

## WITT EQUIVALENCE OF GLOBAL FIELDS. II: RELATIVE QUADRATIC EXTENSIONS

KAZIMIERZ SZYMICZEK

**ABSTRACT.** This paper explores the consequences of the Hasse Principle for Witt equivalence of global fields in the case of relative quadratic extensions. We are primarily interested in generating the Witt equivalence classes of quadratic extensions of a given number field, and we study the structure of the class, the number of classes, and the structure of the set of classes. Along the way, we reprove several results obtained earlier in the absolute case of the rational ground field, giving unified and short proofs based on the Hasse Principle.

### INTRODUCTION

A fundamental problem in bilinear algebra is to classify fields with respect to Witt equivalence. Recall that two fields are said to be *Witt equivalent*, if their Witt rings of symmetric bilinear forms are isomorphic (this includes fields of characteristic two). The classification problem for Witt rings turns out to be manageable only when restricted to some specific classes of fields such as fields with finite numbers of square classes, or with finite numbers of quaternion algebras, or Pythagorean fields. A complete structure theory has been known so far only for Pythagorean fields with a finite number of square classes.

Global fields (algebraic number and function fields) do not belong to any of the above classes of fields and a recent solution to the classification problem of Witt rings of global fields amounts to the following Hasse Principle (see [P-S-C-L, §6]):

*Two global fields  $K$  and  $L$  are Witt equivalent if and only if there is a bijective matching of primes of  $K$  and  $L$  such that, if the primes  $P$  and  $Q$  correspond to each other, then the completions  $K_P$  and  $L_Q$  are Witt equivalent.*

As a result, Witt equivalence of global function fields is governed by two invariants: the parity of characteristic and the level of the field (cf. [S2]). This is a very simple situation and it allows us to ignore the function fields in the sequel.

A nontrivial consequence of the Hasse Principle is that, for a given number field  $K$ , all finite extensions of  $K$ , of a fixed degree  $n$ , form only a finite number of Witt equivalence classes. In this paper we investigate the number of

---

Received by the editors November 13, 1990 and, in revised form, January 21, 1992 and August 10, 1992.

1991 *Mathematics Subject Classification.* Primary 11E12; Secondary 11E81.

*Key words and phrases.* Witt equivalence, relative quadratic extensions, Hasse principle.

Supported in part by the State Committee for Scientific Research (KBN) of Poland.

those classes and their structure in the case of relative quadratic extensions.

In §1 we study the behavior of invariants of Witt equivalence under quadratic extensions. We show that the Witt equivalence class of  $K(\sqrt{a})$ , where  $K$  is a number field, is completely determined by the class of  $K$ , and by the location of the square class of  $a$  in the completions of  $K$  at dyadic and infinite real primes of  $K$ . Interestingly enough, if the square classes of  $a$  and  $b$  follow the same pattern of location, then not only  $K(\sqrt{a})$  and  $K(\sqrt{b})$ , but also  $K(\sqrt{-a})$  and  $K(\sqrt{-b})$  are Witt equivalent.

The next section is concerned with the number  $w(K, 2)$  of Witt equivalence classes obtained from a given field  $K$  by all quadratic extensions. We give precise bounds for  $w(K, 2)$ , and also we compute  $w(K, 2)$  for several classes of number fields  $K$ , including all quadratic and cubic number fields  $K$ . We also present a complete classification of quartic 2-extensions of the rationals with respect to Witt equivalence.

Section 3 gives criteria for a given Witt equivalence class to come from a class of lower degree fields by quadratic extensions. Classes reachable from exactly one lower class, called here singular classes, are of importance in studying the graph of Witt equivalence classes. The classes of degree  $n$ , and the classes of degree  $2n$  reachable by quadratic extensions, can be naturally viewed as vertices of a bipartite graph. We show in §4 how to compute the number of connected components of this graph.

We use notation and terminology introduced in [S2]. Thus for a given number field  $K$ , we define the Witt equivalence invariant  $S(K)$  to be the following sequence of field invariants:

$$(0.0.1) \quad S(K) = (n, r, s, g; n_1, \dots, n_g; s_1, \dots, s_g),$$

where

$n = [K : \mathbb{Q}]$  is the absolute degree of  $K$ ,

$r$  = number of infinite real primes (real embeddings) of  $K$ ,

$s$  = level of  $K$ , the minimal number of summands in a representation of  $-1$  as a sum of squares, and  $s = 0$  if  $r > 0$ ,

$g$  = number of dyadic primes  $p_1, \dots, p_g$  of  $K$ ,

$n_i = [K_{p_i} : \mathbb{Q}_2]$  is the local degree of the completion  $K_{p_i}$  of  $K$  at  $p_i$ , over the field  $\mathbb{Q}_2$  of 2-adic numbers,

$s_i = s(K_{p_i})$  is the level of  $K_{p_i}$ .

We call  $n_i$  and  $s_i$  the local data at  $p_i$ . In contrast to [S2], we do not require any particular ordering of the local data. The numbering of local degrees and local levels will be determined by the numbering of dyadic primes. Sometimes it is more convenient to write the invariant in the form

$$(0.0.2) \quad S(K) = (n, r, s, g; (n_1, s_1), \dots, (n_g, s_g)),$$

where  $(n_i, s_i)$  is the local data at  $p_i$ . When  $K$  and  $L$  are Witt equivalent, we write  $K \sim L$ . The following three results will be used freely throughout the paper.

**Theorem (0.1)** (Hasse Principle). *For number fields  $K$  and  $L$ ,*

$$K \sim L \text{ if and only if } S(K) = S(L).$$

(Cf. [S2].) Here the equality of Witt equivalence invariants means that the

four global invariants  $n, r, s, g$  are equal for  $K$  and  $L$ , and the local data coincide up to a permutation of the indices.

**Proposition (0.2).** *Let  $K_p$  and  $L_q$  be completions of number fields  $K$  and  $L$  at the dyadic primes  $p$  and  $q$  of  $K$  and  $L$ , respectively.*

*$K_p \sim L_q$  if and only if  $[K_p : \mathbb{Q}_2] = [L_q : \mathbb{Q}_2]$  and  $s(K_p) = s(L_q)$  (cf. [S2, Proposition (1.2)]).*

**Lemma (0.3).** *Let  $J$  be a finite set of primes of a number field  $K$ . For every set  $\{a_p : a_p \in \dot{K}_p, p \in J\}$ , there exists an  $a \in \dot{K} \setminus \pm \dot{K}^2$  such that  $a \in a_p \dot{K}_p^2$  for every  $p \in J$ .*

This follows by a standard application of the approximation theorem and the use of the openness of  $\dot{K}_p^2$  (see [O'M, p. 188], for an argument using those ideas).

### 1. WITT EQUIVALENCE INVARIANT OF A QUADRATIC EXTENSION

We show here how to determine the Witt equivalence invariant for an arbitrary quadratic extension of a number field, and give several applications. We fix an algebraic number field  $K$  and assume that the Witt equivalence invariant  $S(K)$  is given by (0.0.1). The sets of infinite real and dyadic primes of  $K$  will be denoted  $\text{Pr}_\infty K$  and  $\text{Pr}_2 K$ , respectively. Let  $E = K(\sqrt{a})$ , where  $a \in \dot{K} \setminus \dot{K}^2$ , be an arbitrary quadratic extension of  $K$  and let

$$S(E) = (N, R, S, G; N_1, \dots, N_G; S_1, \dots, S_G)$$

be its Witt equivalence invariant.

**Theorem (1.1).** *The invariant  $S(E)$  is determined as follows.*

(1)  $N = 2n$ .

(2)  $R = 2r(a)$ , where  $r(a) := \#\{q \in \text{Pr}_\infty K : a \in \dot{K}_q^2\}$ .

(3)

$$S = \begin{cases} 0 & \text{if } R \neq 0, \\ 1 & \text{if } s = 1 \text{ or } -a \in \dot{K}^2, \\ 4 & \text{if } R = 0 \text{ and } S_j = 4 \text{ for at least one } j, \\ 2 & \text{otherwise.} \end{cases}$$

(4)  $G = g + k(a)$ , where  $k(a) := \#\{p \in \text{Pr}_2 K : a \in \dot{K}_p^2\}$ .

(5) For  $P_j \in \text{Pr}_2 E$  and  $p_i \in \text{Pr}_2 K$ , if  $P_j$  lies above  $p_i$  and  $(N_j, S_j)$  and  $(n_i, s_i)$  are the local data at  $P_j$  and  $p_i$ , resp., then

$$N_j = \begin{cases} n_i & \text{if } a \in \dot{K}_{p_i}^2, \\ 2n_i & \text{if } a \notin \dot{K}_{p_i}^2, \end{cases}$$

$$S_j = \begin{cases} s_i & \text{if } s_i = 1 \text{ or } a \in \dot{K}_{p_i}^2, \\ 1 & \text{if } s_i \neq 1, a \notin \dot{K}_{p_i}^2, \text{ and } -a \in \dot{K}_{p_i}^2, \\ 2 & \text{if } s_i \neq 1, a \notin \dot{K}_{p_i}^2, \text{ and } -a \notin \dot{K}_{p_i}^2. \end{cases}$$

*Proof.* Everything follows from classical number theory. The prime  $p_i$  splits in  $E$  iff the polynomial  $X^2 - a$  splits into linear factors over  $K_{p_i}$ . This explains (4) and the determination of  $N_j$  in (5). The values of  $S_j$  and  $S$  are obtained

by elementary algebra, except  $S = 2$  and  $4$ , obtained from the Hasse Principle (for isotropy of quadratic forms), and  $S_j = 2$ , which follows from the fact that any quadratic extension of a local field splits the unique quaternion division algebra over the field (cf. [L, Lemma 2.14, p. 157 and Example 2.4(7), p. 304]).

*Remark (1.2).* In general,  $E$  can be reached by quadratic extensions from several lower degree subfields of  $E$ . The invariants of those subfields can differ significantly. Thus, for instance, if  $K_1 = \mathbb{Q}(\sqrt{2})$ ,  $K_2 = \mathbb{Q}(\sqrt{-7})$ , then for  $E = K_1(\sqrt{-7}) = K_2(\sqrt{2})$  we have

$$S(E) = (4, 0, 2, 2; 2, 2; 2, 2),$$

$$S(K_1) = (2, 2, 0, 1; 2; 2),$$

$$S(K_2) = (2, 0, 4, 2; 1, 1; 4, 4).$$

Here are two special cases of determining the Witt equivalence invariant that we will use later on.

**Example (1.3).** Suppose  $K$  is a number field with  $-1 \notin \dot{K}^2$ . We arrange the dyadic primes of  $K$  to get  $s_1 = \dots = s_k = 1$ , where  $k = k(-1)$ . Then

$$S(K(\sqrt{-1})) = (2n, 0, 1, g + k; n_1, n_1, \dots, n_k, n_k, 2n_{k+1}, \dots, 2n_g; 1, 1, \dots, 1).$$

**Example (1.4).** Suppose  $K$  is a number field and  $a \in \dot{K} \setminus \pm \dot{K}^2$  is chosen to satisfy  $a \in \dot{K}_q^2$  for every infinite real prime  $q$ , and  $a \in \dot{K}_p^2$  for every dyadic prime  $p$  (see Lemma (0.3)). Then

$$S(K(\sqrt{a})) = (2n, 2r, s, 2g; n_1, n_1, \dots, n_g, n_g; s_1, s_1, \dots, s_g, s_g).$$

Moreover, if  $r \neq 0$ , then each of  $2r, 2g$  is the largest possible value of the invariant assumed on quadratic extensions of  $K$ . If  $r = 0$ , then each of  $s, 2g$  is the largest possible value. Observe also that when the global invariants assume their maximal values, the local degrees and local levels are uniquely determined. Hence, there is exactly one Witt equivalence class of quadratic extensions of  $K$ , where the global invariants  $R, G$  or  $S, G$  assume their maximal values.

Recall that we have agreed to write  $K \sim L$ , when  $K$  and  $L$  are Witt equivalent, i.e., when  $S(K) = S(L)$ .

**Corollary (1.5).** Let  $K$  and  $L$  be Witt equivalent number fields and  $a \in \dot{K}$ . Then

- (1)  $K(\sqrt{-1}) \sim L(\sqrt{-1})$ .
- (2)  $K(\sqrt{-a}) \sim L(\sqrt{-1})$  iff  $a \in \dot{K}^2$ .

In particular,  $K(\sqrt{-a}) \sim K(\sqrt{-1})$  iff  $K(\sqrt{-a}) = K(\sqrt{-1})$ .

*Proof.* (1) follows from the Example (1.3).

(2) If  $a \in \dot{K}^2$ , then (1) applies. So assume  $K(\sqrt{-a}) \sim L(\sqrt{-1})$ . If  $-1 \in \dot{L}^2$ , then  $s(K) = s(L) = 1$ , and we get  $K(\sqrt{a}) \sim L$ . Hence  $a \in \dot{K}^2$ . If  $-1 \notin \dot{L}^2$ , then from  $s(K(\sqrt{-a})) = s(L(\sqrt{-1}))$  it easily follows that  $a \in \dot{K}^2$ .

If  $-1 \notin \dot{K}^2$ , then the Witt equivalence class of  $K(\sqrt{-1})$  contains just one quadratic extension of  $K$ . Extending the terminology introduced by Robert

Perlis in the case  $K = \mathbb{Q}$ , we can say that  $K(\sqrt{-1})$  is a relatively lonely field (lonely among quadratic extensions of  $K$ ).

We will use Theorem (1.1) to compare Witt equivalence classes of quadratic extensions of two number fields  $K$  and  $L$ . It is important to notice that  $S(E)$ , as determined in Theorem (1.1), depends only on  $S(K)$ ,  $r(a)$ , and on whether or not  $\pm a$  is a square at dyadic primes, and in  $K$ . Thus, if  $K \sim L$  and the local square classes of  $a \in \dot{K}$  and  $b \in \dot{L}$  follow the same pattern, we may expect that  $K(\sqrt{a}) \sim L(\sqrt{b})$ . We formalize these ideas as follows.

**Definition (1.6).** Let  $K$  and  $L$  be Witt equivalent number fields. Assume that  $a \in \dot{K}$  and  $b \in \dot{L}$  satisfy the following conditions:

$$(1.6.1) \quad \pm a \in \dot{K}^2 \Leftrightarrow \pm b \in \dot{L}^2,$$

$$(1.6.2) \quad r(\pm a) = r(\pm b).$$

Let  $T: \mathbb{P}_2 K \rightarrow \mathbb{P}_2 L$  be a bijective map such that

$$(1.6.3) \quad K_p \sim L_{Tp} \quad \text{for every } p \in \mathbb{P}_2 K.$$

(I) The map  $T$  is said to *preserve splitting of dyadic primes of  $K$*  if

$$(1.6.4) \quad \pm a \in \dot{K}_p^2 \Leftrightarrow \pm b \in \dot{L}_{Tp}^2 \quad \text{for every } p \in \mathbb{P}_2 K.$$

(II) The map  $T$  is said to *preserve local Witt equivalences* if

$$(1.6.5) \quad K_p(\sqrt{a}) \sim L_{Tp}(\sqrt{b}) \quad \text{for every } p \in \mathbb{P}_2 K.$$

We write  $a \sim b$  if  $a, b$  satisfy (1.6.1), (1.6.2) and there is a map  $T$  satisfying (1.6.3) and (1.6.4). Similarly, we write  $a \approx b$ , if  $a, b$  satisfy (1.6.1), (1.6.2) and there is a map  $T$  satisfying (1.6.3) and (1.6.5).

The condition (1.6.2) is equivalent to  $r(a) = r(b)$ , since

$$r(a) + r(-a) = r(K) = r(L) = r(b) + r(-b).$$

We prefer the formulation (1.6.2) because it makes evident the useful fact that  $a \sim b$  iff  $-a \sim -b$ . Let us also observe that (1.6.4) is equivalent to the following conditions: for every  $p \in \mathbb{P}_2 K$ ,

$$p \text{ splits in } K(\sqrt{\pm a}) \quad \text{iff} \quad Tp \text{ splits in } L(\sqrt{\pm b}).$$

This explains the terminology used in (1.6)(I).

**Proposition (1.7).** Let  $K$  and  $L$  be Witt equivalent number fields and  $a \in \dot{K}$ ,  $b \in \dot{L}$ .

- (1) If  $a \sim b$ , then  $K(\sqrt{a}) \sim L(\sqrt{b})$  and  $K(\sqrt{-a}) \sim L(\sqrt{-b})$ .
- (2) If  $a \approx b$ , then  $K(\sqrt{a}) \sim L(\sqrt{b})$ .

*Proof.* (1) follows from Theorem (1.1) and from the fact that  $a \sim b$  implies  $-a \sim -b$ . (2) follows from the Hasse Principle for Witt equivalence of number fields (Theorem (0.1)).

We will determine the full strength of the relations  $\sim$  and  $\approx$  in Theorem (1.13). First, however, we collect several corollaries to the simpler result in Proposition (1.7). It will be useful to introduce the following notation.

Given a number field  $K$  and a positive integer  $m$ , we write  $\text{Witt}(K, m)$  for the set of all Witt equivalence classes represented by extensions of  $K$  of degree  $m$ :

$$\text{Witt}(K, m) := \{S(E) : E \supset K \text{ and } [E : K] = m\}.$$

Here we identify the Witt equivalence class of  $E$  with its invariant  $S(E)$ . More generally, if  $S$  is any Witt equivalence class, we consider

$$\text{Witt}(S, m) := \{S(E) : E \supset K, [E : K] = m, \text{ and } S(K) = S\},$$

the set of all Witt equivalence classes obtained from all extensions of degree  $m$  of all fields  $K$  in the class  $S$ . Clearly, for any field  $K$ , and any  $m$ , we have

$$\text{Witt}(K, m) \subseteq \text{Witt}(S(K), m).$$

**Corollary (1.8).**  $\text{Witt}(K, 2) = \text{Witt}(S(K), 2)$ , for every number field  $K$ .

*Proof.* Given any field  $L$  with  $L \sim K$ , and any quadratic extension  $L(\sqrt{b})$  of  $L$ , there always exists  $a \in \dot{K}$  such that  $a \sim b$  (by Lemma (0.3)). Then  $L(\sqrt{b}) \sim K(\sqrt{a})$ , by Proposition (1.7).

**Corollary (1.9).** If  $K \sim L$ , then  $\text{Witt}(K, 2) = \text{Witt}(L, 2)$ .

*Proof.*  $\text{Witt}(K, 2) = \text{Witt}(S(K), 2) = \text{Witt}(S(L), 2) = \text{Witt}(L, 2)$ .

If  $K$  and  $L$  are Witt equivalent, then there is an isomorphism  $t: \dot{K}/\dot{K}^2 \rightarrow \dot{L}/\dot{L}^2$  of groups of square classes such that  $t(-1) = -1$  and  $1 \in D_K(a, b)$  if and only if  $1 \in D_L(ta, tb)$ , for all square classes  $a$  and  $b$  in  $\dot{K}$ . Such a map  $t$  is said to be a Harrison map between  $K$  and  $L$  (cf. [P-S-C-L]).

**Corollary (1.10).** If  $K$  and  $L$  are Witt equivalent number fields and  $t$  is a Harrison map between  $K$  and  $L$ , then

$$K(\sqrt{a}) \sim L(\sqrt{ta}) \text{ and } K(\sqrt{-a}) \sim L(\sqrt{-ta}) \text{ for every } a \in \dot{K}.$$

*Proof.*  $a \sim ta$ , by the Hasse Principle (Theorem (0.1)) and Lemma 4 in [P-S-C-L].

An earlier version of this result was obtained by J. Carpenter. She proved that under the assumptions of (1.10), the fields  $K(\sqrt{a})$  and  $L(\sqrt{ta})$  are reciprocity equivalent [C, Corollary 3.4].

**Corollary (1.11).** Let  $a \in \dot{K}$  and  $b \in \dot{L}$  be local squares at every dyadic prime of  $K$  and  $L$ , respectively. Moreover, assume that (1.6.1) and (1.6.2) hold. Then

$$K \sim L \text{ if and only if } K(\sqrt{a}) \sim L(\sqrt{b}).$$

*Proof.* If  $K \sim L$ , then  $a \approx b$ , hence Proposition (1.7) gives the result. If  $K(\sqrt{a}) \sim L(\sqrt{b})$ , then from Theorem (1.1) it follows that  $S(K) = S(L)$ , hence  $K \sim L$ .

**Corollary (1.12)** (A. Czogała [Cz2]). For number fields  $K$  and  $L$ , if  $\text{Witt}(K, 2) = \text{Witt}(L, 2)$ , then  $K \sim L$ .

*Proof.* Choose  $a$  and  $b$  as in Corollary (1.11) and require additionally that  $\pm a \notin \dot{K}^2$  and  $r(a) = r$ . Then the global invariants of  $K(\sqrt{a})$  and  $L(\sqrt{b})$  assume their largest possible values and, by Example (1.4), we must have  $K(\sqrt{a}) \sim L(\sqrt{b})$ . Hence  $K \sim L$ , by Corollary (1.11).

Here is the result explaining the relationship between the two relations  $\sim$  and  $\approx$  introduced in Definition (1.6).

**Theorem (1.13).** *Let  $K$  and  $L$  be Witt equivalent number fields and  $a \in \dot{K}$ ,  $b \in \dot{L}$ . The following statements are equivalent.*

- (I)  $a \sim b$ .
- (II)  $a \approx b$ .
- (III)  $K(\sqrt{a}) \sim L(\sqrt{b})$  and  $K(\sqrt{-a}) \sim L(\sqrt{-b})$ .

*Proof.* (I)  $\Rightarrow$  (II) By (1.6.3) and (1.6.4), the fields in (1.6.5) have equal degrees. Thus it remains to show that they have the same levels, and this follows easily from (1.6.3), (1.6.4), and Theorem (1.1)(5).

(II)  $\Rightarrow$  (III) As we have already observed, (II)  $\Rightarrow K(\sqrt{a}) \sim L(\sqrt{b})$ . The fact that (II)  $\Rightarrow K(\sqrt{-a}) \sim L(\sqrt{-b})$  follows from the following lemma.

**Lemma (1.13.0).** *Let  $p \in \text{Pr}_2 K$ ,  $q \in \text{Pr}_2 L$ ,  $K_p \sim L_q$ ,  $a \in \dot{K}$ ,  $b \in \dot{L}$ . The following are equivalent.*

- (1)  $K_p(\sqrt{a}) \sim L_q(\sqrt{b})$ .
- (2)  $K_p(\sqrt{-a}) \sim L_q(\sqrt{-b})$ .

*Proof of the lemma.* It is sufficient to prove that (1)  $\Rightarrow$  (2). We conclude from (1) that

$$(1.13.1) \quad a \in \dot{K}_p^2 \Leftrightarrow b \in \dot{L}_q^2 \quad \text{and} \quad s(K_p(\sqrt{a})) = s(L_q(\sqrt{b}))$$

and to prove (2), we need

$$(1.13.2) \quad -a \in \dot{K}_p^2 \Leftrightarrow -b \in \dot{L}_q^2 \quad \text{and} \quad s(K_p(\sqrt{-a})) = s(L_q(\sqrt{-b})).$$

If  $s(K_p) = s(L_q) = 1$ , we get immediately (1.13.2) from (1.13.1). So assume that  $s(K_p) = s(L_q) \neq 1$ . If  $a$  and  $b$  are squares at  $p$  and  $q$ , resp., then  $-a$  and  $-b$  are not. So assume that  $a$  and  $b$  are nonsquares at  $p$  and  $q$ , resp. If  $-a \in \dot{K}_p^2$ , then  $1 = s(K_p(\sqrt{a})) = s(L_q(\sqrt{b}))$ , whence  $-b \in \dot{L}_q^2$ . By symmetry,  $-b \in \dot{L}_q^2 \Rightarrow -a \in \dot{K}_p^2$ . It remains to show the equality of levels in (1.13.2), and this follows from the equivalences in (1.13.1) and (1.13.2), and from Theorem (1.1)(5).

Returning now to the proof of Theorem (1.13) we observe that  $a \approx b \Rightarrow -a \approx -b$ , by the lemma. Hence (II)  $\Rightarrow$  (III).

(III)  $\Rightarrow$  (I) Here (1.6.1) follows from (III) and from the fact that Witt equivalence of number fields preserves the field degrees (cf. [S1]). And (1.6.2) follows from (III) and Theorem (1.1)(2). The proof that there exists a map  $T$  preserving the splitting of dyadic primes is much harder. This will be accomplished in two steps.

*Step 1.* If (III) holds, then there are primes  $p \in \text{Pr}_2 K$  and  $q \in \text{Pr}_2 L$  such that simultaneously

$$(1.13.3) \quad K_p \sim L_q, \quad K_p(\sqrt{a}) \sim L_q(\sqrt{b}), \quad K_p(\sqrt{-a}) \sim L_q(\sqrt{-b}).$$

We will show that  $p$  and  $q$  can be chosen from among the primes with minimal degrees. So let  $n_1 = \min\{n_1, \dots, n_g\}$  and suppose there are exactly  $k$  primes  $p_1, \dots, p_k$  and  $q_1, \dots, q_k$  in  $\text{Pr}_2 K$  and  $\text{Pr}_2 L$ , resp., with local degree  $n_1$ .

Consider first the case where one of the  $p_i$ 's, say  $p_1$ , splits in  $K(\sqrt{a})$ . Then the local data  $(n_1, s_1)$  at  $p_1$  produces a pair  $(n_1, s_1), (n_1, s_1)$  of local data at the primes lying above  $p_1$ . Since  $K(\sqrt{a}) \sim L(\sqrt{b})$ , the same pair occurs in

$S(L(\sqrt{b}))$ . By the minimality of  $n_1$ , one such a pair  $(n_1, s_1)$ ,  $(n_1, s_1)$  comes from a split prime  $q_j$ ,  $1 \leq j \leq k$ . Write  $p$  and  $p_1$  and  $q$  for  $q_j$ . Then

$$K_p \sim L_q \quad \text{and} \quad K_p(\sqrt{a}) \sim L_q(\sqrt{b}),$$

and (1.13.3) follows from Lemma (1.13.0).

Now consider the case where all the  $p_1, \dots, p_k$  are nonsplit in  $K(\sqrt{a})$ . By the minimality of  $n_1$ , all the primes  $q_1, \dots, q_k$  are nonsplit in  $L(\sqrt{b})$ . There are two subcases.

*Subcase 1.* All the  $p_1, \dots, p_k$  are nonsplit in  $K(\sqrt{-a})$ . Then, as above, the primes  $q_1, \dots, q_k$  are also nonsplit in  $L(\sqrt{-b})$ . Thus  $\pm a \notin \dot{K}_{p_i}^2$  and  $\pm b \notin \dot{L}_{q_i}^2$  for all  $i$ ,  $1 \leq i \leq k$ . Without loss of generality we can assume that the local data  $(n_i, s_i)$  at  $p_i$  coincides with the local data at  $q_i$ ,  $1 \leq i \leq k$ . Then it follows from Theorem (1.1)(5) that  $s(K_{p_i}(\sqrt{\pm a})) = s(L_{q_i}(\sqrt{\pm b}))$ , and so  $K_{p_i}(\sqrt{\pm a}) \sim L_{q_i}(\sqrt{\pm b})$  for all  $i$ ,  $1 \leq i \leq k$  (which is more than we need, if  $k > 1$ ).

*Subcase 2.*  $p_1$  splits in  $K(\sqrt{-a})$ . The local data  $(n_1, s_1)$ ,  $(n_1, s_1)$  is found in  $S(L(\sqrt{-b}))$  and, by the minimality of  $n_1$ , such a pair can come only from a prime  $q_1$  which splits in  $L(\sqrt{-b})$ . Thus

$$K_{p_1} \sim L_{q_1} \quad \text{and} \quad K_{p_1}(\sqrt{-a}) \sim L_{q_1}(\sqrt{-b}),$$

and again (1.13.3) follows from Lemma (1.13.0).

*Step 2.* Now we prove the existence of a map  $T$  satisfying (1.6.3) and (1.6.4). This will be done by induction on  $g = g(K) = g(L)$ , the number of dyadic primes in  $K$  and  $L$ . If  $g = 1$ , the result follows from the fact that Witt equivalence preserves the number of dyadic primes. So assume  $g > 1$ , and let  $K$  and  $L$  satisfy (III), and  $g(K) = g(L) = g$ . We have

$$S(K) = (n, r, s, g; (n_1, s_1), \dots, (n_g, s_g)) = S(L),$$

where  $(n_i, s_i)$  is the local data at  $p_i \in \text{Pr}_2 K$  and at  $q_i \in \text{Pr}_2 L$ ,  $i = 1, \dots, g$ . Let  $p = p_1$  and  $q = q_1$  be the primes satisfying (1.13.3). Then setting  $TP_1 = q_1$  we get (1.6.3) and (1.6.4) for  $p = p_1$ . Now we show how to extend  $T$  onto  $\text{Pr}_2 K$ . According to Theorem (2.1) in [S2], there exists a number field  $F$  such that

$$S(F) = (n - n_1, n - n_1, 0, g - 1; (n_2, s_2), \dots, (n_g, s_g)),$$

where  $(n_i, s_i)$  is the local data at the dyadic prime  $P_i$  of  $F$ ,  $i = 2, \dots, g$ . Now we pick up  $a_1$  and  $b_1$  in  $\dot{F} \setminus \pm \dot{F}^2$  satisfying

$$\pm a_1 \in \dot{F}_{P_i}^2 \Leftrightarrow \pm a \in \dot{K}_{p_i}^2, \quad \pm b_1 \in \dot{F}_{P_i}^2 \Leftrightarrow \pm b \in \dot{L}_{q_i}^2, \quad i = 2, \dots, g,$$

and  $r(\pm a_1) = r(\pm b_1)$ . The existence of  $a_1$  and  $b_1$  follows from Lemma (0.3). By (III) and Theorem (1.1), this choice of  $a_1$ ,  $b_1$  guarantees that  $F(\sqrt{a_1}) \sim F(\sqrt{b_1})$  and  $F(\sqrt{-a_1}) \sim F(\sqrt{-b_1})$ . But  $g(F) = g - 1$ . Hence by the induction hypothesis there exists a bijective map  $T_1: \text{Pr}_2 F \rightarrow \text{Pr}_2 F$  preserving the splitting of dyadic primes of  $F$ . We define now  $T: \text{Pr}_2 K \rightarrow \text{Pr}_2 L$  by putting  $TP_1 = q_1$ ,  $TP_i = q_j$  if  $T_1 P_i = P_j$ , for  $i = 2, \dots, g$ . Then also  $T$  preserves the splitting of dyadic primes of  $K$ , and the theorem is proved.

The relations  $\sim$  and  $\approx$  have been introduced as possible candidates for a NSC for  $K(\sqrt{a}) \sim L(\sqrt{b})$ . Theorem (1.13) shows that presumably  $\sim$  and  $\approx$



are stronger than we need. In the following example we show that, in general,  $K \sim L$  and  $K(\sqrt{a}) \sim L(\sqrt{b})$  are not strong enough to imply  $a \sim b$ . As Theorem (1.13) shows, to get  $a \sim b$  one needs additionally the Witt equivalence of  $K(\sqrt{-a})$  and  $L(\sqrt{-b})$ .

**Example (1.14).** Let  $K$  and  $L$  be Witt equivalent fields of degree 6 and

$$S(K) = (6, r, 0, 4; (2, 2), (2, 1), (1, 4), (1, 4)) = S(L),$$

where  $r$  is any even number,  $0 \leq r \leq 6$  (the existence of  $K$  and  $L$  follows from Theorem (2.1) in [S2]). Let  $p_1, \dots, p_4$  and  $q_1, \dots, q_4$  be the dyadic primes of  $K$  and  $L$  matching the given local data. Choose  $a \in \dot{K}$  and  $b \in \dot{L}$  satisfying the following conditions:

$a$  and  $b$  are totally positive in  $K$  and  $L$ , resp.,

$$a \in \dot{K}_{p_1}^2, a \notin \dot{K}_{p_i}^2, i = 2, 3, 4, -a \in \dot{K}_{p_i}^2, i = 3, 4,$$

$$b \in \dot{L}_{q_2}^2, b \notin \dot{L}_{q_j}^2, j = 1, 3, 4, -b \in \dot{L}_{q_1}^2, -b \notin \dot{L}_{q_j}^2, j = 3, 4$$

(see Lemma (0.3)). Then according to Theorem (1.1), we have

$$S(K(\sqrt{a})) = (12, 2r, 0, 5; (2, 2), (2, 2), (4, 1), (2, 1), (2, 1)),$$

$$S(L(\sqrt{b})) = (12, 2r, 0, 5; (4, 1), (2, 1), (2, 1), (2, 2), (2, 2)),$$

so that  $K(\sqrt{a}) \sim L(\sqrt{b})$ . Nevertheless, we will show that  $a \not\sim b$ .

Indeed,  $p_1$  and  $q_1$  are the only dyadic primes of  $K$  and  $L$ , resp., with the local data  $(n_1, s_1) = (2, 2)$ , hence for every bijection  $T: \text{Pr}_2 K \rightarrow \text{Pr}_2 L$  satisfying  $K_{p_1} \sim L_{Tp_1}$  we must have  $Tp_1 = q_1$ . However,  $p_1$  splits in  $K(\sqrt{a})$ , while  $q_1$  does not in  $L(\sqrt{b})$ . Similarly, we must have  $Tp_2 = q_2$ , and  $q_2$  splits, while  $p_2$  does not. Thus we have  $K \sim L$ ,  $K(\sqrt{a}) \sim L(\sqrt{b})$  and  $a \not\sim b$ . By Theorem (1.13), also  $K(\sqrt{-a}) \sim L(\sqrt{-b})$ . This last assertion can also be checked directly by observing that the dyadic primes  $p_3$  and  $p_4$  of  $K$  split in  $K(\sqrt{-a})$  producing four dyadic primes of  $K(\sqrt{-a})$  of degree 1, while all the dyadic primes of  $L(\sqrt{-b})$  have degrees  $\geq 2$  (in fact, equal 2).

**Proposition (1.15).** Let  $K$  and  $L$  be Witt equivalent number fields each with  $g$  dyadic primes. If  $g \leq 3$ , then for every  $a \in \dot{K}$ ,  $b \in \dot{L}$  the following are equivalent:

- (1)  $a \sim b$ .
- (2)  $a \approx b$ .
- (3)  $K(\sqrt{a}) \sim L(\sqrt{b})$ .

*Proof.* By Theorem (1.13), we have (1)  $\Leftrightarrow$  (2)  $\Rightarrow$  (3), and it remains to prove that (3)  $\Rightarrow$  (2). So assume (3) holds. Then (1.6.1) and (1.6.2) follow from Theorem (1.1). To establish (1.6.3) and (1.6.5) we will consider separately the cases  $g = 1$ ,  $g = 2$ , and  $g = 3$ . If  $g = 1$ , then  $a \approx b$  follows directly from Theorem (0.1). So assume  $g = 2$  and  $(n_1, s_1)$ ,  $(n_2, s_2)$  are the local data at the dyadic primes  $p_1, p_2$  and  $q_1, q_2$  of  $K$  and  $L$ , respectively.

*Case 1.*  $p_1$  and  $p_2$  split in  $K(\sqrt{a})$ . Then we have  $4 = g(K(\sqrt{a})) = g(L(\sqrt{b}))$ , the latter by (3), and so  $q_1$  and  $q_2$  also split in  $L(\sqrt{b})$ . Clearly,  $p_1 \leftrightarrow q_1$ ,  $p_2 \leftrightarrow q_2$  establishes  $a \approx b$ .

*Case 2.*  $p_1$  and  $p_2$  are nonsplit in  $K(\sqrt{a})$ . Then  $2 = g(K(\sqrt{a})) = g(L(\sqrt{b}))$ . Hence  $q_1$  and  $q_2$  are nonsplit in  $L(\sqrt{b})$ . Let  $(2n_1, S_1)$ ,  $(2n_2, S_2)$  and  $(2n_1, S_1^*)$ ,  $(2n_2, S_2^*)$  be the local data at the dyadic primes of  $K(\sqrt{a})$  and

$L(\sqrt{b})$ , respectively. If  $S_1 = S_1^*$ , then  $S_2 = S_2^*$  by (3) and the Hasse Principle, and  $a \approx b$  follows. Similarly, if  $S_2 = S_2^*$ , then  $a \approx b$  follows. Assume now that  $S_1 \neq S_1^*$  and  $S_2 \neq S_2^*$ . Then we must have

$$(2n_1, S_1) = (2n_2, S_2^*) \quad \text{and} \quad (2n_2, S_2) = (2n_1, S_1^*),$$

so that  $n_1 = n_2$ ,  $S_1 = S_2^*$ , and  $S_2 = S_1^*$ . If  $s_1 = s_2$ , then the matching  $p_1 \leftrightarrow q_2$ ,  $p_2 \leftrightarrow q_1$  establishes  $a \approx b$ . On the other hand,  $s_1 \neq s_2$  and  $n_1 = n_2$  would imply that  $n_1$  is even (for otherwise  $s_1 = s_2 = 4$ ) and so  $s_1 = 1$ ,  $s_2 = 2$ , up to the order of  $p_1$ ,  $p_2$ . Since  $S_1 \leq s_1$ ,  $S_1^* \leq s_1$ , it follows  $S_1 = S_1^* = 1$ , a contradiction.

*Case 3.*  $p_1$  split and  $p_2$  nonsplit in  $K(\sqrt{a})$ . If  $q_1$  splits in  $L(\sqrt{b})$ , then  $q_2$  does not, and  $a \approx b$  follows. If  $q_1$  does not split in  $L(\sqrt{b})$ , the local data at the dyadic primes of  $K(\sqrt{a})$  and  $L(\sqrt{b})$  looks as follows:  $(n_1, s_1)$ ,  $(n_1, s_1)$ ,  $(2n_2, S_2)$  and  $(2n_1, S_1)$ ,  $(n_2, s_2)$ ,  $(n_2, s_2)$ . By (3) and the Hasse Principle, we must have  $(n_1, s_1) = (n_2, s_2)$  and  $(2n_1, S_1) = (2n_2, S_2)$ . Hence  $p_1 \leftrightarrow q_2$ ,  $p_2 \leftrightarrow q_1$  establishes  $a \approx b$ .

Finally, we consider the case  $g = 3$ . Let  $(n_i, s_i)$  be the local data at the dyadic primes  $p_i$  and  $q_i$  of  $K$  and  $L$ , respectively,  $i = 1, 2, 3$ . If for some  $i$ ,  $1 \leq i \leq 3$ , the primes  $p_i$  and  $q_i$  simultaneously split in  $K(\sqrt{a})$  and  $L(\sqrt{b})$ , we set  $TP_i = q_i$  and match the remaining primes as in the case  $g = 2$ . Thus we are left with only two cases.

*Case 1.* All the  $p_i$ 's are nonsplit in  $K(\sqrt{a})$ . By (3), all the  $q_i$ 's are nonsplit in  $L(\sqrt{b})$ . Let  $(2n_i, S_i)$  and  $(2n_i, S_i^*)$  be the local data at the dyadic primes lying above  $p_i$  and  $q_i$ , respectively,  $i = 1, 2, 3$ . Here  $S_i$  and  $S_i^*$  assume the values 1 or 2, and since the sequences  $S_1, S_2, S_3$  and  $S_1^*, S_2^*, S_3^*$  differ only in the order of the entries, we must have  $S_i = S_i^*$  for some  $i$ . Then we set  $TP_i = q_i$  and match the remaining primes as in the case  $g = 2$ .

*Case 2.*  $p_1$  and  $q_2$  split, and  $p_2, p_3, q_1, q_3$  do not split in  $K(\sqrt{a})$  and  $L(\sqrt{b})$ , respectively. Here the local data at the dyadic primes of  $K(\sqrt{a})$  and  $L(\sqrt{b})$  look as follows:

$$\begin{aligned} & (n_1, s_1), (n_1, s_1), (2n_2, S_2), (2n_3, S_3), \\ & (2n_1, S_1^*), (n_2, s_2), (n_2, s_2), (2n_3, S_3^*). \end{aligned}$$

Since these two sequences differ only in the order of the entries, we must have  $(n_1, s_1) = (n_2, s_2)$ . Thus we can put  $TP_1 = q_2$ , and the proof is completed as in the case  $g = 2$ .

**Corollary (1.16).** *Let  $K \sim L$  and  $g(K) = g(L) \leq 3$ . Then for any  $a \in \dot{K}$ ,  $b \in \dot{L}$ ,*

$$(1.16.1) \quad K(\sqrt{a}) \sim L(\sqrt{b}) \quad \text{iff} \quad K(\sqrt{-a}) \sim L(\sqrt{-b}).$$

*In particular, for any nonzero rational numbers  $a, b$ ,*

$$(1.16.2) \quad \mathbb{Q}(\sqrt{a}) \sim \mathbb{Q}(\sqrt{b}) \quad \text{iff} \quad \mathbb{Q}(\sqrt{-a}) \sim \mathbb{Q}(\sqrt{-b}).$$

*Proof.* Combine Theorem (1.13) and Proposition (1.15).

*Remark (1.17).* Since  $g \leq n$ , the conclusions of (1.15) and (1.16) hold when  $K \sim L$  and the degrees of  $K$  and  $L$  are  $\leq 3$ . One can also show that when the degrees of  $K$  and  $L$  are 4 or 5, then the results hold. Thus Example (1.14)

with  $g = 4$  and  $n = 6$ , is a minimal counterexample to the equivalence of (1) and (3) in Proposition (1.15). Let us also mention that an independent proof for (1.16.2) can be obtained from the classification of quadratic number fields with respect to Witt equivalence, as presented in [S2, p. 1143].

Finally, we prove the conclusions of (1.15) and (1.16) in the case where  $K$  and  $L$  are normal extensions of the rationals. In fact, Proposition (1.18) is more general. We need some more notation. We choose and fix a numbering of dyadic primes  $p_1, \dots, p_g$  of  $K$ , and then, for any  $a \in \dot{K}$ , we introduce the set of indices

$$(1.17.1) \quad I_K(a) = I(a) := \{i \in \{1, \dots, g\} : a \in \dot{K}_{p_i}^2\}.$$

We have already used  $k(a) = |I(a)|$ , and we will need the following three cardinalities:

$$(1.17.2) \quad \begin{aligned} A(a) &:= |I(a) \cap I(-a)|, \\ B(a) &:= |I(a) \setminus I(-a)|, \\ C(a) &:= |I(-a) \setminus I(a)|. \end{aligned}$$

**Proposition (1.18).** *Let  $K$  and  $L$  be Witt equivalent number fields,  $a \in \dot{K} \setminus \pm \dot{K}^2$ ,  $b \in \dot{L} \setminus \pm \dot{L}^2$ . If the local degrees of the dyadic primes of  $K$  are all equal, i.e.  $n_1 = \dots = n_g$ , then the following are equivalent:*

- (1)  $a \sim b$ .
- (2)  $K(\sqrt{a}) \sim L(\sqrt{b})$ .
- (3)  $K(\sqrt{-a}) \sim L(\sqrt{-b})$ .
- (4)  $r(a) = r(b)$ ,  $A(a) = A(b)$ ,  $B(a) = B(b)$ ,  $C(a) = C(b)$ .

*Proof.* It follows from Theorem (1.1) that any quadratic extension of  $K$  can have only dyadic primes with local data of one of the following types:

$$\begin{aligned} (n_1, 1), (n_1, 2), (2n_1, 1), (2n_1, 2) & \text{ if } n_1 \text{ is even,} \\ (n_1, 4), (2n_1, 1), (2n_1, 2) & \text{ if } n_1 \text{ is odd.} \end{aligned}$$

Moreover, the numbers of dyadic primes of these types in  $K(\sqrt{a})$  are

$$\begin{aligned} 2A(a), \quad 2B(a), \quad C(a), \quad g - A(a) - B(a) - C(a) & \text{ if } n_1 \text{ is even,} \\ 2B(a), \quad C(a), \quad g - B(a) - C(a) & \text{ if } n_1 \text{ is odd,} \end{aligned}$$

respectively. This proves (2)  $\Leftrightarrow$  (4). But since

$$A(-a) = A(a), \quad B(-a) = C(a), \quad C(-a) = B(a),$$

the same argument shows that (3)  $\Leftrightarrow$  (4). Hence (2)  $\Leftrightarrow$  (3), and so, (1)  $\Leftrightarrow$  (2), by Theorem (1.13).

**Remark (1.19).** The cardinalities  $A$ ,  $B$ ,  $C$  are not, in general, invariants of Witt equivalence. For instance, if  $K$  and  $L$  are the fields in Example (1.14), we have  $K \sim L$ ,  $K(\sqrt{a}) \sim L(\sqrt{b})$  and  $A(a) = 0$ ,  $B(a) = 1$ ,  $C(a) = 2$ , but  $A(b) = 1$ ,  $B(b) = 0$ ,  $C(b) = 1$ . Observe, however, that  $A + B$  and  $A + C$  are invariant under Witt equivalence. For  $A(a) + B(a) = |I(a)| = k(a)$  and

$A(a) + C(a)$  is the increment in the number of local levels equal to 1 when we pass from  $K$  to  $K(\sqrt{a})$ .

## 2. THE NUMBER $w(K, 2)$

This section establishes exact bounds for the number  $w(K, 2) := |\text{Witt}(K, 2)|$  of Witt equivalence classes of all quadratic extensions of a given number field  $K$ . Moreover, we compute  $w(K, 2)$  in several cases, including normal extensions  $K$  of  $\mathbb{Q}$ , and use these results to compute  $w(K, 2)$  for any quadratic and any cubic field  $K$ . We also give a complete classification of quartic 2-extensions of  $\mathbb{Q}$  with respect to Witt equivalence.

We retain the notation of §1, in particular, we will use (1.17.1). For  $a, b \in \dot{K} \setminus \pm \dot{K}^2$  we will write

$$(2.0.1) \quad a \simeq b \quad \text{if } r(a) = r(b), \quad I(a) = I(b), \quad I(-a) = I(-b).$$

This is a special case of Definition (1.6), where  $K = L$  and (1.6.4) is required via the identity map  $T$ . Hence, by Proposition (1.7),

$$(2.0.2) \quad a \simeq b \Rightarrow a \sim b \Rightarrow K(\sqrt{a}) \sim K(\sqrt{b}).$$

We also continue to assume that  $K$  has the Witt equivalence invariant

$$S(K) = (n, r, s, g; (n_1, s_1), \dots, (n_g, s_g)).$$

We will seek an upper bound for  $w(K, 2)$  in the class of number fields  $K$  with fixed values of  $r, g$  and  $k := |I(-1)| = |\{i: s_i = 1\}|$ . For brevity, we denote this class of fields  $C(r, g, k)$ . We also denote  $l := g - k = |\{i: s_i \neq 1\}|$ .

**Theorem (2.1).** *For any number field  $K$  in  $C(r, g, k)$ , we have*

$$w(K, 2) \leq (r + 1)2^k 3^l + 1,$$

and

$$w(K, 2) \leq 2^g, \quad \text{if } -1 \in \dot{K}^2.$$

The bound is attained if and only if the following classification criterion holds: For  $a, b \in \dot{K} \setminus \pm \dot{K}^2$ ,

$$(2.1.1) \quad K(\sqrt{a}) \sim K(\sqrt{b}) \Leftrightarrow a \simeq b.$$

*Proof.* Let  $m$  be an integer and  $I, J$  be subsets of  $\{1, \dots, g\}$ . We call  $(m, I, J)$  an admissible triple, if  $0 \leq m \leq r$  and

$$(2.1.2) \quad I \cap J \subseteq I(-1), \quad I \cap I(-1) = J \cap I(-1).$$

The set of all admissible triples will be denoted  $\text{Adm}(r, g, k)$ . It follows from Lemma (0.3) that for any  $(m, I, J)$  in  $\text{Adm}(r, g, k)$  and for any field  $K$  in  $C(r, g, k)$  there exists  $a \in \dot{K} \setminus \pm \dot{K}^2$  such that

$$(2.1.3) \quad m = r(a), \quad I = I(a), \quad J = I(-a).$$

Moreover, if  $b \in \dot{K} \setminus \pm \dot{K}^2$  is another element satisfying

$$m = r(b), \quad I = I(b), \quad J = I(-b),$$

then  $a \simeq b$ , hence  $K(\sqrt{a}) \sim K(\sqrt{b})$ , by (2.0.2). Thus for every field  $K$  in  $C(r, g, k)$  there is a well-defined surjective map

$$(2.1.4) \quad \begin{aligned} \mu: \text{Adm}(r, g, k) &\rightarrow \text{Witt}(K, 2) \setminus \{S(K(\sqrt{-1}))\}, \\ \mu(m, I, J) &= S(K(\sqrt{a})), \end{aligned}$$

where  $a \in \dot{K} \setminus \pm \dot{K}^2$  satisfies (2.1.3). The bounds for  $w(K, 2)$  will be established when we prove that

$$(2.1.5) \quad |\text{Adm}(r, g, k)| = (r+1)2^k 3^l.$$

If  $I, J$  is a pair of subsets of  $\{1, \dots, g\}$  satisfying (2.1.2), then there are subsets  $A, B, C$  of  $\{1, \dots, g\}$  such that

$$(2.1.6) \quad \begin{aligned} I &= A \cup B, & J &= A \cup C, & A &\subseteq I(-1), \\ B \cap C &= \emptyset, & B \cap I(-1) &= C \cap I(-1) = \emptyset. \end{aligned}$$

Here  $A$  can be any subset of the  $k$ -element set  $I(-1)$ , hence there are  $2^k$  possible choices for  $A$ . Each of these can be combined with a certain number of pairs  $B, C$ , and we will show now that there are exactly  $3^l$  choices for  $B, C$ . For  $I(-1) = \{1, \dots, k\}$ ,  $B$  and  $C$  are contained in the  $l$ -element set  $\{k+1, \dots, g\}$  and  $B \cap C = \emptyset$ . If  $B$  is any of the  $\binom{l}{h}$  subsets containing  $h$  elements, then  $C$  can be chosen as any subset from the remaining  $l-h$  elements left in  $\{k+1, \dots, g\}$ . Thus there are

$$\sum_{h=0}^l \binom{l}{h} 2^{l-h} = (1+2)^l = 3^l$$

pairs  $B, C$  satisfying (2.1.6). Combined with  $2^k$  sets  $A$  and  $r+1$  possible values of  $m$ , this proves (2.1.5).

The attainability statement in Theorem (2.1) follows from the fact that the bounds are attained if and only if the map  $\mu$  in (2.1.4) is injective, and this, in turn, is equivalent to (2.1.1). This proves the theorem.

We can now compute  $w(K, 2)$  for any field  $K$  satisfying (2.1.1). To come up with examples of such fields we prove first the following lemma.

**Lemma (2.2).** *Let  $K$  be a number field with pairwise distinct local dyadic degrees:  $n_i \neq n_j$  for  $i \neq j$ . Then for every  $a, b \in \dot{K}$ ,*

$$K(\sqrt{a}) \sim K(\sqrt{b}) \Rightarrow I(a) = I(b).$$

*Proof.* This is clear if  $a \in \pm \dot{K}^2$  or  $b \in \pm \dot{K}^2$ , so assume that  $a, b \notin \pm \dot{K}^2$ . Suppose  $i \in I(a)$ . Then  $p_i$  splits in  $K(\sqrt{a})$ , and so we have the pair of local data  $(n_i, s_i), (n_i, s_i)$  both in  $S(K(\sqrt{a}))$  and  $S(K(\sqrt{b}))$ . Suppose  $i \notin I(b)$ . Then  $(n_i, s_i)$  does not come from a split prime in  $K(\sqrt{b})$ , since  $n_i \neq n_j$  for  $i \neq j$ . Hence there are two distinct primes  $p_{j_1}$  and  $p_{j_2}$  which do not split in  $K(\sqrt{b})$  and produce the local data  $(2n_{j_1}, S_{j_1}) = (n_i, s_i), (2n_{j_2}, S_{j_2}) = (n_i, s_i)$ . It follows  $n_{j_1} = n_{j_2}$ , contrary to the assumptions. Hence  $i \in I(b)$ . Thus  $I(a) \subseteq I(b)$ , and by symmetry,  $I(a) = I(b)$ .

**Proposition (2.3).** *Let  $K$  be a number field with pairwise distinct local dyadic degrees and at most three dyadic primes. Then (2.1.1) holds, and*

$$w(K, 2) = \begin{cases} (r+1) \cdot 2^k \cdot 3^l + 1, & \text{if } -1 \notin \dot{K}^2, \\ 2^g, & \text{if } -1 \in \dot{K}^2. \end{cases}$$

*Proof.* If  $K(\sqrt{a}) \sim K(\sqrt{b})$ , then  $r(a) = r(b)$  by Theorem (1.1), and  $I(a) = I(b)$ , by Lemma (2.2). Since  $g \leq 3$ , we get  $K(\sqrt{-a}) \sim K(\sqrt{-b})$ , by Corollary (1.16). Hence  $I(-a) = I(-b)$ , by Lemma (2.2). This proves  $a \simeq b$  (cf. (2.0.1)),

and the converse follows from (2.0.2). Thus (2.1.1) holds and Theorem (2.1) yields the result.

*Remark (2.4).* Another possibility to obtain an upper bound for  $w(K, 2)$ , where  $K$  is an arbitrary number field, comes from the fact that if  $c \in K_{\text{sq}}$ , the group of nonzero elements of  $K$ , which are squares at every infinite and every dyadic prime, then  $K(\sqrt{a}) \sim K(\sqrt{ac})$  for every  $a \in \dot{K} \setminus \dot{K}^2$ . This is so, since  $a \sim ac$ , and even  $a \simeq ac$ . Thus we get

$$(2.4.1) \quad w(K, 2) \leq [\dot{K} : K_{\text{sq}}] + 1.$$

The index  $[\dot{K} : K_{\text{sq}}]$  can be computed from the following exact sequence

$$1 \rightarrow K_{\text{sq}} \rightarrow \dot{K} \rightarrow \prod \dot{K}_p / \dot{K}_p^2 \times \prod \dot{K}_q / \dot{K}_q^2 \rightarrow 1$$

where  $p$  and  $q$  range over dyadic and infinite real primes of  $K$ , resp. It follows that  $[\dot{K} : K_{\text{sq}}] = 2^{n+2g+r}$ . As our results show, the upper bound (2.4.1) is never attained.

We now come to a general lower bound for  $w(K, 2)$ .

**Theorem (2.5).** *For any number field  $K$  in  $\mathbf{C}(r, g, k)$ , we have*

$$\begin{aligned} w(K, 2) &\geq (r+1)(k+1)(l+1) + 1, & \text{if } -1 \notin \dot{K}^2, \\ w(K, 2) &\geq g + 1, & \text{if } -1 \in \dot{K}^2. \end{aligned}$$

*The bounds are attained for fields  $K$  with  $k = g$  and pairwise equal local dyadic degrees  $n_1 = \dots = n_g$ , for example, when  $K$  is a normal extension of  $\mathbb{Q}$  and  $s_1 = \dots = s_g = 1$ .*

*Proof.* Consider the map

$$\begin{aligned} \mu_* : \mathbb{Z}_{r+1} \times \mathbb{Z}_{k+1} \times \mathbb{Z}_{l+1} &\rightarrow \text{Witt}(K, 2) \setminus \{\mathbf{S}(K(\sqrt{-1}))\}, \\ \mu_*(m, u, v) &= \mathbf{S}(K(\sqrt{a})), \end{aligned}$$

where  $a \in \dot{K} \setminus \pm \dot{K}^2$  is chosen to satisfy

$$r(a) = m, \quad I(a) = \{1, \dots, u, k+1, \dots, k+v\}, \quad I(-a) = \{1, \dots, u\}.$$

Here  $\mathbb{Z}_{r+1}$  stands for  $\{0, 1, \dots, r\}$ , and the existence of  $a$  follows from Lemma (0.3). We show that the map  $\mu_*$  is injective. So suppose

$$\mu_*(m, u, v) = \mathbf{S}(K(\sqrt{a})) = \mathbf{S}(K(\sqrt{b})) = \mu_*(m_1, u_1, v_1).$$

Then  $m = r(a) = r(b) = m_1$ , by Theorem (1.1),

$$\begin{aligned} k+u &= \text{the number of local levels in } \mathbf{S}(K(\sqrt{a})) \text{ equal to } 1 \\ &= \text{the number of local levels in } \mathbf{S}(K(\sqrt{b})) \text{ equal to } 1 \\ &= k+u_1, \end{aligned}$$

$$u+v = |I(a)| = k(a) = k(b) = |I(b)| = u_1 + v_1,$$

by Theorem (1.1). Hence  $u = u_1$  and  $v = v_1$ . This proves the injectivity of  $\mu_*$ , and so the inequalities in Theorem (2.5) follow.

If  $n_1 = \dots = n_g$  and  $s_1 = \dots = s_g = 1$ , then  $l = 0$ , and for any  $a \in \dot{K} \setminus \pm \dot{K}^2$ ,

$$\mathbf{S}(K(\sqrt{a})) = \mu_*(r(a), k(a), 0).$$

Therefore  $\mu_*$  is bijective and the bounds are attained.

The following theorem computes  $w(K, 2)$  in an important special case including all normal extensions  $K$  of the rationals.

**Theorem (2.6).** *Let  $K$  be a number field in  $C(r, g, k)$  with all the dyadic primes of the same degree, i.e.,  $n_1 = \dots = n_g$ . Then*

$$w(K, 2) = \frac{1}{2}(r+1)(k+1)(l+1)(l+2) + 1, \quad \text{if } -1 \notin \dot{K}^2,$$

$$w(K, 2) = g + 1, \quad \text{if } -1 \in \dot{K}^2.$$

*Proof.* Consider the map

$$\begin{aligned} \mu^* : \text{Witt}(K, 2) \setminus \{S(K(\sqrt{-1}))\} &\rightarrow \mathbb{Z}_{r+1} \times \mathbb{Z}_{k+1} \times \mathbb{Z}_{l+1} \times \mathbb{Z}_{l+1}, \\ \mu^*(S(K(\sqrt{a}))) &= (r(a), A(a), B(a), C(a)), \end{aligned}$$

where  $A, B, C$  are defined as in (1.17.2). By Proposition (1.18), the map  $\mu^*$  is well defined and injective. It remains to determine the image of  $\mu^*$ . We have  $0 \leq r(a) \leq r$ ,  $0 \leq A(a) \leq k$ ,  $0 \leq B(a) \leq l$ ,  $0 \leq C(a) \leq l - B(a)$ . By Lemma (0.3), for any integers  $m, A, B, C$  satisfying

$$(2.6.1) \quad 0 \leq m \leq r, \quad 0 \leq A \leq k, \quad 0 \leq B \leq l, \quad 0 \leq C \leq l - B,$$

there exists an  $a \in \dot{K} \setminus \dot{K}^2$  such that  $\mu^*(S(K(\sqrt{a}))) = (m, A, B, C)$ . Therefore the image of  $\mu^*$  consists of all quadruplets  $(m, A, B, C)$  satisfying (2.6.1), and so we have

$$|\text{Im } \mu^*| = (r+1)(k+1) \cdot \frac{1}{2}(l+1)(l+2).$$

If  $-1 \notin \dot{K}^2$ , then  $w(K, 2) = |\text{Im } \mu^*| + 1$ , and we get the desired result. If  $-1 \in \dot{K}^2$ , then  $r = 0$ ,  $k = g$ ,  $l = 0$ , and

$$w(K, 2) = |\text{Im } \mu^*| = g + 1.$$

**Corollary (2.7).** *Let  $K \in C(r, 1, k)$  be a number field with a unique dyadic prime. Then*

$$w(K, 2) = \begin{cases} 2 & \text{if } -1 \in \dot{K}^2, \\ 2r+3 & \text{if } -1 \notin \dot{K}^2, \quad k=1, \quad l=0, \\ 3r+4 & \text{if } -1 \notin \dot{K}^2, \quad k=0, \quad l=1. \end{cases}$$

As an example,  $w(\mathbb{Q}, 2) = 3r+4 = 7$ . We will go, however, a little deeper, and determine completely the set  $\text{Witt}(\mathbb{Q}, 2)$  using the methods of Proposition (1.18) and Theorem (2.6).

For  $K = \mathbb{Q}$ , we have  $r = 1$ ,  $k = 0$ ,  $l = 1$ , and by the bijectivity of  $\mu^*$ , the Witt equivalence classes of quadratic extensions of  $\mathbb{Q}$  distinct from  $S(\mathbb{Q}(\sqrt{-1}))$  can be matched with the triples,  $m, B, C$  satisfying  $0 \leq m \leq 1$ ,  $0 \leq B \leq 1$ ,  $0 \leq C \leq 1 - B$ . When  $m = 1$ , this gives three possible pairs  $(B, C) = (0, 0), (0, 1), (1, 0)$ , and then  $r(a) = m = 1$ ,  $B(a) = B$ , and  $C(a) = C$  for  $a = 2, 7, 17$ , respectively. Thus the fields  $\mathbb{Q}(\sqrt{a})$ ,  $a = 2, 7, 17$ , represent all possible Witt equivalence classes of real quadratic number fields. By (1.16.2), the values  $a = -2, -7, -17$ , and  $-1$  produce all Witt equivalence classes of nonreal quadratic number fields. In view of this, we get the following description of  $\text{Witt}(\mathbb{Q}, 2)$ .

**Corollary (2.8).**  $\text{Witt}(\mathbb{Q}, 2) = \{S(\mathbb{Q}(\sqrt{a})): a = -1, \pm 2, \pm 7, \pm 17\}$ .

Earlier proofs of this result required the classification of quadratic number fields with respect to reciprocity equivalence, found in [Cz1], and independently

in [C]. Invoking then the fact that reciprocity equivalence of number fields coincides with Witt equivalence (proved in [S1] and in [P-S-C-L]), gives the result.

As an application of Proposition (2.3) and Theorem (2.6) we compute now the number  $w(K, 2)$  for any quadratic, and any cubic number field  $K$ . We use the numbering of classes introduced in [S2]. For quadratic fields the representatives of the classes are as in Corollary (2.8) and the numbers  $w(K, 2)$  have been computed according to Theorem (2.6). For a classification of cubic fields, including a list of representatives of Witt equivalence classes, see [S2]. In Corollary (2.10) the numbers  $w(K, 2)$  in the cases I, IV, V, VIII have been computed according to Theorem (2.6), and in the remaining cases according to Proposition (2.3).

**Corollary (2.9).** *For a quadratic number field  $K$  the number  $w(K, 2)$  is determined as follows:*

$S(K)$	$K \sim \mathbb{Q}(\sqrt{a})$	$r$	$s$	$g$	$n_i$	$s_i$	$k$	$l$	$w(K, 2)$
I	$\mathbb{Q}(\sqrt{17})$	2	0	2	1, 1	4, 4	0	2	19
II	$\mathbb{Q}(\sqrt{2})$	2	0	1	2	2	0	1	10
III	$\mathbb{Q}(\sqrt{7})$	2	0	1	2	1	1	0	7
IV	$\mathbb{Q}(\sqrt{-7})$	0	4	2	1, 1	4, 4	0	2	7
V	$\mathbb{Q}(\sqrt{-2})$	0	2	1	2	2	0	1	4
VI	$\mathbb{Q}(\sqrt{-17})$	0	2	1	2	1	1	0	3
VII	$\mathbb{Q}(\sqrt{-1})$	0	1	1	2	1	1	0	2

**Corollary (2.10).** *For a cubic number field  $K$  the number  $w(K, 2)$  is determined as follows:*

$S(K)$	$r$	$s$	$g$	$n_i$	$s_i$	$k$	$l$	$w(K, 2)$
I	1	0	1	3	4	0	1	7
II	1	0	2	1, 2	4, 1	1	1	13
III	1	0	2	1, 2	4, 2	0	2	19
IV	1	0	3	1, 1, 1	4, 4, 4	0	3	21
V	3	0	1	3	4	0	1	13
VI	3	0	2	1, 2	4, 1	1	1	25
VII	3	0	2	1, 2	4, 2	0	2	37
VIII	3	0	3	1, 1, 1	4, 4, 4	0	3	41

We end this section with some results on quartic fields. As shown in [S2],  $w(4) := |\text{Witt}(\mathbb{Q}, 4)| = 29$ , and the question arises, how many of the 29 quartic Witt equivalence classes can be represented by quartic 2-extensions, i.e., quadratic extensions of quadratic number fields. The only obstacle seems to be the situation where the quartic field  $E$  has two dyadic primes  $p_1$  and  $p_2$  of degrees  $n_1 = 1$ ,  $n_2 = 3$ , since then it is clear that  $E_{p_2}$  is not a 2-extension of  $\mathbb{Q}_2$  (see also Theorem (3.2)). There are exactly three such classes (with  $r = 0, 2, 4$ )



of quartic fields, and one can expect that all the remaining 26 quartic classes can be represented by suitably chosen 2-extensions of  $\mathbb{Q}$ . This has recently been verified by Jakubec and Marko [JM]. We are in a position to give a new and well-motivated proof for this result.

Our aim here is to classify quartic 2-extensions of  $\mathbb{Q}$  with respect to Witt equivalence. First observe that given a quartic 2-extension  $E/\mathbb{Q}$  with an intermediate quadratic number field  $K$ , we use Theorem (1.1) to compute the Witt equivalence invariant  $S(K)$ , and then once again use the same result to compute  $S(E)$ . This solves, in principle, the first part of the classification problem. The second part of the problem is to find a complete list of representatives of Witt equivalence classes of quartic 2-extensions of  $\mathbb{Q}$ . We will show that the representatives can be chosen from among the quadratic extensions of two quadratic fields only, namely  $\mathbb{Q}(\sqrt{17})$  and  $\mathbb{Q}(\sqrt{2})$  (see Corollary (3.13) for an explanation of the role played by these two fields in our problem). This will follow from the following result:

$$(2.10.1) \quad |\text{Witt}(\mathbb{Q}(\sqrt{17}), 2) \cup \text{Witt}(\mathbb{Q}(\sqrt{2}), 2)| = 26.$$

We begin with quadratic extensions of  $K = \mathbb{Q}(\sqrt{17})$ . By Corollary (2.9), we have  $w(K, 2) = 19$  and by Proposition (1.18), the invariants  $r, A, B, C$  classify quadratic extensions of  $K$  with respect to Witt equivalence. According to (2.6.1),  $0 \leq r \leq 2$ ,  $A = 0$ ,  $0 \leq B \leq 2$ ,  $0 \leq C \leq 2 - B$ . In each of these 18 cases we find appropriate  $a \in K \setminus \pm K^2$  satisfying  $r(a) = r$ ,  $B(a) = B$ ,  $C(a) = C$ . Table 1 gives the representatives  $E = K(\sqrt{a}) = \mathbb{Q}(\sqrt{17}, \sqrt{a})$  of the 19 Witt equivalence classes in  $\text{Witt}(K, 2)$  for  $K = \mathbb{Q}(\sqrt{17})$ , and also the values of the invariants  $r(a)$ ,  $B(a)$ ,  $C(a)$  and  $S(E) = (4, r, s, g; (n_i, s_i), 1 \leq i \leq 4)$ .

Finding  $a \in K$  for the 19 cases in the table is quite straightforward. Since  $\sqrt{17} \equiv 1 \pmod{8}$  in  $\mathbb{Q}_2$ , we find easily the residues of the numbers  $x + y\sqrt{17} \pmod{8}$  in  $\mathbb{Q}_2$ , and compute  $B(a)$  and  $C(a)$ . For example, when  $a = 10 + \sqrt{17}$ , we have  $a \equiv 3 \pmod{8}$ ,  $\bar{a} \equiv 1 \pmod{8}$ , bar denoting the conjugation in  $K$ . Thus  $B(a) = 1$  and  $C(a) = 0$ . Another observation is that

$$(2.10.2) \quad B(-a) = C(a) \quad \text{and} \quad C(-a) = B(a),$$

which makes cases 1–6 and 13–18 symmetric to a certain extent. Also the cases 8, 9 and 10, 12 are symmetric, the cases 7 and 11 being self-symmetric. The symmetry reflects the fact that

$$K(\sqrt{a}) \sim K(\sqrt{b}) \quad \text{iff} \quad K(\sqrt{-a}) \sim K(\sqrt{-b})$$

when  $g \leq 3$  (cf. Corollary (1.6) and Proposition (1.18)).

Now, with even less effort, we compile the table (see Table 2) of the 10 representatives of Witt equivalence classes of quadratic extensions of the field  $L = \mathbb{Q}(\sqrt{2})$ . Here the invariants  $r, A, B, C$  assume the values  $0 \leq r \leq 2$ ,  $A = 0$ ,  $0 \leq B \leq 1$ ,  $0 \leq C \leq 1 - B$ . Most of the choices for  $a \in L = \mathbb{Q}(\sqrt{2})$  are obvious. We have  $L_p = \mathbb{Q}_2(\sqrt{2})$ , and so in case 4,  $\pm(1 + \sqrt{2}) \notin \dot{L}_p^2$ , because  $N_{L_p/\mathbb{Q}_2}(1 + \sqrt{2}) = -1 \notin \mathbb{Q}_2^2$ . In case 6, we show that  $X^4 - X^2 + 8$  has a zero  $x \equiv 3 \pmod{4}$  in  $\mathbb{Q}_2$  (by Hensel's lemma), and from this it follows that

$$1 + 4\sqrt{2} = (x + 2\sqrt{2}/x)^2 \in \dot{L}_p^2.$$

TABLE 1

	$r(a)$	$B(a)$	$C(a)$	$r$	$s$	$g$	$n_i$	$s_i$	$a$	$E = K(\sqrt{a})$
1.	2	0	0	4	0	2	2, 2	2, 2	2	$\mathbb{Q}(\sqrt{17}, \sqrt{2})$
2.	2	0	1	4	0	2	2, 2	2, 1	$6 + \sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
3.	2	0	2	4	0	2	2, 2	1, 1	7	$\mathbb{Q}(\sqrt{17}, \sqrt{7})$
4.	2	1	0	4	0	3	1, 1, 2	4, 4, 2	$10 + \sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
5.	2	1	1	4	0	3	1, 1, 2	4, 4, 1	$8 + \sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
6.	2	2	0	4	0	4	1, 1, 1, 1	4, 4, 4, 4	33	$\mathbb{Q}(\sqrt{17}, \sqrt{33})$
7.	1	0	0	2	0	2	2, 2	2, 2	$4 + \sqrt{17}$	$\mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{-a})$
8.	1	0	1	2	0	2	2, 2	2, 1	$-2 - \sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
9.	1	0	2	2	0	2	2, 2	1, 1	$-5 - 4\sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
10.	1	1	0	2	0	3	1, 1, 2	4, 4, 2	$2 + \sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
11.	1	1	1	2	0	3	1, 1, 2	4, 4, 1	$4 + 5\sqrt{17}$	$\mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{-a})$
12.	1	2	0	2	0	4	1, 1, 1, 1	4, 4, 4, 4	$5 + 4\sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
13.	0	0	0	0	2	2	2, 2	2, 2	-2	$\mathbb{Q}(\sqrt{17}, \sqrt{-2})$
14.	0	0	1	0	2	2	2, 2	2, 1	$-10 - \sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
15.	0	0	2	0	2	2	2, 2	1, 1	-33	$\mathbb{Q}(\sqrt{17}, \sqrt{-33})$
16.	0	1	0	0	4	3	1, 1, 2	4, 4, 2	$-6 - \sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
17.	0	1	1	0	4	3	1, 1, 2	4, 4, 1	$-8 - \sqrt{17}$	$\mathbb{Q}(\sqrt{a})$
18.	0	2	0	0	4	4	1, 1, 1, 1	4, 4, 4, 4	-7	$\mathbb{Q}(\sqrt{17}, \sqrt{-7})$
19.	0	0	2	0	1	2	2, 2	1, 1	-1	$\mathbb{Q}(\sqrt{17}, \sqrt{-1})$

TABLE 2

	$r(a)$	$B(a)$	$C(a)$	$r$	$s$	$g$	$n_i$	$s_i$	$a$	$E = L(\sqrt{a})$
1.	2	0	0	4	0	1	4	2	3	$\mathbb{Q}(\sqrt{2}, \sqrt{3})$
2.	2	0	1	4	0	1	4	1	7	$\mathbb{Q}(\sqrt{2}, \sqrt{7})$
3.	2	1	0	4	0	2	2, 2	2, 2	17	$\mathbb{Q}(\sqrt{2}, \sqrt{17})$
4.	1	0	0	2	0	1	4	2	$1 + \sqrt{2}$	$\mathbb{Q}(\sqrt{a}), \mathbb{Q}(\sqrt{-a})$
5.	1	0	1	2	0	1	4	1	$-1 - 4\sqrt{2}$	$\mathbb{Q}(\sqrt{a})$
6.	1	1	0	2	0	2	2, 2	2, 2	$1 + 4\sqrt{2}$	$\mathbb{Q}(\sqrt{a})$
7.	0	0	0	0	2	1	4	2	-3	$\mathbb{Q}(\sqrt{2}, \sqrt{-3})$
8.	0	0	1	0	2	1	4	1	-17	$\mathbb{Q}(\sqrt{2}, \sqrt{-17})$
9.	0	1	0	0	2	2	2, 2	2, 2	-7	$\mathbb{Q}(\sqrt{2}, \sqrt{-7})$
10.	0	0	1	0	1	1	4	1	-1	$\mathbb{Q}(\sqrt{2}, \sqrt{-1})$

We also use the symmetry of the cases 1–3 and 7–9, and of 5 and 6, based on the observation (2.10.2).

Comparing now the Witt's equivalence invariants of the fields  $K(\sqrt{a})$  and  $L(\sqrt{a})$  in the two tables, we find that the tables overlap only in the three cases where  $g = 2$  in Table 2 (cases 1, 7 and 13 in Table 1). This proves (2.10.1) and gives an explicit list of representatives of all the 26 Witt equivalence classes of quartic 2-extensions of the rationals.

## 3. BASIC AND SINGULAR CLASSES

Let  $S$  be a Witt equivalence class of algebraic number fields. In §§1 and 2 we have studied the classes  $T$  in  $\text{Witt}(S, 2)$ , that is, classes coming from quadratic extensions of (fields in) the class  $S$ . Here we consider the dual problem: given a class  $T$ , we ask when, and in how many ways,  $T$  can be reached from classes  $S$  of lower degree by quadratic extensions. We begin with two existence theorems. Below we use the following notations:

$$\begin{aligned} S &= (n, r, s, g; (n_i, s_i), i = 1, \dots, g), \\ T &= (N, R, S, G; (N_j, S_j), j = 1, \dots, G). \end{aligned}$$

**Theorem (3.1).** *Let  $S$  and  $T$  be Witt equivalence classes of algebraic number fields. In order that  $T \in \text{Witt}(S, 2)$  it is necessary and sufficient that*

- (1)  $N = 2n$ .
- (2)  $0 \leq R \leq 2r$ , and if  $r = 0$ , then  $0 \leq S \leq s$ .
- (3)  $g \leq G \leq 2g$ , and there exists an integer  $k$ ,  $0 \leq k \leq g$ , such that after renumbering the local data in  $S$  and  $T$ , if necessary, we have  $N_1 = N_2 = n_1, \dots, N_{2k-1} = N_{2k} = n_k, N_{2k+1} = 2n_{k+1}, \dots, N_G = 2n_g, S_1 = S_2 = s_1, \dots, S_{2k-1} = S_{2k} = s_k, S_{2k+j} \leq s_{k+j}$  for  $j = 1, \dots, g - k$ .
- (4) If  $S = 1$  and  $s \neq 1$ , then  $k = |\{i: s_i = 1\}|$ .

*Proof.* The necessity of these conditions follows from Theorem (1.1). Now we prove the sufficiency. Suppose the conditions (1) through (4) are satisfied and let  $K$  be any field with  $S(K) = S$ . If  $S = 1$  and  $s \neq 1$ , then  $S(K(\sqrt{-1})) = T$ , by Example (1.3). Therefore we can assume that either  $S \neq 1$  or  $s = 1$ . By Lemma (0.3), there is an  $a \in \dot{K} \setminus \pm \dot{K}^2$  such that simultaneously

$$\begin{aligned} I_K(a) &= \{1, 2, \dots, k\}, & r(a) &= \tfrac{1}{2}R, \\ I_K(-a) &= \{i: 1 \leq i \leq k, s_i = 1\} \\ &\cup \{k+j: 1 \leq j \leq g-k, S_{2k+j} = 1 \text{ and } s_{k+j} \neq 1\}. \end{aligned}$$

(Here we use the notation (1.17.1).)

Then  $S(K(\sqrt{a})) = T$ , by Theorem (1.1), and so  $T \in \text{Witt}(K, 2)$ .

**Theorem (3.2).** *Let  $T$  be a given Witt equivalence class of number fields. In order that there exists a Witt equivalence class  $S$  such that  $T \in \text{Witt}(S, 2)$  it is necessary and sufficient that*

- (1)  $N$  is even.
- (2) Every odd local degree  $N_j$  occurs an even number of times.

*Proof.* The necessity of (1) and (2) follows immediately from Theorem (1.1) (or from Theorem (3.1)). To prove sufficiency, we will construct a Witt equivalence class  $S$  such that  $S$  and  $T$  satisfy the conditions (1) through (4) in Theorem (3.1). So assume (1) and (2) in (3.2) hold. We choose  $n := \frac{1}{2}N$ ,  $r := \frac{1}{2}N$  and  $s = 0$ .

If  $2k \geq 0$  is the number of odd local degrees  $N_j$ , we may assume that they are  $N_1, \dots, N_{2k}$  and that  $N_1 = N_2, \dots, N_{2k-1} = N_{2k}$ . Then we put  $n_i := N_{2i}$  for  $i = 1, \dots, k$ , and  $g := G - k$ . The remaining local degrees  $N_{2k+j}$ ,  $j = 1, \dots, g - k$ , are all even, and we put  $n_{k+j} := \frac{1}{2}N_{2k+j}$  for  $j = 1, \dots, g - k$ .

We also set  $s_i = 4$  for  $i = 1, \dots, k$ , and  $s_{k+j} = 2$  for  $j = 1, \dots, g - k$ . If  $S = 1$ , a part of this construction is void. All  $S_j = 1$  and all  $N_j$  are even, hence  $k = 0$ ,  $g = G$  and all  $s_j = 2$ .

It follows that the set  $S = (n, r, s, g; (n_i, s_i), i = 1, \dots, g)$  satisfies the conditions (1)–(4) in Theorem (3.1). Moreover,  $S$  is realizable as the Witt equivalence invariant of a certain number field, according to Theorem (2.1) in [S2]. Hence Theorem (3.1) applies and gives  $T \in \text{Witt}(S, 2)$ , as required.

**Remark (3.3).** The above proof shows that if a class  $T$  is reachable from a lower class by quadratic extensions, then it can be reached from the class of a totally real number field (i.e., from a class with  $r = n$ ).

**Corollary (3.4).** Let  $K$  be a number field with  $-1 \in \dot{K}^2$ . Then there exists a totally real number field  $L$  such that  $g(K) = g(L)$  and  $K \sim L(\sqrt{-1})$ .

*Proof.* Put  $T := S(K)$ . We have  $K \supset \mathbb{Q}(\sqrt{-1})$ , hence the degree  $N = [K : \mathbb{Q}]$  is even. Also  $-1 \in \dot{K}_p^2$  for every dyadic prime  $p$  of  $K$ , hence all local degrees  $N_j$  are even. By Theorem (3.2) and Remark (3.3), there exists a totally real number field  $L$  such that  $K \sim L(\sqrt{a})$  for some  $a \in \dot{L} \setminus \dot{L}^2$ . Moreover,  $S = s(K) = 1$ . Hence the construction in the proof of Theorem (3.2) gives  $g(K) = g = G = g(L)$ . Since  $L$  is a real field and the level  $s(L(\sqrt{a})) = s(K) = 1$ , it follows that  $a \in -\dot{L}^2$ . Thus  $K \sim L(\sqrt{-1})$ , as desired.

**Remark (3.5).** If  $-1 \in \dot{K}^2$ , then, in general, there does not exist a subfield  $L \subset K$  such that  $K = L(\sqrt{-1})$ .

We know from Theorem (2.5) that quadratic extensions of any fixed number field form always at least two distinct Witt equivalence classes. In contrast to this, if a class  $T$  comes from quadratic extensions of fields of a certain class  $S$ , it may happen that  $S$  is unique. This deserves a closer look.

**Definition (3.6).** A class  $T$  of Witt equivalent number fields is said to be *singular* if there exists a unique class  $S$  such that  $T \in \text{Witt}(S, 2)$ . The class  $S$  is then said to *support*  $T$ . A class  $S$  supporting a singular class is said to be *basic*.

An obvious example of singular classes comes from quadratic extensions of  $\mathbb{Q}$ . Clearly,  $S = S(\mathbb{Q})$  is basic, and each of the seven classes in  $\text{Witt}(\mathbb{Q}, 2)$  is singular and supported by  $S$ .

**Theorem (3.7).** A class  $T = (N, R, S, G; (N_j, S_j), j = 1, \dots, G)$  is singular if and only if the following conditions are satisfied:

- (1)  $N$  is even and every odd  $N_j$  occurs an even number of times.
- (2)  $R = N$  or  $N - 2$ .
- (3) The even local degrees are pairwise distinct.
- (4) If  $N_j$  is divisible by 4, then  $S_j = 2$ .

*Proof.* If  $N = 2$ , then every class  $T$  is singular, and every class of degree 2 satisfies (1)–(4). Thus we may assume that  $N \geq 4$ . Assume first that  $T$  is a singular class and  $S$  is the unique supporting class of  $T$ . Then  $n = \frac{1}{2}N$  and  $r = n$ , the latter by Remark (3.3), and by the singularity of  $T$ . Condition (1) is satisfied in view of Theorem (3.2).

To prove (2), suppose  $R = 2(n - t)$ , where  $t \geq 2$ . Consider the sequence

$$U = (n, n - 2, s^*, g; (n_i, s_i), i = 1, \dots, g),$$

where  $s^* = s$ , unless  $n = 2$ , in which case we choose  $s^* = 2$  or  $4$  (depending on  $g = 1$  or  $2$ ). Here  $U$  is indeed the invariant of a field of degree  $n$ , by Theorem (2.1) in [S2]. In such a case, we will say that  $U$  is realizable (as the Witt equivalence invariant of a number field). By Theorem (3.1), we have  $T \in \text{Witt}(U, 2)$ , and since  $U \neq S$ , this contradicts the singularity of  $T$ . Hence  $t = 0$  or  $1$ , and  $R = 2(n - t) = N$  or  $N - 2$ , as required.

Now we prove (3). Suppose  $N_1$  and  $N_2$  are even and equal. There are two cases. First, if  $N_1$  and  $N_2$  are local degrees at conjugate primes  $P_1$  and  $P_2$  lying over  $p_1$ , say, then  $n_1 = N_1 = N_2 = 2m_1$ , for a positive integer  $m_1$ , and so  $g < n$ . Then we form a realizable sequence

$$U = (n, n, 0, g + 1; m_1, m_1, n_2, \dots, n_g; s_1^*, s_1^*, s_2, \dots, s_g),$$

where  $s_1^* = 4$  if  $m_1$  is odd, and  $s_1^* = 2$  otherwise. Then, by Theorem (3.1),  $T \in \text{Witt}(U, 2)$  and  $U \neq S$ , a contradiction. The second case is when  $N_1$  and  $N_2$  are local degrees at nonconjugate primes  $P_1$  and  $P_2$  lying over distinct primes  $p_1$  and  $p_2$ , say. Then  $g \geq 2$  and we construct the realizable sequence

$$U = (n, n, 0, g - 1; 2n_1, n_3, \dots, n_g; 2, s_3, \dots, s_g).$$

Again,  $T \in \text{Witt}(U, 2)$ , by Theorem (3.1), and  $U \neq S$ , a contradiction. This proves the necessity of (3). We notice that (3) implies that the even local degrees in  $S$  are also pairwise distinct.

To prove (4), assume  $N_1 = 4m_1$  and  $S_1 = 1$ . By (3), no other local degree  $N_j$ ,  $j \neq 1$ , is equal to  $N_1$ . Hence  $N_1 = 2n_1$ , where  $n_1$  is the local degree at a nonsplit prime  $p_1$ . Thus  $n_1 = 2m_1$  is even. Hence  $s_1 = 1$  or  $2$ . Now we set up realizable

$$U = (n, n, 0, g; n_1, \dots, n_g; s_1^*, s_2, \dots, s_g),$$

where  $s_1^* = 1$  or  $2$  when  $s_1 = 2$  or  $1$ , respectively. Then  $T \in \text{Witt}(U, 2)$ , by Theorem (3.1). Since  $U \neq S$ , this is a contradiction. Hence  $S_1 = 2$ , as required.

Now we prove the sufficiency of conditions (1)–(4). From (1) and Theorem (3.2) it follows that there exists a class  $S$  such that  $T \in \text{Witt}(S, 2)$ . We will show that (1)–(4) imply the uniqueness of  $S$ . So let  $S = (n, r, s, g; (n_i, s_i), i = 1, \dots, g)$ . Clearly,  $n = \frac{1}{2}N$ . Then we have  $r \leq n$  and also  $R \leq 2r$ . Hence  $N - 2 = 2n - 2 \leq R \leq 2r \leq 2n$ , and so  $n - 1 \leq r \leq n$ . Since  $r \equiv n \pmod{2}$ , we must have  $r = n$ . It follows that  $s = 0$ . Thus  $n, r, s$  are uniquely determined by  $T$ . Assume that  $e$  is the number of even local degrees in  $T$ , and rearrange the  $N_j$ 's, if necessary, to get  $N_1, \dots, N_e$  even. Since these are pairwise distinct by (3), we must have  $N_1 = 2n_1, \dots, N_e = 2n_e$ , after renumbering the  $n_i$ 's, if necessary. This fixes the degrees  $n_1, \dots, n_e$  in  $S$ . Now the remaining local degrees in  $T$  and  $S$  can be rearranged and matched to satisfy  $N_{e+1} = N_{e+2} = n_{e+1}, \dots, N_{G-1} = N_G = n_g$ . Thus the local degrees  $n_1, \dots, n_g$  are uniquely determined by  $T$ , and so is  $g$ . By our choice of  $N_1, \dots, N_e$ , all the  $n_{e+1}, \dots, n_g$  are odd. Hence the local levels  $s_{e+1} = \dots = s_g = 4$ . Further, by (4), we have  $S_j = 2$  when  $4 \nmid N_j$  for  $j < e$ . Hence from  $N_j = 2n_j$  it follows that  $s_j = 2$  as well ( $n_j$  is even, hence  $s_j \leq 2$ , but  $s_j = 1$  would imply  $S_j = 1$ ). If  $N_j$  is even but not divisible by 4, then  $n_j$  is odd, so  $s_j = 4$ . This proves the uniqueness of  $S$  and singularity of  $T$ .

**Proposition (3.8).** *A class  $S = (n, r, s, g; (n_i, s_i), i = 1, \dots, g)$  is basic (that is, it supports a singular class of degree  $2n$ ) if and only if*

- (1)  $r = n$  and  $s = 0$ .
- (2) *The even local degrees are pairwise distinct.*
- (3) *The local levels are all  $\neq 1$ .*

*Proof.* The necessity of (1) and (2) has been shown in the proof of the necessity part of Theorem (3.7). As to (3), if  $n_i$  is odd, then  $s_i = 4$ , and if  $n_i$  is even, then by (3.7)(3) the corresponding  $N_j$  is necessarily divisible by 4, hence  $S_j = 2$  by (3.7)(4), and so  $s_i \geq 2$ . Conversely, if  $S$  satisfies (1), (2) and (3), and if  $n_1, \dots, n_e$  are even and  $n_{e+1}, \dots, n_g$  are odd, then

$$T := (2n, 2n, 0, e + 2(g - e); 2n_1, \dots, 2n_e, n_{e+1}, n_{e+1}, \dots, n_g, n_g; \\ 2, \dots, 2, 4, 4, \dots, 4, 4)$$

is singular by Theorem (3.7), and  $T \in \text{Witt}(S, 2)$  by Theorem (3.1). Thus  $S$  supports a singular class.

**Corollary (3.9).** (1)  $S(\mathbb{Q}(\sqrt{2}))$  and  $S(\mathbb{Q}(\sqrt{17}))$  are the only basic classes of degree 2.

(2) *The only basic classes of degree 3 are the three classes listed in Corollary (2.10) as V, VII, and VIII.*

*Proof.* Combine Proposition (3.8) and the local data given in Corollaries (2.9) and (2.10).

Basic classes occur in every degree  $n$ , and singular classes occur in every even degree  $2n$ .

**Example (3.10).** Let  $F$  be a number field with

$$S(F) = (n, n, 0, n; 1, \dots, 1; 4, \dots, 4).$$

Then  $S(F)$  is basic by Proposition (3.8). If we choose  $a \in \dot{F}$  as in Example (1.4), then

$$S(F(\sqrt{a})) = (2n, 2n, 0, 2n; 1, \dots, 1; 4, \dots, 4)$$

is singular by Theorem (3.7). However, it is also basic by Proposition (3.8), and gives rise to a singular class of degree  $4n$ . This procedure can be used to produce an infinite tower of quadratic extensions each of which is both basic and singular.

Here is an explicit example. Let  $F_1 = \mathbb{Q}(\sqrt{17})$  and  $F_{n+1} = F_n(\sqrt{p_{n+1}})$ , where  $p_n$  is the  $n$ th prime number congruent to 1 (mod 8) (thus  $p_1 = 17$ ,  $p_2 = 41$ , etc.). Then by Kummer theory,  $[F_{n+1} : F_n] = 2$  for every  $n \geq 1$  (cf. [E-L-W, Theorem 2.1]), and each  $F_n$  is both basic and singular (supported by  $F_{n-1}$ , where  $F_0 = \mathbb{Q}$ ).

Using Theorem (3.7) we can manufacture a formula for the number  $\text{Sing } N$  of singular Witt equivalence classes of a given degree  $N \geq 4$  (recall that  $\text{Sing } 2 = 7$ ). If  $T = (N, R, S, G; (N_j, S_j), j = 1, \dots, G)$  is a singular class, then  $R$  assumes two values  $N$  and  $N - 2$ , each combined with any admissible local degrees and local levels. Thus

$$(3.10.1) \quad \text{Sing } N = 2 \cdot p_2(N), \quad \text{where } p_2(N) = \sum \mu \cdot 2^e,$$

the summation ranging over all partitions of  $N$  and a given partition  $N = N_1 + \cdots + N_G$  contributing  $\mu \cdot 2^e$ , where  $e$  is the number of even parts  $N_j$  not divisible by 4 (here  $S_j$  can be either 1 or 2), and  $\mu = 0$  if there are two even equal parts, or an odd part occurs an odd number of times, while  $\mu = 1$  otherwise.

On the other hand, Proposition (3.8) allows us to compute the number  $\text{Basic } n$  of basic classes of degree  $n$  (supporting some singular classes of degree  $2n$ ).  $\text{Basic } n$  is the number of partitions of  $n$  with the property that each even part occurs exactly once. Using this and (3.10.1) for  $N \geq 4$ , we have computed the values of  $\text{Basic } n$  and  $\text{Sing } 2n$  for  $n \leq 5$ . For comparison, we have also computed the number  $w(n, 2)$  of classes of degree  $2n$  obtainable by quadratic extensions from classes of degree  $n$ . Here Theorem (3.2) has been used to determine the admissible local degrees  $N_1, \dots, N_G$ , and then  $w(n, 2)$  has been found by applying the counting method from [S2]. In the following table the last row shows the total number  $w(2n)$  of classes of degree  $2n$  (over  $\mathbb{Q}$ ), taken from [S2].

$2n :$	2	4	6	8	10
$\text{Basic } n$	1	2	3	4	6
$\text{Sing } 2n$	7	8	18	32	48
$w(n, 2)$	7	26	79	210	505
$w(2n)$	7	29	95	270	715

For a set  $A \subseteq \text{Witt}(\mathbb{Q}, n)$  of classes of degree  $n$ , we write

$$\text{Witt}(A, 2) := \bigcup \{ \text{Witt}(S, 2) : S \in A \}.$$

We will be interested in the case when  $A = \text{Witt}(\mathbb{Q}, n)$ , and then  $\text{Witt}(A, 2)$  is the set of all classes of degree  $2n$  obtainable from classes of degree  $n$  by quadratic extensions. We use the following abbreviated notation

$$\text{Witt}(n, 2) := \text{Witt}(\text{Witt}(\mathbb{Q}, n), 2).$$

From Theorem (3.2) it follows that for any  $n \geq 2$ ,

$$\text{Witt}(n, 2) \subsetneq \text{Witt}(\mathbb{Q}, 2n).$$

We will make a few comments on the structure of the set  $\text{Witt}(n, 2)$ .

A subset  $B$  of  $\text{Witt}(\mathbb{Q}, n)$  such that

$$(3.10.2) \quad \text{Witt}(n, 2) = \bigcup \{ \text{Witt}(T, 2) : T \in B \}$$

is said to generate  $\text{Witt}(n, 2)$ . A minimal generating set  $B$  is said to be a basis for  $\text{Witt}(n, 2)$ . Clearly, bases do exist. For instance,

$$\text{Witt}(2, 2) = \text{Witt}(S(\mathbb{Q}(\sqrt{17})), 2) \cup \text{Witt}(S(\mathbb{Q}(\sqrt{2})), 2),$$

according to the results in §2, and the classes of  $\mathbb{Q}(\sqrt{17})$  and  $\mathbb{Q}(\sqrt{2})$  form a basis for  $\text{Witt}(2, 2)$ .

**Lemma (3.11).** (1) *If  $B$  is a basis for  $\text{Witt}(n, 2)$ , then  $B$  contains every basic class  $S$  in  $\text{Witt}(\mathbb{Q}, n)$ .*

(2) If all the basic classes  $S$  in  $\text{Witt}(\mathbb{Q}, n)$  form a basis for  $\text{Witt}(n, 2)$ , then it is the unique basis for  $\text{Witt}(n, 2)$ .

*Proof.* (1) Singular classes do belong to  $\text{Witt}(n, 2)$  and can be reached only from their supporting basic classes.

(2) This follows from (1).

**Proposition (3.12).** *The basic classes in  $\text{Witt}(\mathbb{Q}, n)$  form a basis for  $\text{Witt}(n, 2)$  if and only if  $n \leq 7$ .*

*Proof.* First suppose  $n \geq 8$ . Then there is a class  $T$  in  $\text{Witt}(n, 2)$  with four local degrees equal to 4,  $N_1 = N_2 = N_3 = N_4 = 4$ , say. If  $T \in \text{Witt}(S, 2)$ , then one of the sets  $(2, 2, 2, 2)$ ,  $(2, 2, 4)$  or  $(4, 4)$  must be a subset of the set of local degrees of  $S$ . Then, however,  $S$  is not basic, by Proposition (3.8). Thus basic classes are insufficient to generate  $\text{Witt}(n, 2)$  for  $n \geq 8$ .

Now assume that  $n \leq 7$ . If  $T \in \text{Witt}(n, 2)$ , we will point out a basic  $S \in \text{Witt}(\mathbb{Q}, n)$  such that  $T \in \text{Witt}(S, 2)$ . We have

$$2n = N_1 + \cdots + N_G,$$

where  $N_1, \dots, N_G$  are the local degrees of  $T$ . By Theorem (3.2), each odd summand occurs an even number of times. To find a set of local degrees  $n_1, \dots, n_g$  for a basic  $S$  we construct the  $n_i$ 's from the  $N_j$ 's as follows. In the sequence  $N_1, \dots, N_g$  we replace each even  $N_j$  with  $\frac{1}{2}N_j$ , and from each pair of odd and equal degrees we delete one of the two. If in the new sequence  $n_1, \dots, n_g$  the even  $n_i$ 's are pairwise distinct, we are through by Proposition (3.8). Otherwise, since  $n \leq 7$ , we must have two or three 4's among the  $N_j$ 's. Then, if  $N_1 = N_2 = 4$ , say, we take  $n_1 = 4$  and find the remaining  $n_i$ 's as before. Again by Proposition (3.8) we construct  $S$  which is basic and  $T \in \text{Witt}(S, 2)$ .

**Corollary (3.13).** (1)  $\text{Witt}(2, 2)$  has precisely one basis. It consists of  $S(\mathbb{Q}(\sqrt{2}))$  and  $S(\mathbb{Q}(\sqrt{17}))$ .

(2)  $\text{Witt}(3, 2)$  has precisely one basis. It consists of the three classes listed as V, VII, and VIII in Corollary (2.10).

*Proof.* Combine Corollary (3.9), Proposition (3.12), and Lemma (3.11).

#### 4. CONNECTIVITY OF THE $\text{Witt Graph}(n, 2)$

We wish to define a bipartite graph  $\text{Witt Graph}(n, 2)$  on the set of vertices

$$V(n) := \text{Witt}(\mathbb{Q}, n) \cup \text{Witt}(n, 2).$$

The vertices  $S \in \text{Witt}(\mathbb{Q}, n)$  and  $T \in \text{Witt}(n, 2)$  are connected with an edge if and only if  $T \in \text{Witt}(S, 2)$ . According to Theorem (2.5), the valency of any vertex in  $\text{Witt}(\mathbb{Q}, n)$  is at least 2. The monovalent vertices all belong to  $\text{Witt}(n, 2)$  and are called singular classes (cf. Definition (3.6)). A vertex in  $\text{Witt}(\mathbb{Q}, n)$  connected with a monovalent vertex is said to support the monovalent vertex and has been called basic. It is a natural question to ask whether our bipartite graph is connected.

**Proposition (4.1).** *The  $\text{Witt Graph}(n, 2)$  is connected if and only if  $n \leq 2$ .*

*Proof.* Obviously,  $\text{Witt Graph}(1, 2)$  is connected. In view of Corollary (3.13)(1), the connectivity of  $\text{Witt Graph}(2, 2)$  follows from the fact that



$\text{Witt}(\mathbb{Q}(\sqrt{2}), 2) \cap \text{Witt}(\mathbb{Q}(\sqrt{17}), 2) \neq \emptyset$  (see the computation at the end of §2). The converse will follow from the general result in Theorem (4.2).

Let  $n$  be a natural number and let  $(n_1, \dots, n_g)$  and  $(m_1, \dots, m_h)$  be two partitions of  $n$ . We say that the two partitions are equivalent, written  $(n_1, \dots, n_g) \sim (m_1, \dots, m_h)$ , if one can be obtained from the other by a sequence of transformations of the following type:

- (1) replacing two equal parts  $a, a$  with  $2a$ ,
- (2) replacing an even part  $2b$  with  $b, b$ .

Clearly, the relation  $\sim$  is an equivalence relation on the set of partitions of  $n$ . For  $n = 1$  and  $n = 2$ , every two partitions of  $n$  are equivalent. But for  $n \geq 3$  there are always at least two distinct equivalence classes. For  $(n) \not\sim (n-1, 1)$ , since when  $n > 2$  is even, then  $(n-1, 1)$  is not transformable at all, and if  $n$  is odd, then  $(n)$  is not transformable.

**Theorem (4.2).** *Let  $S_1, S_2 \in \text{Witt}(\mathbb{Q}, n)$  be two classes with local degrees  $(n_1, \dots, n_g)$  and  $(m_1, \dots, m_h)$ , respectively. Then the following are equivalent:*

- (1)  $(n_1, \dots, n_g) \sim (m_1, \dots, m_h)$ .
- (2) *There is a path between the vertices  $S_1$  and  $S_2$  in the  $\text{Witt Graph}(n, 2)$ .*

*Proof.* (1)  $\Rightarrow$  (2) It is enough to show that if  $(m_1, \dots, m_h)$  is obtained from  $(n_1, \dots, n_g)$  by a single transformation  $(a, a) \rightarrow (2a)$ , or  $(2b) \rightarrow (b, b)$ , then there is a path between  $S_1$  and  $S_2$ . So suppose  $(n_1, n_1, n_3, \dots, n_g)$  and  $(2n_1, n_3, \dots, n_g)$  are the sets of local degrees for  $S_1$  and  $S_2$ , respectively. By Theorem (3.1), with properly chosen  $s, s^*$  and  $s_1^* \leq s^*$ , the classes

$$\begin{aligned} T_1 &:= (2n, 0, s, g; 2n_1, 2n_1, 2n_3, \dots, 2n_g; 1, 1, 1, \dots, 1), \\ T_2 &:= (2n, 0, s^*, g; 2n_1, 2n_1, 2n_3, \dots, 2n_g; s_1^*, s_1^*, 1, \dots, 1) \end{aligned}$$

satisfy  $T_1 \in \text{Witt}(S_1, 2)$  and  $T_2 \in \text{Witt}(S_2, 2)$ . We also consider the realizable class

$$S := (n, n, 0, g; n_1, n_1, n_3, \dots, n_g; S_1, S_1, S_3, \dots, S_g),$$

where  $S_i = 2$  or  $4$ , depending on the parity of  $n_i$ . Then, by Theorem (3.1), we have  $T_1, T_2 \in \text{Witt}(S, 2)$ . Thus  $S_1 - T_1 - S - T_2 - S_2$  is a path between  $S_1$  and  $S_2$ , as desired.

(2)  $\Rightarrow$  (1) It suffices to show that, if  $S_1 - T - S_2$  is a path, then the sets of local degrees in  $S_1$  and  $S_2$  are equivalent. So suppose that  $D_1 := (n_1, \dots, n_g)$  and  $D_2 := (m_1, \dots, m_h)$  are the sets of local degrees in  $S_1$  and  $S_2$ , respectively. Since  $T$  belongs to  $\text{Witt}(S_i, 2)$ ,  $i = 1, 2$ , we know from Theorem (1.1) that the set of local degrees in  $T$  is, up to the order of local degrees in  $D_1$  and  $D_2$ , equal to

$$\begin{aligned} D_1^* &:= (n_1, n_1, \dots, n_k, n_k, 2n_{k+1}, \dots, 2n_g), \\ D_2^* &:= (m_1, m_1, \dots, m_l, m_l, 2m_{l+1}, \dots, 2m_h), \end{aligned}$$

for some  $k$  and  $l$ . Here  $g + k = h + l$  and  $D_1^* = D_2^*$  as unordered partitions of  $2n$ .

We induct on  $g$ . If  $g = 1$ , then  $D_1^* = D_2^*$  implies  $D_1 \sim D_2$ , as required. Suppose now that  $g > 1$ . There are two cases. First, if the sets of split degrees in  $D_1$  and  $D_2$  intersect nontrivially,

$$\{n_1, \dots, n_k\} \cap \{m_1, \dots, m_l\} \neq \emptyset,$$

or, if the sets of nonsplit degrees have an element in common,

$$\{n_{k+1}, \dots, n_g\} \cap \{m_{l+1}, \dots, m_h\} \neq \emptyset,$$

then we remove the common parts from the partitions  $D_1$  and  $D_2$  of  $n$ , and by an easy induction argument,  $D_1 \sim D_2$ , as required.

The second case is when both intersections are empty. Then, up to the order of parts in  $D_1$  and  $D_2$ , we must have

$$\begin{aligned} n_1 = 2m_{l+1} = 2m_{l+2}, \dots, n_k = 2m_{l+2k-1} = 2m_{l+2k}, \quad l + 2k = h, \\ m_1 = 2n_{k+1} = 2n_{k+2}, \dots, m_l = 2n_{k+2l-1} = 2n_{k+2l}, \quad k + 2l = g. \end{aligned}$$

Hence,

$$\begin{aligned} D_1 &= (2m_{l+1}, 2m_{l+3}, \dots, 2m_{l+2k-1}, \tfrac{1}{2}m_1, \tfrac{1}{2}m_1, \dots, \tfrac{1}{2}m_l, \tfrac{1}{2}m_l) \\ &\sim (m_{l+1}, m_{l+1}, m_{l+3}, m_{l+3}, \dots, m_{h-1}, m_{h-1}, m_1, \dots, m_l) \\ &= (m_{l+1}, m_{l+2}, m_{l+3}, m_{l+4}, \dots, m_{h-1}, m_h, m_1, \dots, m_l) \\ &= D_2. \end{aligned}$$

This proves the theorem.

As we have already noticed, if  $n \geq 3$ , then  $(n) \approx (n-1, 1)$ . Thus the theorem implies that the Witt Graph( $n, 2$ ) is disconnected when  $n \geq 3$ . This completes the proof of Proposition (4.1).

Following a suggestion of Daniel B. Shapiro we draw the following corollary.

**Corollary (4.3).** *The number of connected components of the Witt Graph( $n, 2$ ) is equal to the number of partitions of  $n$  into odd parts.*

*Proof.* According to Theorem (4.2), the number of connected components of the Witt Graph( $n, 2$ ) is equal to the number of equivalence classes of the set of all partitions of  $n$  with respect to the relation  $\sim$ . Clearly, each equivalence class contains a partition with all parts odd, and it remains to show that there is just one such partition in every equivalence class. If  $(n_1, \dots, n_g)$  is a partition of  $n$  into odd parts  $n_j$ , then any partition in the same equivalence class has parts of the form  $2^i \cdot n_j$ , where  $i \geq 0$  and  $1 \leq j \leq g$ . It follows that two equivalent partitions with all parts odd are identical.

Here is a table showing the number  $cc(n, 2)$  of connected components of the Witt Graph( $n, 2$ ), for  $n \leq 10$ .

$n$	1	2	3	4	5	6	7	8	9	10
$cc(n, 2)$	1	1	2	2	3	4	5	6	8	10

#### ACKNOWLEDGMENT

I wish to thank the referee for a thorough reading of the manuscript and detecting several gaps and incorrect assertions.

#### REFERENCES

- [C] J. Carpenter, *Finiteness theorems for forms over global fields*, Math. Z. **209** (1992), 153–166.
- [Cz1] A. Czogała, *On reciprocity equivalence of quadratic number fields*, Acta Arith. **58** (1991), 27–46.

- [Cz2] ———, *Witt equivalence of quadratic extensions of global fields*, Math. Slovaca **41** (1991), 251–255.
- [E-L-W] R. Elman, T. Y. Lam, and A. R. Wadsworth, *Quadratic forms under multiquadratic extensions*, Indag. Math. (N.S.) **42** (1980), 131–145.
- [J-M] S. Jakubec and F. Marko, *Witt equivalence classes of quartic number fields*, Math. Comp. **58** (1992), 355–368.
- [L] T. Y. Lam, *The algebraic theory of quadratic forms*, Benjamin/Cummings, Reading, MA, 1980.
- [O'M] O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, Berlin, Heidelberg, and New York, 1971.
- [P-S-C-L] R. Perlis, K. Szymiczek, P. E. Conner, and R. Litherland, *Matching Witts with global fields*, Recent Advances in Real Algebraic Geometry and Quadratic Forms (Proc. RAGSQUAD Year, Berkeley, CA, 1990–1991); (W. B. Jacob, T. Y. Lam, and R. O. Robson, eds.), Contemp. Math. (to appear).
- [S1] K. Szymiczek, *Matching Witts locally and globally*, Math. Slovaca **41** (1991), 315–330.
- [S2] ———, *Witt equivalence of global fields*, Comm. Algebra **19** (1991), 1125–1149.

INSTYTUT MATEMATYKI, UNIWERSYTET ŚLASKI, BANKOWA 14, 40-007 KATOWICE, POLAND  
E-mail address: [szymiczek@gate.math.us.edu.pl](mailto:szymiczek@gate.math.us.edu.pl)