Mathematica Slovaca

Marzena Ciemała

Natural homomorphisms of Witt rings of orders in algebraic number fields

*Mathematica Slovaca*, Vol. 54 (2004), No. 5, 473--477

Persistent URL: http://dml.cz/dmlcz/131463

Math. Slovaca, **54** (2004), No. 5, 473–477

Mathematica
Slovaca


# NATURAL HOMOMORPHISMS OF WITT RINGS OF ORDERS IN ALGEBRAIC NUMBER FIELDS

MARZENA CIEMAŁA

(*Communicated by Stanislav Jakubec*)

ABSTRACT. Let $\mathcal{O}$ be an order and $R$ be the maximal order in a nonreal quadratic number field $K$. We prove that the natural homomorphism $\phi\colon W\mathcal{O} \to WR$ of Witt rings is surjective provided the discriminat 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 $A \to B$ induces the natural Witt ring homomorphism $\phi\colon WA \to WB$ defined by sending the class $\langle E\rangle$ of an $A$-space $E$ to the class $\langle E \otimes_A B\rangle$ of the $B$-space $E \otimes_A B$. It is well known that for the maximal order $R$ of a number field $K$ the ring homomorphism $WR \to WK$ 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 $W\mathcal{O} \to WR$ or $W\mathcal{O} \to WK$. 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 $W\mathcal{O} \to WR$ (see [8]). In an attempt to answer partially this question we study the natural ring homomorphism

$$\phi\colon W\mathcal{O} \to WR$$

in the case of orders of quadratic number fields. An order $\mathcal{O}$ of $K$ is a subring of $R$ which is a free abelian group of rank $[K:\mathbb{Q}]$ (see [7; p. 72]). If $\mathcal{O} \neq R$, $\mathcal{O}$ is strictly contained in $R$, 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 $R = \mathbb{Z}[\omega]$ 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 $\mathfrak{f}$ of the ring extension $\mathcal{O} \subseteq R$ is the ideal $fR$. Let $d(K)$ denote the discriminant of $K$ and $p_1, \dots, p_t$ 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 $fR$ in the maximal order $R = \mathbb{Z}[\omega]$ 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

$$\{\langle 1\rangle, \langle p_1\rangle, \dots, \langle p_{t-1}\rangle\}, \tag{1}$$

or by $\{\langle 1\rangle, \langle 2\rangle\}$ 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 $\phi\colon W\mathcal{O} \to WR$ 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 $I^2 = (a)$ for some $a \in \mathcal{O}$, $a \neq 0$. Then $\beta\colon I \times I \to \mathcal{O}$ given by*

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

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

P r o o f. The ideal $I^2$ is additively generated by the elements $xy$ where $x, y \in I$, and hence $xy \in (a)$ 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 $\hat{\beta}\colon I \to I^*$, where $I^* = \operatorname{Hom}_{\mathcal{O}}(I, \mathcal{O})$, 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,

$$x\varphi(y) = \varphi(xy) = y\varphi(x)$$

for all $x, y \in I$. Hence there exists a number $c \in K$ such that $\frac{\varphi(x)}{x} = c$ 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

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

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

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

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. $\square$

**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 $\mathfrak{f} = f\mathbb{Z}[\omega]$ is the conductor of the ring extension $\mathcal{O} \subseteq R$. Then there exist a prime ideal $\mathfrak{q} \lhd \mathcal{O}$ and a nonsingular bilinear form $\beta$ on $\mathfrak{q}$ such that $\phi\big\langle(\mathfrak{q}, \beta)\big\rangle = \langle p \rangle$.*

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

$$R = \mathfrak{f} + pR \subset \mathfrak{p} ,$$

which is a contradiction. Hence $\mathfrak{p} + \mathfrak{f} = R$.

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

$$pR \cap \mathcal{O} = \mathfrak{p}^2 \cap \mathcal{O} = \psi(\mathfrak{p}^2) = \big(\psi(\mathfrak{p})\big)^2 = (\mathfrak{p} \cap \mathcal{O})^2 = \mathfrak{q}^2$$

for the prime ideal $\mathfrak{q} = \mathfrak{p} \cap \mathcal{O}$ in $\mathcal{O}$. We are going to show that $pR \cap \mathcal{O} = p\mathcal{O}$. Let $\alpha \in pR \cap \mathcal{O}$ 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 $pR \cap \mathcal{O} \subseteq p\mathcal{O}$. The opposite inclusion is obvious. Since the condition $\mathfrak{q}^2 = p\mathcal{O}$ is satisfied, Lemma 2 implies that the formula

$$\beta(a, b) = \frac{ab}{p} , \qquad a, b \in \mathfrak{q} ,$$

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

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

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

**PROPOSITION 4.** *Let $K = \mathbb{Q}\bigl(\sqrt{-d}\bigr)$ 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 $\phi\colon W\mathcal{O} \to WR$ 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 $WR$ reduces to the single class $\langle 1\rangle$. Clearly, the class $\langle 1\rangle$ belongs to the image of $W\mathcal{O} \to WR$ 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 $W\mathcal{O} \to WR$ is surjective.

## REFERENCES


[1] CRAVEN, T. C.—ROSENBERG, A.—WARE, R.: *The map of the Witt ring of a domain into the Witt ring of its field of fractions*, Proc. Amer. Math. Soc. **51** (1975), 25–30.

[2] CZOGAŁA, A.: *Generators of the Witt groups of algebraic integers*, Ann. Math. Sil. **12** (1998), 105–121.

[3] GEROLDINGER, A.—HALTER-KOCH, F.—KACZOROWSKI, J.: *Non-unique factorization in orders of global fields*, J. Reine Angew. Math. **459** (1995), 89–118.

[4] MATSUMURA, H.: *Commutative Ring Theory*, Cambridge Univ. Press, Cambridge, 1986.

[5] MILNOR, J.—HUSEMOLLER, D.: *Symmetric Bilinear Forms*, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[6] NARKIEWICZ, W.: *Elementary and Analytic Theory of Algebraic Numbers* (2nd ed.), PWN/Springer-Verlag, Warszawa/Berlin-Heidelberg-New York, 1990.

[7] NEUKIRCH, J.: *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.

[8] SZYMICZEK, K.: *Problem session.* The 4th Czech and Polish Conference on Number Theory, Cieszyn, June 11–14, 2002; Ann. Math. Sil. **16** (2003), 79 81.

Received October 15, 2003

*Instytut Matematyki*
*Uniwersytet Śląski*
*Bankowa 14*
*PL–40007 Katowice*
*POLAND*

*E-mail*: mc@ux2.math.us.edu.pl