\( p \)-Ranks of Class Groups of Witt Equivalent Number Fields

Kazimierz Szymiczek*

Instytut Matematyki, Uniwersytet Śląski, Bankowa 14, 40 007 Katowice, Poland
E-mail: szymiczek@ax2.math.us.edu.pl

Communicated by P. Roquette
Received November 22, 1998

We prove that, for each prime \( p \) dividing \( n \), every infinite class of Witt equivalent number fields of degree \( n \geq 2 \) contains a field with the \( p \)-rank of the ideal class group exceeding any given number. 1999 Academic Press

Key Words: Class group; Witt equivalence.

INTRODUCTION

We know from [CPS] that each infinite class of Witt equivalent quadratic number fields contains a field whose class group has 2-rank as large as we wish. This has been generalized in [Sz2] to number fields of arbitrary even degree \( n \geq 2 \) and to 2-ranks of \( S \)-class groups.

Here we further generalize that result to fields of arbitrary degree \( n \) and \( p \)-ranks of \( S \)-class groups for prime factors \( p \) of \( n \). We prove that for each prime \( p \) dividing \( n \) and for each infinite class \( \mathcal{K} \) of Witt equivalent number fields of degree \( n \) there exists a field in the class \( \mathcal{K} \) with the \( p \)-rank of ideal class group exceeding any given number. Alternatively, by a result of Golod and Shafarevich, the class \( \mathcal{K} \) contains a field with infinite Hilbert \( p \)-class field tower.

In Section 1 we collect some information on the Witt equivalence of number fields and on the existence of number fields with prescribed completions. In Section 2 we prove the main theorem and interpret the result in terms of Hilbert class field towers. In Section 3 we give examples and discuss related results and open questions.

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

Witt Equivalence of Number Fields. We separate algebraic number fields into classes of Witt equivalent fields. Two fields \( K \) and \( L \) are said to be Witt equivalent if their Witt rings of bilinear symmetric forms are isomorphic. For number fields \( K \) and \( L \) it is natural to rephrase this definition in terms of Hilbert symbol preserving maps \( (t, T) \), where \( t \) is a group isomorphism \( t: K^*/K^{*2} \to L^*/L^{*2} \) between the square-class groups of \( K \) and \( L \), and \( T \) is a bijection \( T: \Omega(K) \to \Omega(L) \) between the sets \( \Omega(K) \), \( \Omega(L) \) of all primes (including infinite primes), with \((t, T)\) preserving Hilbert symbols in the sense that

\[
(a, b)_p = (ta, tb)_{T_p}
\]

for all \( a, b \) in \( K^*/K^{*2} \) and all \( p \) in \( \Omega(K) \) (see [PSCL, Theorem 1]). The main result on Witt equivalence of number fields is the following Hasse Principle (see [PSCL, Section 6]):

Two number fields \( K \) and \( L \) are Witt equivalent if and only if there is a bijective matching of primes of \( K \) and \( L \) (including infinite primes) such that, if \( p \in \Omega(K) \) and \( q \in \Omega(L) \) correspond to each other, then the completions \( K_p \) and \( L_q \) are Witt equivalent.

Two simple consequences of the Hasse Principle, not obvious otherwise, are the following. First, the Witt equivalence of number fields preserves the field degrees over \( \mathbb{Q} \), and second, the number of Witt equivalence classes of number fields of a given degree is finite.

More generally, as a consequence of the Hasse Principle, the following field invariants form a complete set of invariants of Witt equivalence,

\[
(n, r, s, g; (n_i, s_i), i = 1, ..., g),
\]

where \( n \) is the field degree over \( \mathbb{Q} \), \( r \) is the number of infinite real primes, \( s \) is the level of the field (the smallest number of terms in a representation of \(-1\) as a sum of squares or zero if there is no such representation), \( g \) is the number of dyadic primes, and \( n_i, s_i \) are local dyadic degrees and the corresponding local dyadic levels (see [Sz1] for details).

Solvable Prescriptions. Here we recall a valuation-theoretic result of O. Endler [En] used in [Sz1] to construct fields with prescribed Witt equivalence invariants. Actually, for our present applications, we need a slightly more flexible version of the result.

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

\[
\sum_{i=1}^{m} [K_p^{(i)}: K_p] = n.
\]
The prescription is said to be solvable if there exists an extension $F$ of $K$ with the following three properties:

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

Observe that if $(K_{i}^{(1)}, \ldots, K_{i}^{(m)})$ is a $p$-prescription and the extension $K_{i}^{(1)}/K_p$ has the ramification index $e_i$ and the inertia degree $f_i$, then we have $\sum_{i=1}^{m} e_i f_i = n$ and $p$ has the prime ideal decomposition

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

in the solution field $F$. Hence prime ideal decompositions can be described in terms of prescriptions.

Endler proved that any prescription is solvable, and more generally, given a finite set of primes $p_1, \ldots, p_k$ of a number field $K$ and any $p_i$-prescriptions of degree $n$, there exists a number field $F$ of degree $n$ over $K$ solving simultaneously all the prescriptions ([En, Satz 7 and Korollar on p. 97]).

As noted in [Sz1], each class $\mathcal{K}$ of Witt equivalent number fields contains a field $F$ which is a solution to a set of prescriptions over $\mathbb{Q}$ or over $\mathbb{Q}(\sqrt{-1})$. Here we will use Endler's theorem to construct, in a given Witt equivalence class, fields with special properties. Recall that if $\mathcal{K}$ is a class of Witt equivalent number fields, then all fields in $\mathcal{K}$ have the same degree $n$ and the same level $s$. The class $\mathcal{K}$ is finite if and only if either $\mathbb{Q} \in \mathcal{K}$ or $\mathbb{Q}(\sqrt{-1}) \in \mathcal{K}$. Actually, in each of these two exceptional cases, $\mathcal{K}$ is a singleton class.

**Proposition.** Let $\mathcal{K}$ be an infinite class of Witt equivalent number fields of degree $n$ and level $s$. Let $\mathcal{F}$ 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 $s = 1$. Then there exists a field $F$ in the class $\mathcal{K}$ with the property that all the primes in $\mathcal{F}$ have prescribed prime ideal decompositions in $F$.

**Proof.** A field $F$ satisfying all the requirements can be obtained as a common solution to the set $\mathcal{P} = \mathcal{P}_1 \cup \mathcal{P}_2$ of prescriptions, where the set $\mathcal{P}_1$ describes a field in the class $\mathcal{K}$ and $\mathcal{P}_2$ is the set of $p$-prescriptions for $p \in \mathcal{F}$ yielding the prescribed prime ideal decompositions. For details see [Sz1] or [Sz2].

2. **$p$-RANKS OF CLASS GROUPS IN WITT CLASSES**

Recall that for a finite Abelian group $A$ and for a prime number $p$, the $p$-rank $rk_p A$ is defined to be the dimension dim $A/A^p$ of the factor group $A/A^p$ viewed as a vector space over the prime field of $p$ elements.
For a finite set \( Q = \{q_1, \ldots, q_k\} \) of rational primes and for a number field \( F \) we write \( \Omega_q(F) \) for the set of all primes \( q \) of \( F \) lying over the primes in the set \( Q \).

**Theorem.** Let \( \mathcal{X} \) be an infinite class of Witt equivalent number fields of degree \( n \) and let \( p \) be a prime factor of \( n \). Let \( Q \) be a finite set of rational odd primes. Then for any positive integer \( r \) there is a field \( F \in \mathcal{X} \) such that for \( S = \Omega_{\neq q}(F) \cup \Omega_q(F) \) we have

\[
\text{rk}_p C(S(F)) = \text{rk}_p C(F) > r.
\]

**Proof.** Our construction of \( F \) will use the above proposition and a theorem of Roquette and Zassenhaus on the existence of fields with large \( p \)-ranks of class groups (see [RZ] or [N, Theorem 8.10, p. 461]). According to that result, there is a constant \( c = c(n) \) depending only on \( n \), with the property that for any field \( F \) of degree \( n \) the \( p \)-rank of the ordinary class group \( C(F) \) satisfies

\[
\text{rk}_p C(F) \geq t(F, p) - c(n),
\]

where \( t(F, p) \) is the number of rational primes which are \( p \)th powers of integral ideals in \( F \). One can take \( c(n) = 2(n - 1) \).

Let \( r \) be a positive integer. We choose a finite set \( \mathcal{T} \) of rational primes congruent to \( 3 \) (mod \( 4 \)) which is disjoint from the given set \( Q \). We require that \( t := \# \mathcal{T} > c(n) + r \).

Depending on whether \( s \neq 1 \) or \( s = 1 \), we set up \( t \) prescriptions over \( \mathcal{Q} \) or over \( \mathcal{Q}(\sqrt{-1}) \), respectively, requiring that each prime in \( \mathcal{T} \) becomes a \( p \)th power of an ideal in the solution field. Moreover, we set up prescriptions for all primes in the set \( \mathcal{Q} \) requiring that each prime in \( \mathcal{Q} \) becomes an \( \ell \)th power of an ideal in the solution field, where \( \ell \) is coprime to \( p \) (we can set \( \ell = 1 \), say). According to the proposition, there is a field \( F \) in the class \( \mathcal{X} \) in which all the primes in \( \mathcal{T} \cup \mathcal{Q} \) have prescribed prime ideal decompositions. Thus, by the theorem of Roquette and Zassenhaus, we get

\[
\text{rk}_p C(F) \geq t(F, p) - c(n) \geq t - c(n) > r.
\]

On the other hand, for each prime \( q \in \Omega_q(F) \) its class \( [q] \) in the class group \( C(F) \) satisfies

\[
[q]^{\ell} = 1,
\]

where \( p \nmid \ell \). Hence, if \( sx + yp = 1 \) for some rational integers \( x, y \), then in \( C(F) \) we have

\[
[q] = [q]^{sx + yp} = ([q]^s)^p,
\]
that is, $\{q\} \in C(F)^p$ for all finite primes in the set $S$. Write $\langle S \rangle$ for the subgroup of $C(F)$ generated by the classes $\{q\}$ with $q \in S$. Then we have

$$C_S(F) = C(F)/\langle S \rangle \quad \text{and} \quad C_S(F)/C_S(F)^p \cong C(F)/\langle S \rangle \cdot C(F)^p$$

$$= C(F)/C(F)^p,$$

the latter by $\langle S \rangle \subseteq C(F)^p$. Hence

$$\text{rk}_p C_S(F) = \text{rk}_p C(F) > r,$$

as required. 

The theorem admits a reformulation in terms of Hilbert class fields. According to a theorem of Golod and Shafarevich (see [R, Theorem 3]) there is a function $\gamma(n)$ with the property that all number fields of degree $n$ with finite Hilbert $p$-class field towers have the $p$-ranks of class groups bounded above by $\gamma(n)$. The theorem supplies in each infinite Witt equivalence class a field with an arbitrarily large $p$-rank of class group. Hence we get the following corollary.

**Corollary.** Let $\mathcal{K}$ be an infinite class of Witt equivalent number fields of degree $n$ and let $p$ be a prime factor of $n$. Then there is a field $F \in \mathcal{K}$ with infinite Hilbert $p$-class field tower.

### 3. Comments and Examples

**Example 1.** Here we illustrate the theorem in the case $n = p = 3$ (for an example in the case $n = p = 2$ see [Sz2]). In each Witt equivalence class of degree 3 we give examples of cubic fields with 3-ranks of class group 0, 1 or 2. Cubic fields are known to split into eight Witt equivalence classes numbered here I, III, ..., VIII (see [Sz1] for details). The equivalence classes can be viewed here simply as the classes of cubic fields Witt equivalent to the appropriate cubic fields with class number one listed in the column of $C_1$. Table I gives the coefficients $(p, q)$ of the cubic polynomial $X^3 + pX + q$ whose zero generates a field in one of the eight classes I, II, ..., VIII with the class group $C_1$, $C_3$, $C_9$, or $C_3 \oplus C_3$. The class groups have been computed by using the Pari/GP computational system.

The question arises whether the result in the theorem still holds when we do not assume that $p$ divides $n$. In the case $n = 3$, $p = 2$ we have found in [Sz2] representatives of the eight cubic Witt equivalence classes with class groups $C_2$, $C_4$, or $C_2 \oplus C_2$. Example 2 gives a similar data in the case $n = 2$, $p = 3$.
TABLE I
Representatives of Cubic Witt Classes with
Prescribed Class Groups

<table>
<thead>
<tr>
<th></th>
<th>$C_1$</th>
<th>$C_2$</th>
<th>$C_9$</th>
<th>$C_3 \oplus C_3$</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>(1,1)</td>
<td>(15,1)</td>
<td>(69,3)</td>
<td>(51,1)</td>
</tr>
<tr>
<td>II</td>
<td>(5,4)</td>
<td>(33,48)</td>
<td>(33,144)</td>
<td>(33,640)</td>
</tr>
<tr>
<td>III</td>
<td>(1,4)</td>
<td>(33,12)</td>
<td>(33,476)</td>
<td>(33,260)</td>
</tr>
<tr>
<td>IV</td>
<td>(11,4)</td>
<td>(27,4)</td>
<td>(1211,4)</td>
<td>(339,4)</td>
</tr>
<tr>
<td>V</td>
<td>(−3,1)</td>
<td>(−21,1)</td>
<td>(−87,1)</td>
<td>(393,1)</td>
</tr>
<tr>
<td>VI</td>
<td>(−3,4)</td>
<td>(−39,8)</td>
<td>(−351,24)</td>
<td>(−1119,8)</td>
</tr>
<tr>
<td>VII</td>
<td>(−7,4)</td>
<td>(−49,42)</td>
<td>(−385,42)</td>
<td>(−441,42)</td>
</tr>
<tr>
<td>VIII</td>
<td>(−13,4)</td>
<td>(−69,20)</td>
<td>(−465,20)</td>
<td>(−921,8)</td>
</tr>
</tbody>
</table>

Example 2. Table II gives representatives of the seven Witt equivalence classes of quadratic number fields with 3-ranks 0, 1, or 2 of the class group $C(F)$. We insist on giving examples with the class groups $C_1$, $C_3$, $C_9$, or $C_1 \oplus C_3$ whenever available. The field $F = \mathbb{Q}(\sqrt{d})$ is represented by the squarefree number $d$. We number the Witt equivalence classes I, II, ..., VII. The classes can be characterized in terms of $d$ (see [Sz1] or [PSCL]) but here we can view them as the seven classes of fields Witt equivalent to the fields $\mathbb{Q}(\sqrt{d})$, where $d = 17, 2, 7, −7, −2, −17, −1$, respectively. As we have already mentioned, class VII consists only of $\mathbb{Q}(\sqrt{-1})$. An $\emptyset$ entry occurs when there does not exist a field with the required class group. The class IV contains no field with the class group $C_1 \oplus C_3$.

By a recent result (see [ARW]) there are exactly 34 imaginary quadratic number fields with class number 9. Using Pari/GP one can check that 33 of them have cyclic class groups. The only imaginary quadratic number field with class group $C_1 \oplus C_3$ is $\mathbb{Q}(\sqrt{-4027})$, and this belongs to class V.

On the other hand the field $\mathbb{Q}(\sqrt{-6583})$ belongs to class IV and has class group $C_{15} \oplus C_1$ of 3-rank 2 (another example is the field $\mathbb{Q}(\sqrt{-5703})$ in the same class with class group $C_{18} \oplus C_3$).

TABLE II
Representatives of Quadratic Witt Classes with Prescribed Class Groups

<table>
<thead>
<tr>
<th></th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
<th>V</th>
<th>VI</th>
<th>VII</th>
</tr>
</thead>
<tbody>
<tr>
<td>$C_1$</td>
<td>17</td>
<td>2</td>
<td>7</td>
<td>−7</td>
<td>−2</td>
<td>$\emptyset$</td>
<td>−1</td>
</tr>
<tr>
<td>$C_3$</td>
<td>257</td>
<td>142</td>
<td>79</td>
<td>−23</td>
<td>−59</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>$C_9$</td>
<td>1129</td>
<td>13009</td>
<td>3719</td>
<td>−199</td>
<td>−419</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
</tr>
<tr>
<td>$C_1 \oplus C_3$</td>
<td>32009</td>
<td>62501</td>
<td>43063</td>
<td>$\emptyset$</td>
<td>−4027</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
</tr>
</tbody>
</table>
The class VI, represented by the field $\mathbb{Q}(\sqrt{-17})$, is known to contain only fields with class numbers divisible by 4 (see [CPS]).

However, for $d = -17$, $-89$, $-5857$ we get fields in the class VI with the 3-ranks of class groups 0, 1, and 2, respectively. For we have

$$C(\mathbb{Q}(\sqrt{-17})) = C_4, \quad C(\mathbb{Q}(\sqrt{-89})) = C_4 \oplus C_3,$$

$$C(\mathbb{Q}(\sqrt{-5857})) = C_4 \oplus C_3 \oplus C_3.$$

Let $K$ be a class of Witt equivalent number fields of degree $n$. The theorem shows that if $n$ is even, the class $K$ contains a field with even class number. However, the following question remains unanswered.

**Question 1.** Is it true that each class $K$ of Witt equivalent number fields of odd degree $n > 1$ contains a field with prescribed parity of class number?

The answer is yes for $n = 3$. Example 1 answers the question when we require odd class numbers and in [Sz2] we have found representatives of the eight cubic Witt equivalence classes with even class numbers (and each of the class groups $C_2$, $C_4$, or $C_2 \oplus C_2$).

On the other hand, for each even number $n$ there are Witt equivalence classes of degree $n$ consisting exclusively of fields with even class numbers. The only known examples of such classes are the ones satisfying the so-called Conner’s Level Condition (CLC). A class $K$ satisfies CLC if for each field $F$ in the class

$$s(F) = 2 \quad \text{and} \quad s(F_{p_i}) = 1, \quad i = 1, \ldots, g,$$

where $F_{p_1}, \ldots, F_{p_g}$ are all of the dyadic completions of the field $F$. For a proof that CLC implies evenness of class number see [JMS, corrigendum]. The following question remains open.

**Question 2.** Is it true that each class $K$ of Witt equivalent number fields of even degree $n$ consisting exclusively of fields with even class numbers has to satisfy CLC?

The answer is known to be yes for $n = 2$ and $n = 4$ (see [JMS]).

**REFERENCES**


