Marzena Ciemała
Natural homomorphisms of Witt rings of orders in algebraic number fields


Persistent URL: [http://dml.cz/dmlcz/131463](http://dml.cz/dmlcz/131463)

**Terms of use:**

© Mathematical Institute of the Slovak Academy of Sciences, 2004

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use.*

This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* [http://project.dml.cz](http://project.dml.cz)
NATURAL HOMOMORPHISMS OF WITT RINGS OF ORDERS IN ALGEBRAIC NUMBER FIELDS

MARZENA CIEMALA

(Communicated by Stanislav Jakubec)

ABSTRACT. Let \( \mathcal{O} \) be an order and \( \mathcal{R} \) be the maximal order in a nonreal quadratic number field \( K \). We prove that the natural homomorphism \( \phi: W\mathcal{O} \rightarrow W\mathcal{R} \) of Witt rings is surjective provided the discriminant of the field and the conductor of the order are relatively prime.

For a commutative ring \( A \) let \( WA \) be the Witt ring of nondegenerate symmetric bilinear forms on finitely generated projective modules over \( A \), as defined by Knebusch in 1970. We shall use the notation and terminology of Milnor and Husemoller’s book [5]. Any ring homomorphism \( A \rightarrow B \) induces the natural Witt ring homomorphism \( \phi: WA \rightarrow WB \) defined by sending the class \( [E] \) of an \( A \)-space \( E \) to the class \( [E \otimes_A B] \) of the \( B \)-space \( E \otimes_A B \). It is well known that for the maximal order \( \mathcal{R} \) of a number field \( K \) the ring homomorphism \( W\mathcal{R} \rightarrow WK \) is injective and the cokernel turns out to be \( C/C^2 \), where \( C \) is the ideal class group of \( K \) ([5; pp. 93–94]). On the other hand, when \( \mathcal{O} \) is a nonmaximal order in \( K \), very little is known about the ring homomorphisms \( W\mathcal{O} \rightarrow W\mathcal{R} \) or \( W\mathcal{O} \rightarrow WK \). During the 4th Czech and Polish Conference on Number Theory in Cieszyn 2002, K. Szymiczek posed the problem of identifying the kernel and the cokernel of the homomorphism \( W\mathcal{O} \rightarrow W\mathcal{R} \) (see [8]). In an attempt to answer partially this question we study the natural ring homomorphism

\[
\phi: W\mathcal{O} \rightarrow W\mathcal{R}
\]

in the case of orders of quadratic number fields. An order \( \mathcal{O} \) of \( K \) is a subring of \( \mathcal{R} \) which is a free abelian group of rank \( [K : \mathbb{Q}] \) (see [7; p. 72]). If \( \mathcal{O} \neq \mathcal{R} \), \( \mathcal{O} \) is strictly contained in \( \mathcal{R} \), and we cannot in general expect that \( \phi \) is surjective. Nevertheless, we will show that \( \phi \) is surjective for a class of orders \( \mathcal{O} \) in any nonreal quadratic number field.

2000 Mathematics Subject Classification: Primary 11E81, 19G12.

Keywords: Witt ring, orders in number fields, bilinear forms on ideals.

The work supported by the KBN grant 1 P03A 02526.
Let $K$ be a quadratic number field, that is, $K = \mathbb{Q}(\sqrt{d})$, where $d$ is a square-free integer, and let $\mathcal{O} = \mathbb{Z}[\omega]$ be the maximal order in $K$. Any order $\mathcal{O}$ in $K$ is of the form $\mathcal{O} = \mathbb{Z}[f\omega]$, where $f$ is a natural number. The conductor $f$ of the ring extension $\mathcal{O} \subseteq \mathcal{R}$ is the ideal $f\mathcal{R}$. Let $d(K)$ denote the discriminant of $K$ and $p_1, \ldots, p_t$ be all, pairwise distinct, prime divisors of $d(K)$. We agree that $p_1 = 2$ whenever $d \equiv 3 \pmod{4}$.

The result reads as follows.

**Theorem 1.** Let $K$ be a nonreal quadratic number field. Let $\mathcal{O} = \mathbb{Z}[f\omega]$ be an order in $K$ with conductor $f\mathcal{R}$ in the maximal order $\mathcal{R} = \mathbb{Z}[\omega]$ in $K$. If $\gcd(f, d(K)) = 1$, then $\phi(W\mathcal{O}) = WR$.

Due to the injectivity of $WR \to WK$, the Witt ring $WR$ is usually viewed as a subring of $WK$. We adopt the convention, and as a consequence we can say that when $K$ is a nonreal quadratic field distinct from $\mathbb{Q}(\sqrt{-1})$, the ring $WR$ is additively generated by the set

$$\{(1), (p_1), \ldots, (p_{t-1})\},$$

or by $\{(1), (2)\}$ if $K = \mathbb{Q}(\sqrt{-1})$, (see [2; pp. 116–117]).

Observe that without assuming $WR \subseteq WK$ we could not consider the class $\langle p \rangle$ to lie in $WR$. For a ring $A$ and $a \in A$ we have $\langle a \rangle \in WA$ if and only if $a$ is an invertible element of $A$. One consequence of assuming that $WR \subseteq WK$ is that our homomorphism $\phi: W\mathcal{O} \to WR$ assumes values in $WK$. So, to prove the theorem, we must show that the generators (1) lie in the image of $\phi$. For this we use the following two lemmas.

**Lemma 2.** Let $\mathcal{O}$ be an order in a number field $K$ and $I$ an ideal in $\mathcal{O}$ such that $I^2 = \langle a \rangle$ for some $a \in \mathcal{O}$, $a \neq 0$. Then $\beta: I \times I \to \mathcal{O}$ given by

$$\beta(x, y) := \frac{xy}{a} \quad \text{for all } x, y \in I$$

is a nonsingular bilinear form on $I$ and so $(I, \beta)$ is an inner product space over $\mathcal{O}$.

**Proof.** The ideal $I^2$ is additively generated by the elements $xy$ where $x, y \in I$, and hence $xy \in \langle a \rangle$ for $x, y \in I$. Thus $\beta$ assumes the values in $\mathcal{O}$. Since $I^2$ is a nonzero principal ideal, $I$ is invertible, and hence is a projective $\mathcal{O}$-module ([6; p. 26, Proposition 1.15]). Clearly, $I$ is a finitely generated $\mathcal{O}$-module. In order to prove the lemma it remains to show that the adjoint homomorphism $\hat{\beta}: I \to I^*$, where $I^* = \text{Hom}_\mathcal{O}(I, \mathcal{O})$, is an isomorphism of $\mathcal{O}$-modules.

First we show that $\hat{\beta}$ is a surjective map. Let $\varphi \in I^*$. Since $\varphi$ is $\mathcal{O}$-linear,

$$x\varphi(y) = \varphi(xy) = y\varphi(x)$$
NATURAL HOMOMORPHISMS OF WITT RINGS

for all \( x, y \in I \). Hence there exists a number \( c \in K \) such that \( \varphi(x) = c \) for all \( x \in I \), \( x \neq 0 \), that is \( \varphi(x) = cx \) for \( x \in I \). In particular, taking \( x = a \), we get \( c = \frac{\varphi(a)}{a} \). Since \( a \in I^2 \) there exist \( x_i, y_i \in I \) for which \( a = \sum x_i y_i \). Hence

\[
\varphi(a) = \sum \varphi(x_i y_i) = \sum x_i \varphi(y_i) \in I
\]

and

\[
\hat{\beta}(\varphi(a))(x) = \beta(\varphi(a), x) = \frac{\varphi(a)}{a} x = \varphi(x) \quad \text{for all} \quad x \in I.
\]

Hence \( \hat{\beta}(\varphi(a)) = \varphi \), which shows that \( \hat{\beta} \) is a surjection. Further, if \( \hat{\beta}(m) = 0 \) for some \( m \in I \), then

\[
\beta(m, n) = 0 \quad \text{for all} \quad n \in I.
\]

Hence \( mn = 0 \) for every \( n \in I \). Since \( \mathcal{O} \) is an integral domain and \( I \) is a nonzero ideal, we get \( m = 0 \). This implies injectivity of \( \hat{\beta} \) and finishes the proof of lemma. \( \Box \)

**Lemma 3.** Let \( K \) be a quadratic field. Let \( p \) be a prime number such that \( p \mid d(K) \) and \( p \nmid f \) where \( f = fI[\omega] \) is the conductor of the ring extension \( \mathcal{O} \subset \mathcal{R} \). Then there exist a prime ideal \( q \subset \mathcal{O} \) and a nonsingular bilinear form \( \beta \) on \( q \) such that \( \phi(\langle q, \beta \rangle) = \langle p \rangle \).

**Proof.** Since \( p \mid d(K) \), the ideal \( p\mathbb{Z} \) ramifies in \( \mathcal{R} \). Hence there exists a prime ideal \( p \) in \( \mathcal{R} \) such that \( p^2 = p\mathcal{R} \). We claim that \( p + f = \mathcal{R} \). Otherwise \( p + f \nsubseteq \mathcal{R} \), and since \( p \) is maximal, we get \( f \subset p \) and \( f \in p \). Since \( p \nmid f \), the ideals \( f \) and \( p\mathcal{R} \) are relatively prime and so

\[
\mathcal{R} = f + p\mathcal{R} \subset p,
\]

which is a contradiction. Hence \( p + f = \mathcal{R} \).

Write \( I_1(\mathcal{R}) \) and \( I_1(\mathcal{O}) \) for the multiplicative semigroups of invertible ideals relatively prime to the conductor \( f \) in \( \mathcal{R} \) and \( \mathcal{O} \), respectively. Since \( \psi: I_1(\mathcal{R}) \to I_1(\mathcal{O}) \), given by the formula \( \psi(I) = I \cap \mathcal{O} \) for \( I \in I_1(\mathcal{R}) \), is a semigroup isomorphism [3], we obtain

\[
p\mathcal{R} \cap \mathcal{O} = p^2 \cap \mathcal{O} = \psi(p^2) = (\psi(p))^2 = (p \cap \mathcal{O})^2 = q^2
\]

for the prime ideal \( q = p \cap \mathcal{O} \) in \( \mathcal{O} \). We are going to show that \( p\mathcal{R} \cap \mathcal{O} = p\mathcal{O} \). Let \( \alpha \in p\mathcal{R} \cap \mathcal{O} \) and \( \alpha = p(a + b\omega) \) for some \( a, b \in \mathbb{Z} \). Since \( \gcd(f, p) = 1 \), we get

\[
\alpha \in \mathcal{O} \iff f \mid pb \iff f \mid b.
\]

Hence \( \alpha \in p\mathcal{O} \) and \( p\mathcal{R} \cap \mathcal{O} \subseteq p\mathcal{O} \). The opposite inclusion is obvious. Since the condition \( q^2 = p\mathcal{O} \) is satisfied, Lemma 2 implies that the formula

\[
\beta(a, b) = \frac{ab}{p}, \quad a, b \in q,
\]

for all \( a, b \in q \).
defines a nonsingular bilinear form $\beta$ on $q$. Consider the class $\langle q \rangle := \langle (q, \beta) \rangle \in \mathcal{W}O$ and its image $\phi(q) = \langle q \otimes_\mathcal{O} K \rangle$ in $\mathcal{W}K$. The $K$-module $q \otimes K$ is free and one-dimensional. It is generated as a $K$-module by the element $p \otimes 1$. The matrix of $q \otimes_\mathcal{O} K$ in the basis $(p \otimes 1)$ equals $(p)$ and hence $\langle q \otimes_\mathcal{O} K \rangle = \langle p \rangle$, as desired.

To prove the theorem we must show that the generators in the list (1) lie in the image of $\phi$. Obviously $\langle 1 \rangle \in \text{im} \phi$. Let $p$ be a prime number and $p \mid d(K)$. Since $\gcd(f, d(K)) = 1$, we have $p \nmid f$ and, by Lemma 3, $\langle p \rangle \in \text{im} \phi$, as required.

Finally, we observe that for some special quadratic number fields $K$ the ring homomorphisms $\phi: \mathcal{W}O \to \mathcal{W}R$ are surjective for all orders $\mathcal{O}$ in $K$.

**Proposition 4.** Let $K = \mathbb{Q}(\sqrt{-d})$ with $d = 2$ or $d = p$, where $p$ is a prime satisfying $p \equiv 3 \pmod{4}$. Then for every order $\mathcal{O}$ in $R$ the ring homomorphism $\phi: \mathcal{W}O \to \mathcal{W}R$ is surjective.

**Proof.** For the field $K$ the number $t$ of prime divisors of the discriminant $d(K)$ equals 1. Hence the set (1) of generators for $\mathcal{W}R$ reduces to the single class $\langle 1 \rangle$. Clearly, the class $\langle 1 \rangle$ belongs to the image of $\mathcal{W}O \to \mathcal{W}R$ for any order $\mathcal{O}$ in the ring of algebraic integers $R$.

Hence there are infinitely many nonreal quadratic fields $K$ with the property that for every order $\mathcal{O}$ in $K$ the natural homomorphism $\mathcal{W}O \to \mathcal{W}R$ is surjective.

**References**


Received October 15, 2003

Instytut Matematyki
Uniwersytet Śląski
Bankowa 14
PL-40007 Katowice
POLAND
E-mail: mc@ux2.math.us.edu.pl