ to a set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k, \mathfrak{p}_{k+1}, \ldots, \mathfrak{p}_l\}$ of finite primes of K such that $\mathsf{cl}\,\mathfrak{p}_1, \ldots, \mathsf{cl}\,\mathfrak{p}_l$ form a basis of C_K/C_K^2.

Let $\mathcal{D}$ be the set of all infinite and dyadic primes of K and denote $m = \#\mathcal{D}$. Then $C_{\mathcal{D}}/C_{\mathcal{D}}^2 = C_K/C_K^2$ and $\mathsf{rk}_2\, E_{\mathcal{D}}/\dot{K}^2 = m + l$.

Denote $\mathcal{S} = \mathcal{D} \cup \{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\}$. Then $\mathsf{rk}_2\, C_{\mathcal{S}} = 0$, so $\mathsf{rk}_2\, E_{\mathcal{S}}/\dot{K}^2 = m + l$. Therefore $E_{\mathcal{D}}/\dot{K}^2 = E_{\mathcal{S}}/\dot{K}^2$.

The self-equivalence (T,t) is tame outside $\mathcal{S}$, hence

$$t(E_{\mathcal{S}}/\dot{K}^2) = E_{T\mathcal{S}}/\dot{K}^2.$$

In particular, $\mathsf{rk}_2\, E_{T\mathcal{S}}/\dot{K}^2 = m + l$. The bijection T sends $\mathcal{D}$ onto $\mathcal{D}$ (cf. [PSCL, Lemma 4]), therefore $\mathcal{D} \subset T\mathcal{S}$, so $E_{\mathcal{D}}/\dot{K}^2 \subset E_{T\mathcal{S}}/\dot{K}^2$. This inclusion implies that $E_{T\mathcal{S}}/\dot{K}^2 = E_{\mathcal{D}}/\dot{K}^2$, because $\mathsf{rk}_2\, E_{\mathcal{D}}/\dot{K}^2 = m + l = \mathsf{rk}_2\, E_{T\mathcal{S}}/\dot{K}^2$. We get

$$t(E_{\mathcal{S}}/\dot{K}^2) = E_{\mathcal{D}}/\dot{K}^2. \tag{5.1}$$

From Proposition 2.3 it follows that there exists $b_1 \in \Delta_{\mathcal{D}} \subset E_{\mathcal{S}}$ such that $\left(\frac{b_1}{\mathfrak{p}_1}\right) = -1$, i.e. $b_1 = u_{\mathfrak{p}_1} \bmod \dot{K}_{\mathfrak{p}_1}^2$.

Observe that $tb_1 \in E_{\mathcal{D}}/\dot{K}^2$, by (5.1). Hence tb_1 is a $T\mathfrak{p}_1$-adic unit modulo $\dot{K}_{T\mathfrak{p}_1}^2$.

Using [PSCL, Lemma 4] again, we deduce that $\left(\frac{tb_1}{T\mathfrak{p}_1}\right) = -1$. This means that tb_1 is a $T\mathfrak{p}_1$-primary unit. Therefore

$$(-1)^{\mathrm{ord}_{\mathfrak{p}_1} y} = (b_1, y)_{\mathfrak{p}_1} = (tb_1, ty)_{T\mathfrak{p}_1} = (-1)^{\mathrm{ord}_{T\mathfrak{p}_1} ty} \qquad \text{for every } y \in \dot{K},$$

i.e. $\mathfrak{p}_1$ is a tame prime of (T,t). This is a contradiction. ■

References

[C] J. P. Carpenter, *Finiteness theorems for forms over global fields*, Math. Z. 209 (1992), 153–166.

[C1] A. Czogała, *On reciprocity equivalence of quadratic number fields*, Acta Arith. 58 (1991), 27–46.

[C2] A. Czogała, *Witt rings of Hasse domains of global fields*, J. Algebra 244 (2001), 604–630.

[LW] D. B. Leep and A. R. Wadsworth, *The Hasse norm theorem mod squares*, J. Number Theory 42 (1992), 337–348.

[N] J. Neukirch, *Class Field Theory*, Springer, Berlin, 1986.

[PSCL] R. Perlis, K. Szymiczek, P. Conner and R. Litherland, *Matching Witts with global fields*, in: Contemp. Math. 155, Amer. Math. Soc., 1994, 365–387.

[RC] B. Rothkegel and A. Czogała, *Singular elements and the Witt equivalence of rings of algebraic integers*, Ramanujan J. 17 (2008), 185–217.
[S1] M. Somodi, *A characterization of the finite wild sets of rational self-equivalences*, Acta Arith. 121 (2006), 327–334.
[S2] M. Somodi, *On the size of the wild set*, Canad. J. Math. 55 (2005), 180–203.
[S3] M. Somodi, *Self-equivalences of the Gaussian field*, Rocky Mountain J. Math. 38 (2008), 2077–2089.
[S] K. Szymiczek, *Bilinear Algebra: An Introduction to Algebraic Theory of Quadratic Forms*, Gordon and Breach, Amsterdam, 1997.

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

Received on 11.2.2014
and in revised form on 29.7.2014 (7728)