

## A characterization of the finite wild sets of rational self-equivalences

by

MARIUS SOMODI (Cedar Falls, IA)

**1. Introduction.** In [4] it is shown that two number fields have isomorphic Witt rings of quadratic forms if and only if there is a Hilbert symbol equivalence between them. A *Hilbert symbol equivalence* between two number fields  $K$  and  $L$  is a pair of maps  $(t, T)$ , where  $t : K^*/K^{*2} \rightarrow L^*/L^{*2}$  is a group isomorphism and  $T : \Omega_K \rightarrow \Omega_L$  is a bijection between the sets of finite and infinite primes of  $K$  and  $L$  respectively, such that the Hilbert symbols are preserved: for any  $a, b \in K^*/K^{*2}$  and for any  $P \in \Omega_K$ ,

$$(a, b)_P = (t(a), t(b))_{T(P)}.$$

In 1991 K. Szymiczek ([6]) proved that there is a Hilbert symbol equivalence between two number fields if and only if the two number fields have the same level, the same number of real embeddings, and there is a bijection between the dyadic primes of the two fields such that the corresponding dyadic completions have the same level and degree over the field of dyadic numbers  $\mathbb{Q}_2$ . Thus Hilbert symbol equivalent number fields have the same degree over the field of rational numbers  $\mathbb{Q}$ , so  $\mathbb{Q}$  is the only number field which is Hilbert symbol equivalent with itself. A Hilbert symbol equivalence between  $\mathbb{Q}$  and itself will be called a *rational self-equivalence*.

If  $(t, T)$  is a rational self-equivalence, then  $T$  induces a bijection between the set of prime integers and itself, denoted again by  $T$ . A prime integer  $p$  is called *tame* with respect to  $(t, T)$  if

$$\text{ord}_p(a) \equiv \text{ord}_{T(p)}(t(a)) \pmod{2}$$

for any square class  $a$ , and *wild* if it is not tame ([4]).

The set of wild primes of a Hilbert symbol equivalence is called the *wild set* of the equivalence. In [1] it is shown that between any two Hilbert symbol equivalent number fields there are Hilbert symbol equivalences that have

finite wild sets. In this paper we will investigate rational self-equivalences that have finite wild sets. We will prove the following result:

**THEOREM 1.** *Let  $W$  be a finite set of prime integers. There is a rational self-equivalence that has the set of wild primes equal to  $W$  if and only if no prime in  $W$  is congruent to  $3 \pmod{4}$ .*

Recall that a necessary condition for a finite set of prime ideals of an arbitrary number field  $K$  to be the wild set of a Hilbert symbol equivalence between  $K$  and some number field  $L$  is that  $-1$  is a local square at each non-dyadic prime in that set (see, for instance, the comments following Corollary 5 in [3]). Theorem 1 implies that for the field of rational numbers this condition is also sufficient. In a separate paper we will prove that this condition is sufficient for the field of Gaussian numbers  $\mathbb{Q}(\sqrt{-1})$ . We ask whether any finite set  $W$  of prime ideals of an arbitrary number field  $K$  such that  $-1$  is a local square at each non-dyadic prime in  $W$  is the wild set of a Hilbert symbol equivalence between  $K$  and some number field  $L$ .

**2. Rational self-equivalences.** This section contains basic properties of the self-equivalences of  $\mathbb{Q}$ . Let  $(t, T)$  be a rational self-equivalence. Then  $t : \mathbb{Q}^*/\mathbb{Q}^{*2} \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$  is a group isomorphism, and  $T : \Omega \rightarrow \Omega$  is a bijection from the set of finite and infinite primes of  $\mathbb{Q}$  to itself, such that  $T(2) = 2$  and  $T(\infty) = \infty$ . If  $p$  and  $q$  are two prime integers such that  $T(p) = q$ , then  $t$  induces a local map

$$t_p : \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \rightarrow \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}.$$

Note that  $t_p$  is a group isomorphism that satisfies  $t_p(-1) = -1$  (see [4]). Since  $-1$  is a square in  $\mathbb{Q}_p^*$  if and only if  $p \equiv 1 \pmod{4}$ , it follows that  $p \equiv 1 \pmod{4}$  if and only if  $q \equiv 1 \pmod{4}$ .

If  $p$  is a prime integer, then there is a unique non-trivial square class  $u_p \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$  such that  $\mathbb{Q}_p(\sqrt{u_p})$  is the non-trivial unramified local quadratic extension of  $\mathbb{Q}_p$ .

If  $p = 2$  then

$$\mathbb{Q}_2^*/\mathbb{Q}_2^{*2} = \{1, -1, 5, 3, 2, -2, 10, 6\}$$

and in this case  $u_2 = 5$ .

If  $p \neq 2$  then

$$\mathbb{Q}_p^*/\mathbb{Q}_p^{*2} = \{1, u_p, \pi_p, u_p\pi_p\},$$

with  $\pi_p = \varrho_p(p)$ , where  $\varrho_p : \mathbb{Q}^*/\mathbb{Q}^{*2} \rightarrow \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$  is the projection map.

In all cases,  $u_p$  has the following characteristic property:

$$(1) \quad (u_p, x)_p = (-1)^{\text{ord}_p(x)} \quad \forall x \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}.$$

From now on we will assume that  $(t, T)$  has a finite wild set  $W$ . If  $p$  is a prime integer and  $q = T(p)$  then (1) implies that  $p$  is tame if and only if

$t_p(u_p) = u_q$ . Note that if  $p \equiv 3 \pmod{4}$  then  $-1$  is a non-square unit in  $\mathbb{Q}_p$ . Since  $-1$  is a unit in  $\mathbb{Q}_q$  and  $t_p(-1) = -1$ , we have  $t_p(u_p) \in \{1, u_q\}$ . But  $t_p(u_p) \neq 1$ , hence  $t_p(u_p) = u_q$ . Thus  $p$  is necessarily tame. This proves that all the primes  $p$  that are congruent to  $3 \pmod{4}$  are tame with respect to any rational self-equivalence. Therefore, no element in  $W$  is congruent to  $3 \pmod{4}$ .

Let  $p$  be a prime integer,  $(t, T)$  a rational self-equivalence, and let  $q = T(p)$ . If  $p$  is tame, there are two possible types of local maps  $t_p$ :

- Type A:  $t_p(u_p) = u_q, \quad t_p(\pi_p) = \pi_q;$
- Type B:  $t_p(u_p) = u_q, \quad t_p(\pi_p) = u_q\pi_q.$

If  $p$  is wild, there are four possible types of local maps  $t_p$ :

- Type 1:  $t_p(u_p) = \pi_q, \quad t_p(\pi_p) = u_q;$
- Type 2:  $t_p(u_p) = u_q\pi_q, \quad t_p(\pi_p) = u_q;$
- Type 3:  $t_p(u_p) = u_q\pi_q, \quad t_p(\pi_p) = \pi_q;$
- Type 4:  $t_p(u_p) = \pi_q, \quad t_p(\pi_p) = u_q\pi_q.$

Let  $W = \{p_1, \dots, p_n\}$ . We will regard  $W$  as an ordered set, with the elements of  $W$  listed in a fixed order. For every  $i \in \{1, \dots, n\}$  let  $q_i = T(p_i)$  and  $W' = \{q_1, \dots, q_n\}$ , regarded as an ordered set with the ordering induced by the ordering of  $W$ . Note that  $p_i = 2$  if and only if  $q_i = 2$ . Moreover,  $W'$  is the wild set of the inverse self-equivalence  $(t^{-1}, T^{-1})$ .

In order to avoid multiple subscripts, we will use the following notations: if  $p_j \in W$  and  $p_j \neq 2$  then we will denote the elements of  $\mathbb{Q}_{p_j}^*/\mathbb{Q}_{p_j}^{*2}$  by  $\{1, u_j, \pi_j, u_j\pi_j\}$ , and the elements of  $\mathbb{Q}_{q_j}^*/\mathbb{Q}_{q_j}^{*2}$  by  $\{1, u'_j, \pi'_j, u'_j\pi'_j\}$ . Also, we will write  $t_j$  instead of  $t_{p_j}$ .

Set  $S = \{\infty, 2\} \cup W$  and  $S' = \{\infty, 2\} \cup W'$ , and define the following sets:

$$E(S) = \{x \in \mathbb{Q}^*/\mathbb{Q}^{*2} : \text{ord}_l(x) \equiv 0 \pmod{2}, \forall l \notin S\},$$

$$E(S') = \{y \in \mathbb{Q}^*/\mathbb{Q}^{*2} : \text{ord}_l(y) \equiv 0 \pmod{2}, \forall l \notin S'\}.$$

Both  $E(S)$  and  $E(S')$  are subgroups of  $\mathbb{Q}^*/\mathbb{Q}^{*2}$ . Let  $E(S)^+$  (and  $E(S')^+$ , respectively) be the subgroup of  $E(S)$  (and  $E(S')$ , respectively) that consists of square classes of positive rationals.

For every  $p \in S$ , consider the projection map  $\nu_p : E(S) \rightarrow \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$ . Since  $S$  contains all the wild primes, the isomorphism  $t : \mathbb{Q}^*/\mathbb{Q}^{*2} \rightarrow \mathbb{Q}^*/\mathbb{Q}^{*2}$  induces an isomorphism  $t : E(S) \rightarrow E(S')$  such that the following diagram is commutative:

$$\begin{CD} E(S) @>\nu_p>> \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \\ @VtVV @VVt_pV \\ E(S') @>\nu_q>> \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \end{CD}$$

In fact, if we denote by  $\nu_S : E(S) \rightarrow \prod_{p \in S} \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$  the diagonal map and by  $t_S$  the direct product of all the local maps  $(t_p)_{p \in S}$ , then there is a commutative diagram

$$\begin{CD} E(S) @>\nu_S>> \prod_{p \in S} \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \\ @VtVV @VVt_SV \\ E(S') @>\nu_{S'}>> \prod_{q \in S'} \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \end{CD}$$

Moreover, since  $t(-1) = -1$  we see that  $t$  induces a group isomorphism  $t : E(S)^+ \rightarrow E(S')^+$ .

**3. Dyadic correspondences.** A *correspondence*  $\mathcal{C}$  between two Hilbert symbol equivalent number fields  $K$  and  $L$  is a composite object  $(S, S', T, (t_P)_{P \in S})$ , where  $S$  (and  $S'$ , respectively) is a finite set of primes in  $K$  (and  $L$ , respectively) that contains all the dyadic and infinite primes,  $T : S \rightarrow S'$  is a bijection that maps infinite primes to infinite primes, and dyadic primes to dyadic primes, and for each  $P \in S$ ,  $t_P : K_P^*/K_P^{*2} \rightarrow L_{T(P)}^*/L_{T(P)}^{*2}$  is a group isomorphism that preserves the Hilbert symbols. Any correspondence between two Hilbert symbol equivalent number fields can be extended to a Hilbert symbol equivalence that has a finite wild set ([5]).

In this section we will investigate the possible correspondences between the field of rational numbers  $\mathbb{Q}$  and itself that involve only the infinite prime  $\infty$  and the dyadic prime  $2$ . These correspondences will be called *dyadic correspondences*. Explicitly, a dyadic correspondence is a composite object  $\mathcal{C} = (S, S', T, t_\infty, t_2)$ , where  $S = S' = \{\infty, 2\}$ . In fact, both  $T$  and  $t_\infty$  are the identity maps, so a dyadic correspondence is uniquely determined by the local map  $t_2$ .

To any correspondence one associates a non-negative integer, called the *defect* of the correspondence ([5]). Specifically, if  $t_S$  is the direct product of the maps  $t_P$  with  $P \in S$  and

$$H(S) = \{\bar{x} \in \nu_S(E(S)) : t_S(\bar{x}) \in \nu_{S'}(E(S'))\}$$

then the defect of the correspondence is the number  $\delta = |S| - \text{rk}_2 H(S)$ . Lemma 5 from [4] implies that if the class number  $h_S(K)$  is odd, then  $\nu_S$  is injective. It follows that if the defect of a rational correspondence is 0 then there is a group isomorphism  $t : E(S) \rightarrow E(S')$  that makes the following diagram commutative:

$$\begin{CD} E(S) @>\nu_S>> \prod_{p \in S} \mathbb{Q}_p^*/\mathbb{Q}_p^{*2} \\ @VtVV @VVt_SV \\ E(S') @>\nu_{S'}>> \prod_{q \in S'} \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \end{CD}$$

and the correspondence can be extended tamely to a rational self-equivalence. There are six local maps  $t_2$  that preserve the Hilbert symbols ([2]). Two of them are tame:

$$\begin{aligned} \text{Type A: } & t_2(2) = 2, & t_2(5) = 5; \\ \text{Type B: } & t_2(2) = 10, & t_2(5) = 5. \end{aligned}$$

The other four are wild (and they match the four types of wild local maps presented in the previous section):

$$\begin{aligned} \text{Type 1: } & t_2(5) = 2, & t_2(2) = 5, & t_2(10) = 10; \\ \text{Type 2: } & t_2(5) = 10, & t_2(2) = 5, & t_2(10) = 2; \\ \text{Type 3: } & t_2(5) = 10, & t_2(2) = 2, & t_2(10) = 5; \\ \text{Type 4: } & t_2(5) = 2, & t_2(2) = 10, & t_2(10) = 5. \end{aligned}$$

In [5] it is proved that any correspondence of defect  $\delta$  can be extended to a Hilbert symbol equivalence that has no less than  $\delta + |\text{rk}_2 C_K(S) - \text{rk}_2 C_L(S')|$  additional wild primes. When  $K = L = \mathbb{Q}$ , the second term in the above formula is 0, so any such correspondence can be extended to a rational self-equivalence that has  $\delta$  additional wild primes.

Among the six dyadic correspondences, two have the defect equal to 0 (Type A and Type 3) and four have the defect equal to 1 (Type B, Type 1, Type 2, and Type 4).

The dyadic correspondence of Type A can be extended (tamely) to the identity self-equivalence of  $\mathbb{Q}$ . The dyadic correspondence of Type 3 can be extended tamely to a rational self-equivalence, denoted by  $(t^{(3)}, T^{(3)})$ .

The dyadic correspondences of Types B, 1, 2, and 4 can be extended to self-equivalences that have one additional wild prime (they cannot be extended tamely to Hilbert symbol equivalences). In the remaining part of this section we will show how to accomplish this when considering correspondences of Types 1, 2, and 4.

Let  $q \equiv 5 \pmod{8}$  be any prime integer, and  $S = \{\infty, 2, q\} = S'$ . For each type of dyadic correspondence we will define a wild local map  $t_q : \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \rightarrow \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$  of a certain type. Let  $t_S = \text{id} \times t_2 \times t_q$ . Consider the following diagram:

$$(2) \quad \begin{array}{ccc} E(S) & \xrightarrow{\nu_S} & \mathbb{R}^*/\mathbb{R}^{*2} \times \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \times \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \\ & & \downarrow t_S \\ E(S') & \xrightarrow{\nu_{S'}} & \mathbb{R}^*/\mathbb{R}^{*2} \times \mathbb{Q}_2^*/\mathbb{Q}_2^{*2} \times \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \end{array}$$

TYPE 1. Define  $t_q : \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \rightarrow \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$  as a local wild map of Type 1. Note that  $\nu_S(-1) = (-1, -1, 1)$ ,  $\nu_S(2) = (1, 2, u_q)$ , and  $\nu_S(q) = (1, 5, \pi_q)$  are mapped by  $t_S$  to  $(-1, -1, 1) = \nu_{S'}(-1)$ ,  $(1, 5, \pi_q) = \nu_{S'}(q)$ , and  $(1, 2, u_q) =$

$\nu_{S'}(2)$  respectively, so the defect of this correspondence is equal to 0. Therefore, the correspondence can be extended tamely to a rational self-equivalence denoted by  $(t^{(1)}, T^{(1)})$ .

TYPE 2. Define  $t_q : \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \rightarrow \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$  as a local wild map of Type 4. In this case  $\nu_S(-1) = (-1, -1, 1)$ ,  $\nu_S(2) = (1, 2, u_q)$ , and  $\nu_S(q) = (1, 5, \pi_q)$  are mapped by  $t_S$  to  $(-1, -1, 1) = \nu_{S'}(-1)$ ,  $(1, 5, \pi_q) = \nu_{S'}(q)$ , and  $(1, 10, u_q\pi_q) = \nu_{S'}(2q)$  respectively, so the defect of this correspondence is equal to 0. Hence this correspondence can be extended tamely to a rational self-equivalence denoted by  $(t^{(2)}, T^{(2)})$ .

TYPE 4. Define  $t_q : \mathbb{Q}_q^*/\mathbb{Q}_q^{*2} \rightarrow \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$  as a local wild map of Type 2. The elements  $\nu_S(-1) = (-1, -1, 1)$ ,  $\nu_S(2) = (1, 2, u_q)$ , and  $\nu_S(q) = (1, 5, \pi_q)$  are mapped by  $t_S$  to  $(-1, -1, 1) = \nu_{S'}(-1)$ ,  $(1, 10, u_q\pi_q) = \nu_{S'}(2q)$ , and  $(1, 2, u_q) = \nu_{S'}(2)$  respectively, so the defect of this correspondence is equal to 0. This correspondence can be extended tamely to a rational self-equivalence denoted by  $(t^{(4)}, T^{(4)})$ .

REMARK 2. When constructing these rational self-equivalences, one can use any prime integer  $q$  that is congruent to 5 (mod 8).

**4. The main results.** Let  $(t, T)$  be a rational self-equivalence with wild set  $W$ . In Section 2 we have seen that if  $p \in W$  then either  $p = 2$  or  $p \equiv 1 \pmod{4}$ . Conversely, let  $p$  be a prime that is not congruent to 3 (mod 4). If  $p = 2$ , then the rational self-equivalence  $(t^{(3)}, T^{(3)})$  has the wild set equal to  $\{2\}$ .

PROPOSITION 3. *For any prime  $p \equiv 1 \pmod{4}$  there is a rational self-equivalence that has the wild set equal to  $\{p\}$ .*

*Proof.* We will consider two cases:

CASE 1:  $p \equiv 1 \pmod{8}$ . In this case,  $\theta_2(p) = 1$ . Let  $q \equiv 1 \pmod{8}$  be an arbitrary prime. Let  $S = \{\infty, 2, p\}$ ,  $S' = \{\infty, 2, q\}$ , and define  $\mathcal{C} = (S, S', T, (t_P)_{P \in S})$  as follows:  $T(\infty) = \infty$ ,  $T(2) = 2$ ,  $T(p) = q$ ,  $t_\infty = \text{id}$ ,  $t_2 = \text{id}$ , and  $t_p$  wild of Type 3. Since

$$\begin{aligned} t_S(\nu_S(-1)) &= t_S(-1, -1, 1) = (-1, -1, 1) = \nu_{S'}(-1), \\ t_S(\nu_S(2)) &= t_S(1, 2, 1) = (1, 2, 1) = \nu_{S'}(2), \\ t_S(\nu_S(p)) &= t_S(1, 1, p) = (1, 1, q) = \nu_{S'}(q), \end{aligned}$$

and  $(-1, -1, 1)$ ,  $(1, 2, 1)$ ,  $(1, 1, p)$  are independent over  $\mathbb{F}_2$ , it follows that the defect of this correspondence is equal to 0. Therefore,  $\mathcal{C}$  can be extended tamely to a rational self-equivalence. The wild set of this self-equivalence is  $W = \{p\}$ .

CASE 2:  $p \equiv 5 \pmod{8}$ . In this case,  $\theta_2(p) = 5$ . Let  $q \equiv 5 \pmod{8}$  be an arbitrary prime. Let  $S = \{\infty, 2, p\}$ ,  $S' = \{\infty, 2, q\}$ , and define  $\mathcal{C} = (S, S', T, (t_P)_{P \in S})$  as follows:  $T(\infty) = \infty$ ,  $T(2) = 2$ ,  $T(p) = q$ ,  $t_\infty = \text{id}$ ,  $t_2$  tame of Type B, and  $t_p$  wild of Type 3. Since

$$\begin{aligned} t_S(\nu_S(-1)) &= t_S(-1, -1, 1) = (-1, -1, 1) = \nu_{S'}(-1), \\ t_S(\nu_S(2)) &= t_S(1, 2, u_p) = (1, 10, u_q q) = \nu_{S'}(2q), \\ t_S(\nu_S(p)) &= t_S(1, 5, p) = (1, 5, q) = \nu_{S'}(q), \end{aligned}$$

and  $(-1, -1, 1)$ ,  $(1, 2, u_p)$ ,  $(1, 5, p)$  are independent over  $\mathbb{F}_2$ , it follows that the defect of this correspondence is equal to 0. Therefore,  $\mathcal{C}$  can be extended tamely to a rational self-equivalence whose wild set is  $W = \{p\}$ .

**COROLLARY 4.** *For any prime  $p$  that is not congruent to  $3 \pmod{4}$  there are infinitely many rational self-equivalences for which  $p$  is the only wild prime.*

*Proof.* If  $p \equiv 1 \pmod{4}$  then the proof of Proposition 3 and Remark 2 show that infinitely many rational self-equivalences (one for each  $q$ ) have the wild set equal to  $\{p\}$ .

If  $p = 2$ , let  $q$  be an arbitrary prime that is congruent to  $5 \pmod{8}$ . Let  $S = \{\infty, 2, 5\}$ ,  $S' = \{\infty, 2, q\}$ , and define  $\mathcal{C} = (S, S', T, (t_P)_{P \in S})$  as follows:  $T(\infty) = \infty$ ,  $T(2) = 2$ ,  $T(5) = q$ ,  $t_\infty = \text{id}$ ,  $t_2$  wild of Type 3, and  $t_q : \mathbb{Q}_5^*/\mathbb{Q}_5^{*2} \rightarrow \mathbb{Q}_q^*/\mathbb{Q}_q^{*2}$  tame of Type B.

Note that  $t_S$  sends  $\nu_S(-1) = (-1, -1, 1)$ ,  $\nu_S(2) = (1, 2, u)$ , and  $\nu_S(5) = (1, 5, \pi)$ , to  $(-1, -1, 1) = \nu_{S'}(-1)$ ,  $(1, 2, u) = \nu_{S'}(2)$ , and  $(1, 10, u\pi) = \nu_{S'}(2q)$  respectively, so the defect of this correspondence is equal to 0. Therefore, the correspondence can be extended tamely to a rational self-equivalence. Note that different primes  $q$  produce different rational self-equivalences, so there are infinitely many rational self-equivalences with wild set equal to  $\{2\}$ .

*Proof of Theorem 1.* We will prove by induction that for any  $n \geq 1$  and any set  $W$  of  $n$  prime integers not congruent to  $3 \pmod{4}$ , there is a self-equivalence with wild set equal to  $W$ .

If  $n = 1$  then for any set  $W$  that consists of one prime not congruent to  $3 \pmod{4}$ , use Proposition 3 to construct a self-equivalence with wild set equal to  $W$ .

Suppose that any set of  $n$  primes not congruent to  $3 \pmod{4}$  is the wild set of a rational self-equivalence; we will prove that any set of  $n + 1$  primes not congruent to  $3 \pmod{4}$  is the wild set of a rational self-equivalence. Let  $W = \{p_1, \dots, p_n, p_{n+1}\}$  be an arbitrary set of primes not congruent to  $3 \pmod{4}$ , and let  $W_n = \{p_1, \dots, p_n\}$ . From the induction hypothesis, there is a rational self-equivalence  $(t, T)$  with wild set equal to  $W_n$ . Let

$q_{n+1} = T(p_{n+1})$ . Use Proposition 3 to construct a rational self-equivalence  $(t', T')$  with wild set equal to  $\{q_{n+1}\}$ .

We claim that  $(t't, T'T')$  is a rational self-equivalence with wild set equal to  $W$ . Indeed,  $(t't)_{p_k} = t'_{T(p_k)}t_{p_k}$  is the composition of a tame map  $(t'_{T(p_k)})$  with a wild map  $(t_{p_k})$ , so  $p_k$  is wild for any  $k \in \{1, \dots, n\}$ . Similarly,  $(t't)_{p_{n+1}} = t'_{T(p_{n+1})}t_{p_{n+1}}$  is the composition of a wild map  $(t'_{T(p_{n+1})})$  with a tame map  $(t_{p_{n+1}})$ , so  $p_{n+1}$  is wild. Finally, if  $q \notin W$  then  $(t't)_q = t'_{T(q)}t_q$  is the composition of two tame maps, so  $q$  is tame.

**COROLLARY 5.** *Any finite set of prime integers that are not congruent to 3 (mod 4) is the wild set of infinitely many rational self-equivalences.*

**Acknowledgments.** The author wishes to thank P. E. Conner for sharing some of his ideas about rational self-equivalences.

### References

- [1] J. Carpenter, *Finiteness theorems for forms over global fields*, Math. Z. 209 (1992), 153–166.
- [2] P. E. Conner, personal communication.
- [3] P. E. Conner, R. Perlis and K. Szymiczek, *Wild sets and 2-ranks of class groups*, Acta Arith. 79 (1997), 83–91.
- [4] R. Perlis, K. Szymiczek, P. E. Conner and R. Litherland, *Matching Witts with global fields*, in: Contemp. Math. 155, Amer. Math. Soc., 1994, 365–387.
- [5] M. Somodi, *On the size of the wild set*, Canad. J. Math. 57 (2005), 180–203.
- [6] K. Szymiczek, *Witt equivalence of global fields*, Comm. Algebra 19 (1991), 1125–1149.

Department of Mathematics  
University of Northern Iowa  
Cedar Falls, IA 50614, U.S.A.  
E-mail: somodi@uni.edu

*Received on 8.2.2005  
and in revised form on 4.10.2005*

(4935)