Title: 2-ranks of class groups of Witt equivalent number fields

Author: Kazimierz Szymiczek

Annales Mathematicae Silesianae 12 (1998), 53–64

Prace Naukowe Uniwersytetu Śląskiego nr 1751, Katowice

2–RANKS OF CLASS GROUPS OF WITT EQUIVALENT NUMBER FIELDS

KAZIMIERZ SZYMICZEK

Dedicated to the memory of Ivan Korec

Introduction

In [CPS] we have observed that each class of Witt equivalent quadratic number fields, except for the singleton class containing only $\mathbb{Q}(\sqrt{-1})$, contains a field whose class group has 2–rank as large as we wish.
Here we generalize this observation from the case of quadratic number fields to fields of arbitrary *even* degree n. We prove that each class of Witt equivalent number fields of even degree $n > 2$ contains a field K with the 2–rank of class group as large as we wish. In fact, we prove a stronger result saying that the field in question has large 2–rank of S–class group for a finite set S of primes of K containing all infinite and all dyadic primes of the field.
We combine here an interpretation of the parity of S–class numbers in terms of a localization map (Proposition 6) with a valuation-theoretic result of Endler on the existence of fields with prescribed completions. The latter has been used in [Sz] to construct fields with prescribed Witt equivalence invariants. Here we discuss this technique again to make clear its applicability in constructing, in a given Witt class, number fields with special properties.

1. Localization

Let K be an algebraic number field, $\Omega = \Omega(K)$ the collection of all primes in K. We write $\Omega_2 = \Omega_2(K)$ for the set of all dyadic primes of K and

Received on August 15, 1998.

1991 *Mathematics Subject Classification.* 11E12, 11R29.

Key words and phrases: Witt equivalence, 2-rank of class group.

Supported by the State Committee for Scientific Research (KBN) of Poland under Grant 2 P03A 024 12.

$g = g(K)$ for the cardinality of Ω_2. By $S \subset \Omega$ we shall denote a finite set of primes which includes, at least, the set $\Omega_\infty = \Omega_\infty(K)$ of all infinite primes in K. We have

$$\#\Omega_\infty = r + c,$$

where $r = r(K)$ and $c = c(K)$ are the numbers of real and complex infinite primes, and $[K : \mathbb{Q}] = r + 2c$.

We define the group $E(S) \subset K^*/K^{*2}$ of *even* square classes as follows.

$$E(S) = \{xK^{*2} \in K^*/K^{*2} : \quad \mathrm{ord}_\mathfrak{p}\, x \equiv 0 \pmod 2 \quad \forall \mathfrak{p} \in \Omega \setminus S\}.$$

When $S = \Omega_\infty$, the group $E(S)$ is also written K_{ev}.

The group K_{ev} was used already by Hecke [H] in his 1923 book. We give here a survey of results on $E(S)$ needed in our discussion of the class number parity questions in Witt equivalence classes of number fields. Most of these results appeared already in [Cz] in the case when $S = \Omega_\infty \cup \Omega_2$. We give a slightly more general version following Conner's manuscript [Con]. Our presentation appears to be simple and elementary due to Conner's approach. We have found it convenient to rearrange Conner's arguments and to replace his use of class field theory with a more elementary argument due to Czogała ([Cz], Lemma 2.6).

We consider the group of $S-$units

$$U_S = \{y \in K^* : \quad \mathrm{ord}_\mathfrak{p}\, y = 0 \quad \forall \mathfrak{p} \in \Omega \setminus S\}.$$

An $S-$unit is a square in K if and only if it is the square of an $S-$unit. Consequently we have an injective homomorphism

$$U(S) := U_S/U_S^2 \to K^*/K^{*2}$$

of the group $U(S)$ of square classes of $S-$units into the group of global square classes K^*/K^{*2}. The group $U(S)$ is a finite elementary Abelian 2-group, and according to the Dirichlet $S-$Units Theorem, we have $\mathrm{rk}_2\, U(S) = \#S$.

The $S-$ideal class group $C_S(K)$ is the quotient of the ordinary ideal class group, $C(K)$, by the subgroup generated by the ideal classes of the finite primes in S. We shall be concerned with the quotient group $C_S(K)/C_S(K)^2$ and the subgroup ${}_2C_S(K)$ of $C_S(K)$,

$${}_2C_S(K) = \{B \in C_S(K) : \quad B^2 = 1 \in C_S(K)\}.$$

The groups ${}_2C_S(K)$ and $C_S(K)/C_S(K)^2$ are finite elementary Abelian 2-groups. Recall that the 2-rank of a finite Abelian group equals the number

of direct summands in a decomposition of the Sylow 2-subgroup of the group into direct sum of cyclic groups. Hence, by elementary group theory,

$$\mathrm{rk}_2\, C_S(K) = \mathrm{rk}_2\ {}_2C_S(K) = \mathrm{rk}_2\, C_S(K)/C_S(K)^2.$$

The group $U(S)$ is a subgroup of the group $E(S)$ of even square classes, but in general the containment is proper. As the following Proposition shows, the 2-ranks of the two groups differ by $\mathrm{rk}_2\, C_S(K)$.

PROPOSITION 1. $\mathrm{rk}_2\, E(S) = \#S + \mathrm{rk}_2\, C_S(K)$.

PROOF. There is a natural short exact sequence

$$1 \to U(S) \to E(S) \xrightarrow{\eta} {}_2C_S(K) \to 1,$$

where η is defined as follows. For $x \in K^*$ with $xK^{*2} \in E(S)$ we have

$$x\mathcal{O}_K = \mathfrak{a} \cdot \mathfrak{b}^2, \quad \text{where} \quad \mathfrak{a} = \prod_{\mathfrak{p} \in S \setminus \Omega_\infty} \mathfrak{p}^a, \quad \mathfrak{b} = \prod_{\mathfrak{q} \in \Omega \setminus S} \mathfrak{q}^b.$$

Setting $\eta(xK^{*2}) = \mathrm{cl}(\mathfrak{b}) \in C_S(K)$ we obtain a well defined homomorphism. Observe that $xK^{*2} \in \ker \eta$ if and only if there is a $y \in K^*$ and an ideal $\mathfrak{a}_1 = \prod_{\mathfrak{p} \in S \setminus \Omega_\infty} \mathfrak{p}^\alpha$ satisfying $\mathfrak{a}_1 \cdot (y) = \mathfrak{b}$. This is equivalent to

$$xy^{-2}\mathcal{O}_K = \mathfrak{a}\mathfrak{a}_1^2$$

meaning $xy^{-2} \in U_S$ and $xK^{*2} \in U(S)$. This shows that $\ker \eta = U(S)$. On the other hand, it is obvious that $\mathrm{cl}(\mathfrak{b}) \in {}_2C_S(K)$, and $\mathrm{im}\, \eta = {}_2C_S(K)$. Thus the sequence is exact. Now it follows that

$$\mathrm{rk}_2\, E(S) = \mathrm{rk}_2\, U(S) + \mathrm{rk}_2\ {}_2C_S(K).$$

To finish the proof it is sufficient to recall that

$$\mathrm{rk}_2\, U(S) = \#S \quad \text{and} \quad \mathrm{rk}_2\ {}_2C_S(K) = \mathrm{rk}_2\, C_S(K). \qquad \square$$

COROLLARY. $\mathrm{rk}_2\, K_{ev} = r + c + \mathrm{rk}_2\, C(K)$. $\square$

At each prime $\mathfrak{p} \in S$ we have the completion $K_\mathfrak{p}$ and the group of local square classes $K_\mathfrak{p}^*/K_\mathfrak{p}^{*2}$. Let

$$G(S) := \prod_{\mathfrak{p} \in S} K_\mathfrak{p}^*/K_\mathfrak{p}^{*2}.$$

PROPOSITION 2. *If* $\Omega_2 \subset S$, *then* $\operatorname{rk}_2 G(S) = 2(\#S)$.

PROOF. $G(S)$ is a finite elementary Abelian 2-group and its order is easily shown to be $4^{\#S}$ (see [O'M], p. 178). Hence the result. □

At each prime $\mathfrak{p} \in S$ we have a localization homomorphism

$$\nu_{\mathfrak{p}} : K^*/K^{*2} \to K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2}.$$

These may be assembled into an epimorphism

$$\nu^S = \prod_{\mathfrak{p} \in S} \nu_{\mathfrak{p}} : K^*/K^{*2} \to G(S).$$

We will write $\nu_S = \nu^S|_{E(S)} : E(S) \to G(S)$ for the restriction of ν^S to $E(S)$. Since $G(S)$ is a finite elementary Abelian 2-group we define an $\mathbb{F}_2$−inner product space structure as follows. For $X, Y \in G(S)$ write

$$X = \{x_{\mathfrak{p}}\}_{\mathfrak{p} \in S}, \quad Y = \{y_{\mathfrak{p}}\}_{\mathfrak{p} \in S}$$

with $x_{\mathfrak{p}}, y_{\mathfrak{p}} \in K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2}$ and define $\beta(X,Y) \in \mathbb{F}_2 = \{0,1\}$ by using Hilbert symbols

$$(-1)^{\beta(X,Y)} = \prod_{\mathfrak{p} \in S} (x_{\mathfrak{p}}, y_{\mathfrak{p}})_{\mathfrak{p}}.$$

Then $(G(S), \beta)$ is a bilinear space over $\mathbb{F}_2$. It is, in fact, nonsingular, that is, an inner product space, since it can be viewed as the product of nonsingular bilinear spaces $(K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2}, \beta_{\mathfrak{p}})$, where

$$(-1)^{\beta_{\mathfrak{p}}(x,y)} = (x,y)_{\mathfrak{p}} \quad \text{for} \quad x, y \in K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2}.$$

PROPOSITION 3. *If* $\Omega_2 \subset S$, *then the image subgroup* $\nu_S(E(S)) \subset G(S)$ *is a totally isotropic subspace of* $(G(S), \beta)$.

PROOF. For $xK^{*2}, yK^{*2} \in E(S)$ we have

$$(x,y)_{\mathfrak{p}} = +1 \quad \forall\, \mathfrak{p} \in \Omega \setminus S,$$

since x, y lie in the unit square classes in $K_{\mathfrak{p}}^*/K_{\mathfrak{p}}^{*2}$ and all $\mathfrak{p} \in \Omega \setminus S$ are finite nondyadic primes. Hence, by the Hilbert Reciprocity,

$$\prod_{\mathfrak{p} \in S} (x,y)_{\mathfrak{p}} = +1.$$

Hence $\beta(\nu_S(x), \nu_S(y)) = 0 \in \mathbb{F}_2$ for all $x, y \in E(S)$. □

PROPOSITION 4. *If* $\Omega_2 \subset S$, *then* $\operatorname{rk}_2 \nu_S(E(S)) \leqslant \#S$.

PROOF. A totally isotropic subspace $\nu_S(E(S))$ of dimension d is contained in a $2d$-dimensional metabolic subspace of $G(S)$. Hence

$$2d \leqslant \operatorname{rk}_2 G(S) = 2(\#S),$$

and $\operatorname{rk}_2 \nu_S(E(S)) = d \leqslant \#S$. □

PROPOSITION 5. *If* $\Omega_2 \subset S$, *then* $\operatorname{rk}_2 \ker \nu_S \leqslant \operatorname{rk}_2 C_S(K)$.

PROOF. If ν_S is injective, there is nothing to prove. So assume that $\ker \nu_S$ has positive dimension. Let $b_1 K^{*2}, \ldots, b_t K^{*2}$ be a basis for $\ker \nu_S$. By a classical theorem (see [H], Satz 169), for each j there are infinitely many prime ideals $\mathfrak{q}_j$ satisfying

$$\left(\frac{b_i}{\mathfrak{q}_j}\right) = (-1)^{\delta_{ij}}, \quad i = 1, \ldots, t,$$

where δ_{ij} is the Kronecker's delta. Clearly we can choose the ideals $\mathfrak{q}_j$ outside S. We assert that the ideal classes $\operatorname{cl}(\mathfrak{q}_1), \ldots, \operatorname{cl}(\mathfrak{q}_t) \in C_S(K)$ belong to linearly independent cosets of $C_S(K)/C_S(K)^2$. Otherwise, after renumbering the ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ if necessary, we would arrive at an $x \in K^*$ such that

$$x\mathcal{O}_K = \mathfrak{q}_1 \cdots \mathfrak{q}_\ell \cdot \mathfrak{a}\mathfrak{b}^2,$$

where $\mathfrak{a}$ is a product of powers of ideals in S, and $\mathfrak{b}$ is a product of powers of ideals outside S. We claim that

$$(b_1, x)_{\mathfrak{q}_1} = -1 \quad \text{and} \quad (b_1, x)_{\mathfrak{r}} = 1$$

for all primes $\mathfrak{r}$, finite or infinite, distinct from $\mathfrak{q}_1$. For simplicity, a unit up to a square at $\mathfrak{P}$ will be called a unit at $\mathfrak{P}$, and similarly, a prime up to a square at $\mathfrak{P}$ will be called a prime at $\mathfrak{P}$. First observe that $b_1 K^{*2} \in E(S)$, hence b_1 is a unit at each prime outside S. Since x is a prime at $\mathfrak{q}_1$ and $\mathfrak{q}_1$ is nondyadic, this explains the first asserted value of the Hilbert symbol. If $\mathfrak{r} \in S$, or if $\mathfrak{r} = \mathfrak{q}_j$ for some $j > 1$, then b_1 is a square at $\mathfrak{r}$. On the other hand, if $\mathfrak{r}$ is outside S and distinct from all $\mathfrak{q}_i$, then b_1 and x are units at $\mathfrak{r}$ and $\mathfrak{r}$ is a nondyadic ideal. This proves our claim. But the claim contradicts Hilbert Reciprocity. This proves the linear independence we are after and establishes the Proposition. □

PROPOSITION 6. *If* $\Omega_2 \subset S$, *then*

$$\mathrm{rk}_2\, \nu_S(E(S)) = \#S \quad \textit{and} \quad \mathrm{rk}_2 \ker \nu_S = \mathrm{rk}_2\, C_S(K).$$

PROOF. From the isomorphism $\nu_S(E(S)) \cong E(S)/\ker \nu_S$, and from Proposition 1,

$$\mathrm{rk}_2\, \nu_S(E(S)) + \mathrm{rk}_2 \ker \nu_S = \mathrm{rk}_2\, E(S) = \#S + \mathrm{rk}_2\, C_S(K).$$

This combined with Propositions 4 and 5 gives the asserted result. □

COROLLARY. *The* $S-$*class number* $h_S(K)$ *is odd if and only if the homomorphism* ν_S *is injective.* □

2. Fields with prescribed completions

For a number field F and a prime $\mathfrak{p}$ of F (finite or infinite) an $m-$tupel $(F_\mathfrak{p}^{(1)}, \dots, F_\mathfrak{p}^{(m)})$ of finite extensions of $F_\mathfrak{p}$ in a fixed algebraic closure of $F_\mathfrak{p}$ is said to be a $\mathfrak{p}-$*prescription* over F of length m and degree n if

$$\sum_{i=1}^{m} [F_\mathfrak{p}^{(i)} : F_\mathfrak{p}] = n.$$

An extension field K of F is said to be a *solution* for the $\mathfrak{p}-$*prescription* (and the prescription is said to be *solvable*) if K has the following three properties:

(a) $[K : F] = n$,
(b) There are exactly m primes $\mathfrak{P}_1, \dots, \mathfrak{P}_m$ in K lying over $\mathfrak{p}$, and
(c) $K_{\mathfrak{P}_i} = F_\mathfrak{p}^{(i)}$ for $i = 1, \dots, m$.

Endler's result in ([En], Satz 7 and Korollar on p. 97) asserts that any prescription is solvable, and more generally, given a finite set of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ of a number field F and any $\mathfrak{p}_i-$prescriptions of degree n, there exists a number field K of degree n over F solving simultaneously all the prescriptions.

REMARK 1. We show here how to obtain from Endler's result Hasse's theorem on the existence of number fields with prescribed prime ideal factorization of (finite) sets of prime ideals of a base field. The point is that

factorizations can be prescribed in terms of completions. We recall some details. Suppose $\mathfrak{p}$ is a prime ideal of the number field F. Let e_i, f_i, m, n be positive integers satisfying

$$\sum_{i=1}^{m} e_i f_i = n. \tag{1}$$

To find an extension field K of F of degree n such that $\mathfrak{p}$ has the prime ideal decomposition

$$\mathfrak{p} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_m^{e_m} \tag{2}$$

in K, where $\mathfrak{P}_i$ is a prime ideal with degree $f(\mathfrak{P}_i|\mathfrak{p}) = f_i$, $i = 1, \ldots, m$, we set up a $\mathfrak{p}$–prescription $(F_{\mathfrak{p}}^{(1)}, \ldots, F_{\mathfrak{p}}^{(m)})$ in the following way.

Let L be an unramified extension of $F_{\mathfrak{p}}$ of degree f_i (so that L is a splitting field of the polynomial $X^{(N\mathfrak{p})^{f_i}} - X$ over the field $F_{\mathfrak{p}}$, see [O'M], 32:9). Let $F_{\mathfrak{p}}^{(i)} = L(\alpha)$, where α is a zero of an Eisenstein polynomial over L of degree e_i. Then $F_{\mathfrak{p}}^{(i)}$ is a fully ramified extension of L of degree e_i (see [O'M], 32:15) and its degree over $F_{\mathfrak{p}}$ is $n_i = e_i f_i$. The extension $F_{\mathfrak{p}}^{(i)}/F_{\mathfrak{p}}$ has the ramification index e_i and the inertia degree f_i. Hence, in a solution field K to the $\mathfrak{p}$–prescription $(F_{\mathfrak{p}}^{(1)}, \ldots, F_{\mathfrak{p}}^{(m)})$, the prime ideal $\mathfrak{p}$ has the decomposition (2).

Furthermore, given any finite set of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_k$ of F and any set of k relations of the type (1), there exists a common solution K to the related k prescriptions. Hence in K the given primes $\mathfrak{p}_i$ have prescribed prime ideal decompositions. And we can impose other extra conditions on K expressed in terms of prescriptions for primes outside $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$.

REMARK 2. We describe here the prescriptions whose solution is a field in a prescribed Witt equivalence class. This has been found in [Sz] but we give it here in a version which is slightly simplified and easier to apply.

So let $\mathcal{K}$ be a class of Witt equivalent number fields. According to [Ca] and [PSCL] the class $\mathcal{K}$ is completely determined by the following invariants

$$(\ n, r, s, g;\ (n_i, s_i),\quad i = 1, \ldots, g\ ).$$

Here s is the level of any field K in the class $\mathcal{K}$ and s_i are the levels of dyadic completions $K_{\mathfrak{p}_i}$ of K, and $n_i = [K_{\mathfrak{p}_i} : \mathbb{Q}_2]$.

We consider first the case when $s \neq 1$. We set up three prescriptions over $F = \mathbb{Q}$ of degree n corresponding to the primes $\infty, 2, P$ of $\mathbb{Q}$, where P is an arbitrary rational prime $\equiv 3 \bmod 4$.

The ∞–prescription $(\mathbb{R}^{(1)}, \ldots, \mathbb{R}^{(r+c)})$ is defined by choosing

$$\mathbb{R}^{(i)} = \mathbb{R} \quad \text{for} \quad i = 1, \ldots, r \quad \text{and} \quad \mathbb{R}^{(i)} = \mathbb{C} \quad \text{for} \quad i = r+1, \ldots, r+c.$$

The 2−prescription $(\mathbb{Q}_2^{(1)}, \dots, \mathbb{Q}_2^{(g)})$ is defined as follows.

If $n_i \equiv 1 \bmod 2$ and $s_i = 4$, take $\mathbb{Q}_2^{(i)}$ any extension of $\mathbb{Q}_2$ of degree n_i.

If $n_i \equiv 0 \bmod 2$ and $s_i = 1$, take $\mathbb{Q}_2^{(i)}$ any extension of $\mathbb{Q}_2(\sqrt{-1})$ of degree $\frac{1}{2}n_i$. Alternatively, take any unramified extension $L_i \supset \mathbb{Q}_2$ of degree $\frac{1}{2}n_i$ and set $\mathbb{Q}_2^{(i)} = L_i(\sqrt{-1})$.

If $n_i \equiv 0 \bmod 2$ and $s_i = 2$, take $\mathbb{Q}_2^{(i)}$ any unramified extension of $\mathbb{Q}_2$ of degree n_i.

Now we choose an arbitrary rational prime $P \equiv 3 \bmod 4$ and define the P−prescription $(\mathbb{Q}_P^{(1)}, \dots, \mathbb{Q}_P^{(n)})$ by setting $\mathbb{Q}_P^{(i)} = \mathbb{Q}_P$ for $i = 1, \dots, n$.

As in [Sz] we can show that the $\infty-$ $2-$ and P−prescriptions have as a solution a field K in the class $\mathcal{K}$.

Now assume that $s = 1$. Let $F = \mathbb{Q}(\sqrt{-1})$ and let $\mathfrak{q}$ be the dyadic prime of F (so that $2\mathcal{O}_F = \mathfrak{q}^2$ and $\mathfrak{q} = (1+\sqrt{-1})\mathcal{O}_F$). Then we consider the $\mathfrak{q}$−prescription $(F_\mathfrak{q}^{(1)}, \dots, F_\mathfrak{q}^{(g)})$ over F of degree $\frac{1}{2}n$, where $F_\mathfrak{q}^{(i)}$ is an arbitrary extension of $F_\mathfrak{q}$ of degree $\frac{1}{2}n_i$. The solution field K to this prescription belongs to the class $\mathcal{K}$.

PROPOSITION 7. *Let $\mathcal{K}$ be a class of Witt equivalent number fields of degree $n > 1$. Let $\mathcal{T}$ be a finite set of odd rational primes when $s \neq 1$, or a finite set of nondyadic primes of $\mathbb{Q}(\sqrt{-1})$ when $n > 2$ and $s = 1$. Let $\mathcal{P}$ be a set of prescriptions for primes in $\mathcal{T}$. Then there exists a field K in the class $\mathcal{K}$ with the property that all the primes in $\mathcal{T}$ have prescribed in $\mathcal{P}$ prime ideal decompositions in K.*

PROOF. A common solution K to the $\infty-$, $2-$, and P−prescriptions in Remark 2 together with the $\mathfrak{p}$−prescriptions, $\mathfrak{p} \in \mathcal{T}$, described in Remark 1, will do. □

3. Even degree Witt classes

For a finite set $Q = \{q_1, \dots, q_k\}$ of rational primes and for a number field K we write $\Omega_Q(K)$ for the set of all primes $\mathfrak{q}$ of K lying over the primes in the set Q.

THEOREM. *Let $\mathcal{K}$ be a class of Witt equivalent number fields of degree n and let Q be a finite set of rational odd primes. If n is even and $\mathcal{K}$ is not the singleton class consisting of the field $\mathbb{Q}(\sqrt{-1})$, then $\mathcal{K}$ contains a field K with even S−class number, where*

$$S = \Omega_\infty(K) \cup \Omega_2(K) \cup \Omega_Q(K).$$

In fact, given a positive integer t, the class $\mathcal{K}$ contains a field with the 2–rank of S–class group at least t.

PROOF. To get a field in the class $\mathcal{K}$ with the 2–rank of the S–class group at least t, we use Proposition 7 to ensure that the constructed field has $\ker \nu_S$ of 2–rank at least t, and then we apply Proposition 6.

Let $Q = \{q_1, \dots, q_k\}$. To start the construction let us take an arbitrary positive integer t, and pick up rational primes $p_1, \dots, p_t$ all congruent to 1 mod $8q_1 \cdots q_k$.

Observe that, for every number field K, each prime p_i is a square at all the primes in the set $S = \Omega_\infty(K) \cup \Omega_2(K) \cup \Omega_Q(K)$.

Hence if $p_i \in E(S)$, then $p_i \in \ker \nu_S$. Thus we need a field K in the given class $\mathcal{K}$ with the property that

$$p_i \in E(S), \quad i = 1, \dots, t,$$

and, moreover, the square classes of the p_i's in K are multiplicatively independent in K^*/K^{*2}.

The first condition will be satisfied if we require that for each p_i there is a prime ideal $\mathfrak{q}_i$ of K satisfying

$$(p_i) = \mathfrak{q}_i^2, \quad i = 1, \dots, t.$$

This is why we assume that the field degree n is even. For if f_i is the degree of $\mathfrak{q}_i$, we have $n = 2f_i$.

The second condition is more involved. For each nonempty set

$$I = \{i_1, \dots, i_k\} \subseteq \{1, \dots, t\}$$

we write $a_I = p_{i_1} \cdots p_{i_k}$ and we choose a rational prime p_I outside the set $\{p_1, \dots, p_t\}$ with the Legendre symbol

$$\left(\frac{a_I}{p_I}\right) = -1.$$

We require that each prime p_I splits completely in the solution field K.

Now suppose the square classes in K containing the primes $p_1, \dots, p_t$ are multiplicatively dependent. Then for a set I we would have $a_I \in K^{*2}$, while $a_I \notin K_{\mathfrak{p}}^{*2}$ for each prime $\mathfrak{p}$ of K lying over p_I, a contradiction.

According to Proposition 7 there is a number field K in the class $\mathcal{K}$ with the prescribed splitting behavior of the primes $p_1, \dots, p_t$ and of the p_I's. Then

the square classes of $p_1, \ldots, p_t$ are in the group $\ker \nu_S$ and they generate a subgroup of 2–rank t. □

COROLLARY. *Let $\mathcal{K}$ be a class of Witt equivalent number fields of degree n. If n is even and $\mathcal{K}$ is not the singleton class consisting of the field $\mathbb{Q}(\sqrt{-1})$, then $\mathcal{K}$ contains a field K with even class number. In fact, given any $t \geqslant 1$, there is a field $K \in \mathcal{K}$ with the 2–rank of class group at least t.* □

The following example shows that we cannot expect the fields in a Witt class to have arbitrarily prescribed class groups of a given 2–rank.

EXAMPLE. The table below gives the representatives of the Witt equivalence classes of quadratic number fields with even class numbers, whenever available. When the class number is 4, we distinguish between the cyclic and Klein four-group of the class group $C(K)$. The field $\mathbb{Q}(\sqrt{d})$ is represented by the squarefree number d.
A blank entry occurs when there does not exist a field with the required property. The situation in the classes VI and VII was known from the very beginning. In particular, the class VI represented by $\mathbb{Q}(\sqrt{-17})$ consists exclusively of fields with class numbers divisible by 4 (see [CPS], p. 89).

The nonexistence of a field in class IV with Klein four-group as class group has not been noticed earlier. It is known that there are exactly 54 imaginary quadratic number fields $\mathbb{Q}(\sqrt{d})$ with class number 4. They satisfy $14 \leqslant -d \leqslant 1555$ (cf. [Ar]). Using the computational system Pari/GP one checks that none of the 54 fields with Klein four-group as class group belongs to the class IV.
On the other hand, the field $\mathbb{Q}(\sqrt{-255})$ belongs to IV and has the ordinary class group $C_6 \oplus C_2$ of 2–rank two.

Table 1
Representatives of quadratic Witt classes with prescribed class groups

	I	II	III	IV	V	VI	VII
C_1	17	2	7	−7	−2		−1
C_2	65	10	15	−15	−10		
C_4	145	82	791	−39	−14	−17	
$C_2 \oplus C_2$	1105	130	231		−21	−33	

We do not know at the moment whether in the Theorem the restriction that n be even can be removed. In the case of cubic number fields there are

8 Witt equivalence classes and we know representatives having ideal class number one (see [JMS], corrigendum). Here we are interested in going in the opposite direction and to produce the representatives with *even* ideal class numbers. Using Pari/GP one can find such examples with class groups C_2, C_4 or $C_2 \oplus C_2$.

The table below gives the coefficients (p, q) of the cubic polynomial $X^3 + pX + q$ whose zero generates a field having the Witt equivalence invariant given in the first column (in the notation of [Sz]) and the class group C_1, C_2, C_4 or $C_2 \oplus C_2$.

Table 2

Representatives of cubic Witt classes with prescribed class groups

	C_1	C_2	C_4	$C_2 \oplus C_2$
I	$(1,1)$	$(7,1)$	$(23,1)$	$(26,2)$
II	$(5,4)$	$(61,4)$	$(157,4)$	$(85,4)$
III	$(1,4)$	$(17,4)$	$(41,4)$	$(81,4)$
IV	$(11,4)$	$(19,4)$	$(83,4)$	$(227,4)$
V	$(-3,1)$	$(-25,1)$	$(-71,1)$	$(-65,1)$
VI	$(-3,4)$	$(-19,4)$	$(-139,4)$	$(-179,4)$
VII	$(-7,4)$	$(-79,4)$	$(-31,4)$	$(-631,4)$
VIII	$(-13,4)$	$(-317,4)$	$(-149,4)$	$(-1021,4)$

References

[Ar] S. Arno, *The imaginary quadratic fields of class number* 4, Acta Arithmetica, **60** (1992), 321–334.

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

[Con] P. E. Conner, *The minimal number of wild primes in a reciprocity equivalence*, manuscript.

[CPS] P. E. Conner, R. Perlis, and K. Szymiczek, *Wild sets and 2-ranks of class groups*, Acta Arithmetica, **79** (1997), 83–91.

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

[En] O. Endler, *Endlich separable Körpererweiterungen mit vorgeschriebenen Bewertungsfortsetzungen. I*, Abh. Math. Sem. Hamburg, **33** (1969), 80–101.

[H] E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Leipzig (1923).

[JMS] S. Jakubec, F. Marko, and K. Szymiczek, *Parity of class numbers and Witt equivalence of quartic fields*, Math. Comput., **64** (1995), 1711–1715; corrigendum, ibid., **66** (1997) pp. 927.

[O'M] O. T. O'Meara, *Introduction to Quadratic Forms*, Grundlehren der mathematischen Wissenschaften, **117**, Springer-Verlag, Berlin–Heidelberg–New York (1971).

[PSCL] R. Perlis, K. Szymiczek, P. E. Conner, and R. Litherland, *Matching Witts with global fields*, Contemp. Math., **155** (1994), 365–387.

[Sz] K. Szymiczek, *Witt equivalence of global fields*, Commun. Algebra **19(4)** (1991), 1125–1149.

Instytut Matematyki
Uniwersytet Śląski
Bankowa 14
40 007 Katowice
Poland

e-mail:
szymicze@ux2.math.us.edu.pl