Acta Mathematica Universitatis Ostraviensis

Marzena Ciemała

Natural homomorphisms of Witt rings of orders in algebraic number fields. II

Acta Mathematica Universitatis Ostraviensis, Vol. 14 (2006), No. 1, 13--16

Persistent URL: `http://dml.cz/dmlcz/137477`

Natural homomorphisms of Witt rings of orders in algebraic number fields, II.

Marzena Ciemała

Abstract. We prove that there are infinitely many real quadratic number fields K with the property that for infinitely many orders $\mathcal{O}$ in K and for the maximal order R in K the natural homomorphism $\varphi : W\mathcal{O} \to WR$ of Witt rings is surjective.

For a commutative ring A let WA be the Witt ring of nondegenerate symmetric bilinear forms on finitely generated projective modules over the ring A. Any ring homomorphism $A \to B$ induces the Witt ring homomorphism $WA \to WB$. In particular the inclusion of a ring A in B induces the Witt ring homomorphism $WA \to WB$ which is said to be natural.

It is well known that for the maximal order R of a number field K the natural ring homomorphism $\psi : WR \to WK$ is injective. This was first proved by M. Knebusch in 1970 (for a proof see [5, p. 93]). On the other hand, for a nonmaximal order $\mathcal{O}$ in K we know very little about the natural homomorphisms $W\mathcal{O} \to WR$ or $W\mathcal{O} \to WK$. Recall that an order $\mathcal{O}$ of K is a subring of R which is a free abelian group of rank $[K : \mathbb{Q}]$ (see [6, p. 72]). We concentrate on the natural homomorphism

$$\varphi : W\mathcal{O} \to WR.$$

It has already been shown that the kernel of such a homomorphism is a nilideal ([2]) and for some classes of orders the kernel is a non-zero ideal in $W\mathcal{O}$ ([3]). A nonmaximal order $\mathcal{O}$ is strictly contained in R, and we cannot in general expect that φ be surjective. However, we have proved in [1] that in every nonreal quadratic number field K there are infinitely many orders $\mathcal{O}$ with the property that the natural homomorphism $\varphi : W\mathcal{O} \to WR$ is surjective. In this paper we prove a similar result for orders in real quadratic number fields. We are unable to cover all real quadratic fields but for any such field with the fundamental unit of norm -1 we show

Received: January 31, 2006.
1991 *Mathematics Subject Classification:* 11E81, 19G12.
Key words and phrases: Witt ring, orders in number fields, bilinear forms on ideals.
Editorial board announces with sorrow that dr. Marzena Ciemała died early on July 9, 2006.

that it contains infinitely many orders $\mathcal{O}$ with surjective natural homomorphism $\varphi : W\mathcal{O} \to WR$.

Notation. Let K be a real quadratic number field, $K = \mathbb{Q}(\sqrt{d}\,)$, where $d > 1$ is a square-free natural number 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. 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 $d \equiv 3 \pmod 4$.

When $-1 \in N(K)$ and $d \not\equiv 1 \pmod 8$, the Witt group $\psi(WR) \subseteq WK$ is additively generated by the following set

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

where $b \in K$ has negative norm and $\mathrm{ord}_{\mathfrak{p}} b \equiv 0 \pmod 2$ for every prime ideal $\mathfrak{p}$ in R (see [4]). Hence, if the fundamental unit ε has norm -1, we can take $b = \varepsilon$ in (1).

The following theorem gives a sufficient condition for surjectivity of the natural homomorphism $\varphi : W\mathcal{O} \to WR$.

Theorem 1. *Let $\mathcal{O} = \mathbb{Z}[f\omega]$ be an order in real quadratic field K and let ε be the fundamental unit in K. If $\varepsilon^n \in \mathcal{O}$ for some odd natural number n and if* $\gcd(d(K), f) = 1$, *then the natural homomorphism $\varphi : W\mathcal{O} \to WR$ is surjective.*

Proof. Since $\psi : WR \to WK$ is injective and $\psi(WR)$ is additively generated by the set S in (1), to prove the surjectivity of φ it is enough to show that the image of $\psi\varphi$ contains S.
It is clear that $\langle 1\rangle$ belongs to the image of the homomorphism $\psi\varphi$.
If p is a prime dividing the discriminant $d(K)$, then $\gcd(d(K), f) = 1$ implies $p \nmid f$ and we have $\langle p\rangle \in \operatorname{im} \psi\varphi$ by [1, Lemma 3].
It remains to show that $\langle\varepsilon\rangle$ also lies in the image. Since ε^n belongs to $\mathcal{O}$ and ε^n is an invertible element in $\mathcal{O}$ we can consider the class $\langle\varepsilon^n\rangle$ in the Witt ring $W\mathcal{O}$. Since n is odd, it is clear that $\psi\varphi\langle\varepsilon^n\rangle = \langle\varepsilon\rangle_K$.

Thus all generators in the set S are in the image of the homomorphism $\psi\varphi : W\mathcal{O} \to WK$, as desired. □

Theorem 1 applies to orders in a real quadratic field K containing an odd power of the fundamental unit of K. We now show that there are infinitely many such orders in K. This follows from the following Lemma. As usual, we say that a prime number p divides the sequence (s_n) if there exists a natural number n such that $p \mid s_n$.

Lemma 2. *Let K be a real quadratic field with maximal order $\mathbb{Z}[\omega]$ and let $\varepsilon = r + s\omega$, where $r, s \in \mathbb{Z}$, be the fundamental unit in K. Let*

$$\varepsilon^n := r_n + s_n\omega, \quad r_n, s_n \in \mathbb{Z}.$$

There are infinitely many prime numbers dividing the sequence $(s_{2n+1})_{n=1}^{\infty}$.

Proof. Write

$$\varepsilon^{n+1} = (r + s\omega)(r_n + s_n\omega).$$

Then

$$r_{n+1} = ar_n + bs_n, \qquad s_{n+1} = cs_n + er_n$$

for some integers a, b, c, e. A simple elimination yields

$$r_{n+1} = (a+c)r_n + (be-ac)r_{n-1}, \qquad s_{n+1} = (a+c)s_n + (be-ac)s_{n-1}.$$

Thus the sequences (r_n) and (s_n) are recurrent sequences of rank 2.

According to a classical theorem of M. Ward ([8]), there are infinitely many primes dividing the sequence (s_n). But we need to prove that the subsequence (s_{2n+1}) also has infinitely many prime divisors. For this it is sufficient to observe that the sequence (u_n), where $u_n = s_{2n+1}$, is recurrent of rank two, and again invoke Ward's theorem. We write

$$u_n = s_{2n+1} = As_{2n} + Bs_{2n-1}, \qquad w_n = s_{2n} = As_{2n-1} + Bs_{2n-2},$$

where $A = a + c$ and $B = be - ac$ and hence

$$u_n = Aw_n + Bu_{n-1}, \qquad w_n = Au_{n-1} + Bw_{n-1}.$$

Similarly as above for (r_n) and (s_n) we conclude that the sequence (u_n) is recurrent of rank 2. Hence by Ward's theorem there are infinitely many primes dividing the sequence (s_{2n+1}). □

Theorem 3. *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field such that the norm of its fundamental unit is -1 and $d \not\equiv 1 \pmod 8$. Then there are infinitely many natural numbers f such that natural homomorphism $W\mathbb{Z}[f\omega] \to WR$ is surjective.*

Proof. By Lemma 2 there exist infinitely many prime numbers dividing the sequence (s_{2n+1}). Hence there are infinitely many natural numbers f such that f divides (s_{2n+1}) and $\gcd(f, d(K)) = 1$. One can choose for f all sufficiently large prime divisors of the sequence (s_{2n+1}). Now it follows from Theorem 1 that the natural homomorphism $W\mathbb{Z}[f\omega] \to WR$ is surjective. □

We conclude with recalling that there exist infinitely many quadratic fields satisfying the assumptions of Theorem 3. For take $K = \mathbb{Q}(\sqrt{t^2+4})$ with t an odd integer. Then the diophantine equation

$$X^2 - (t^2+4)Y^2 = -1$$

has infinitely many integral solutions and the fundamental unit in K has norm -1. This can be seen from the continued fraction expansion of the number $\sqrt{t^2+4}$ which is periodic with the period of length 5 (see, for instance, [7, p. 287]) and hence the equation above has infinitely many integral solutions (by [7, p. 302]). Moreover $t^2 \equiv 1 \pmod 8$ and thus $t^2 + 4 \not\equiv 1 \pmod 8$.

Hence there are infinitely many real quadratic fields K with the property that for infinitely many orders $\mathcal{O}$ in K the natural homomorphism $W\mathcal{O} \to WR$ is surjective.

References

[1] M. Ciemała, Natural homomorphisms of Witt rings of orders in algebraic number fields. *Math. Slovaca* **54** (2004), 473–477.

[2] M. Ciemała, K. Szymiczek, On natural homomorphisms of Witt rings. *Proc. Amer. Math. Soc.* **133** (2005), 2519–2523.

[3] M. Ciemała, K. Szymiczek, On injectivity of natural homomorphisms of Witt rings (submitted).

[4] A. Czogała, Generators of the Witt groups of algebraic integers. *Ann. Math. Siles.* **12** (1998), 105–121.
[5] J. Milnor, D. Husemoller, *Symmetric bilinear forms.* Springer-Verlag, Berlin - Heidelberg - New York 1973.
[6] J. Neukirch *Algebraic number theory.* Springer-Verlag, Berlin 1999.
[7] W. Sierpiński, *Teoria Liczb.* Monografie Matematyczne, Warszawa 1950.
[8] M. Ward, Prime divisors of second order recurring sequences. *Duke Math. J.* **21** (1954), 607–614).

Author(s) Address(es):
Instytut Matematyki, Uniwersytet Śląski, Bankowa 14,
Katowice 40007, Poland

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