Annales Mathematicae Silesianae (2026),
DOI: 10.2478/amsil-2026-0011

# ON EXAMPLES OF WITT FUNCTORS IN QUADRATIC NUMBER FIELDS

Paweł Gładki, Mateusz Pulikowski

**Abstract.** In this paper we provide a series of examples of nonmaximal orders in a quadratic number field $K$ whose Witt ring does not embed into the Witt ring of $K$.

For $R$ a commutative ring with 1, consider the Witt ring $WR$ of Witt equivalence classes of finitely generated projective modules $M$ over $R$ endowed with nondegenerate symmetric bilinear forms $\beta\colon M\times M\to R$ (see Milnor and Husemoller [6] for details). The diagonal form $a_1x_1y_1+\ldots+a_nx_ny_n$ with $a_i\in R$, $i\in\{1,\ldots,n\}$ shall be denoted by $\langle a_1,\ldots,a_n\rangle$, and its Witt equivalence class by $[a_1,\ldots,a_n]$. Pfister forms, i.e. forms of the shape $\langle 1,a_1\rangle\otimes\cdots\otimes\langle 1,a_n\rangle$, shall be denoted by $\langle\langle a_1,\ldots,a_n\rangle\rangle$, and their Witt classes by $[[a_1,\ldots,a_n]]$, $a_i\in R$, $i\in\{1,\ldots,n\}$.

A homomorphism $\varphi\colon R\to R'$ between two commutative rings with 1 $R$ and $R'$ induces in a natural way a homomorphism between their respective Witt rings: $R'$ is made into an $R$-module with multiplication defined by $R\times R'\ni(a,a')\mapsto f(a)\cdot a'\in R'$, so that if $M$ is an $R$-module, it can be naturally extended to an $R'$-module $M'=R'\otimes_R M$ with multiplication given by $a'\cdot(b'\otimes m)=a'b'\otimes m$, for $a'\in R'$ and simple tensors $b'\otimes m\in R'\otimes_R M$; now a bilinear form $\beta\colon M\times M\to R$ uniquely extends to a bilinear form $\beta'\colon M'\times M'\to R'$ such that

$$\beta'(a'\otimes m,b'\otimes n)=a'b'f(\beta(m,n)),$$

*Received: 25.04.2026. Accepted: 13.06.2026.*
(2020) Mathematics Subject Classification: 11E81, 19G12.
*Key words and phrases:* Natural homomorphism of Witt rings, orders.

for $a', b' \in R'$, $m, n \in M$. If $M$ is finitely generated and projective then so is $M'$, and if $\beta$ is symmetric and nondegenerate, then $\beta'$ is such as well – denoting by $f_\sharp(M, \beta)$ (or $f_\sharp(M)$, for short) the pair $(M', \beta')$ we thus obtain a well-defined homomorphism of Witt rings $f_\sharp \colon WR \to WR'$ by assigning to the Witt equivalence class $[M]$ the class $[f_\sharp(M)]$.

We will be concerned with one special class of examples of such homomorphisms here. Let $K$ be a number field and let $\mathcal{O}_K$ be its ring of integers. The natural homomorphism $W\mathcal{O}_K \to WK$ induced by the map $f \colon \mathcal{O}_K \to K$, $f(a) = \frac{a}{1}$, is injective ([5], Satz 11.1.1), but if we replace $\mathcal{O}_K$ with an arbitrary ring $\mathcal{O}$ whose field of fractions is equal to $K$ this may no longer be true.

Consider one particular class of such rings, namely orders of the field $K$, that is subrings $\mathcal{O}$ of $\mathcal{O}_K$ which, as $\mathbb{Z}$-modules, are of rank $n = [K : \mathbb{Q}]$. Craven, Rosenberg and Ware ([2], Remark following Proposition 3.2) showed that $W\mathcal{O} \to WK$ is not injective for $\mathcal{O} = \mathbb{Z}[3i]$ and $K = \mathbb{Q}(i)$. This was later generalized by Ciemała and Szymiczek ([1], Example 4.5), who proved that $W\mathcal{O} \to WK$ is not injective for all orders $\mathcal{O} = \mathbb{Z}[fi]$, with $f > 1$, $K = \mathbb{Q}(i)$. Moreover, they also demonstrated that for an arbitrary number field $K$ and order $\mathcal{O}$ with conductor $\mathfrak{f} = \{a \in \mathcal{O}_K \mid a\mathcal{O}_K \subseteq \mathcal{O}\}$ such that $\mathfrak{f} \subseteq 2\mathcal{O}_K$ the homomorphism $W\mathcal{O} \to WK$ is not injective – these examples led them to conjecture that the only orders $\mathcal{O}$ for which $W\mathcal{O} \to WK$ is injective are, in fact, the maximal orders $\mathcal{O} = \mathcal{O}_K$. This turned out to be false, as shown by Rothkegel ([7], Theorem 2.2), who proved that for $\mathcal{O} = \mathbb{Z}\big[f\sqrt{d}\big]$ and $K = \mathbb{Q}\big(\sqrt{d}\big)$ with $d \not\equiv 1 (\mathrm{mod}\, 4)$, $2 \nmid f$ and $f \mid d$ the homomorphism $W\mathcal{O} \to WK$ is injective. This was further extended by the authors: firstly, in [3], Theorem 1.1 we showed that for $\mathcal{O} = \mathbb{Z}\left[3\sqrt[3]{6}\right]$ and $K = \mathbb{Q}\left(\sqrt[3]{6}\right)$ the homomorphism $W\mathcal{O} \to WK$ is not injective, and then in [4], Theorem 3, we generalized this result to the case when $K = \mathbb{Q}\left(\sqrt[n]{m}\right)$, $n = p^k$, with $k \in \mathbb{N}$, $p$ a prime, $p \neq 2$, with $m$ square-free, $m \neq \pm 1$, $p \mid m$ and $\mathcal{O} = \mathbb{Z}\left[p\sqrt[n]{m}\right]$: here $W\mathcal{O} \to WK$ is also injective.

In this miniature note we add one more piece of puzzle to the big picture. Namely, although in general one expects that for a randomly selected order $\mathcal{O}$ of a number field $K$ the homomorphism $W\mathcal{O} \to WK$ shall not be injective, it appears that other than the few abovementioned examples by Craven-Rosenberg-Ware/Ciemała-Szymiczek for the Gaussian field $\mathbb{Q}(i)$, and the series of orders with "even" conductors – no explicit examples are to be found in literature. We aim to fill that gap here: such examples are relatively easy to build, by combining results obtained by Ciemała and Szymiczek with some (more or less) elementary number theory. We shall discuss it here in some detail. The key result used by Ciemała and Szymiczek to build their examples is the following:

PROPOSITION 1 ([1, Theorem 4.4]). *Let $K$ be a number field, $\mathcal{O}_K$ its ring of integers, $\mathcal{O}$ an order and denote by $U(\mathcal{O})$ the group of units of $\mathcal{O}$. Let $(S, \beta)$ be a nondegenerate symmetric bilinear space over $\mathcal{O}$ with $S$ a free module of rank 2, and assume that in a certain basis $\beta$ has the matrix*

$$\begin{bmatrix} A & C \\ C & B \end{bmatrix}.$$

*If all of the following conditions are met:*
- $A, B, C \in \mathcal{O}$,
- $AB \neq 0$,
- $AB - C^2 = -u^2 \in U(\mathcal{O})$, $D \in K \setminus \{0\}$,
- *denoting by $d$ and $d'$ the roots of the isotropy equation:*

$$B^2X + 2CX + A = 0,$$

*that is $d = \frac{-C+u}{B} = \frac{A}{-C-u}$ and $d' = \frac{-C-u}{B} = \frac{A}{-C+u}$, $d$ and $d'$ are integral over $\mathcal{O}$ each of degree at least 2,*

*then the Witt equivalence class of $(S, \beta)$ is a nonzero element in the kernel of $W\mathcal{O} \to WK$.*

We will use Proposition 1 to exhibit some examples of non-injective natural homomorphisms of Witt rings in quadratic fields. We turn our attention to real quadratic fields first. Let $K = \mathbb{Q}(\sqrt{d})$ with $d > 0$ square free and $d \not\equiv 1 (\mathrm{mod}\, 4)$, so that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and there are infinitely many units, each of the form $\varepsilon^n$, where $\varepsilon = x_0 + y_0\sqrt{d}$ is the fundamental unit of $K$. For an integer $f > 1$ set $\mathcal{O} = \mathbb{Z}[f\sqrt{d}]$. Let $\varepsilon^n = a_n + b_n\sqrt{d}$ with integers $a_n, b_n$.

THEOREM 1. *Suppose there exists an integer $n \geq 1$ such that*

$$a_n \equiv 0 \pmod{f}, \quad b_n \not\equiv 0 \pmod{f}.$$

*Then the natural homomorphism $W\mathcal{O} \to WK$ is not injective.*

PROOF. Set $u = \varepsilon^n = a_n + b_n\sqrt{d}$. By design, $u$ is a unit in $\mathcal{O}_K$. Because $a_n \equiv 0 \pmod{f}$ and $b_n \not\equiv 0 \pmod{f}$, we have that $u \notin \mathcal{O}$. On the other hand, $u^2 = \varepsilon^{2n} = a_{2n} + b_{2n}\sqrt{d}$, and a direct computation gives $b_{2n} = 2a_nb_n$. Since $a_n \equiv 0 \pmod{f}$, we have $b_{2n} \equiv 0 \pmod{f}$, so $u^2 \in \mathcal{O}$. Moreover, the norm $N(u^2) = (N(u))^2 = 1 = a_{2n}^2 - b_{2n}^2 d = \left(a_{2n} + b_{2n}\sqrt{d}\right)\left(a_{2n} - b_{2n}\sqrt{d}\right)$, so that the inverse of $u^2$ is its conjugate, which is an element of $\mathcal{O}$. Therefore, $u^2$ is a unit in $\mathcal{O}$.

Consider the bilinear space $S = \mathcal{O}^2$ with bilinear form whose matrix is

$$\begin{bmatrix} -u^2 & 0 \\ 0 & 1 \end{bmatrix}.$$

It clearly satisfies the conditions of Proposition 1: $-u^2, 1, 0 \in \mathcal{O}$, $-u^2 \neq 0$ is a unit in $\mathcal{O}$, and the isotropy equation is $X^2 - u^2 = 0$ – its roots are $\pm u$, which lie in $\mathcal{O}_K$ and satisfy the monic polynomial equation $X^2 - u^2 = 0$ with coefficients in $\mathcal{O}$, since $u^2 \in \mathcal{O}$. □

The existence of an integer $n$ such that $a_n \equiv 0 (\mathrm{mod}\, f)$ and $b_n \not\equiv 0 (\mathrm{mod}\, f)$ is intimately connected to the splitting behaviour of the prime factors of $f\mathcal{O}_K$ in $\mathcal{O}_K$ and to the order of the fundamental unit modulo those primes. Let $p > 0$ be a rational prime and consider the order $\mathcal{O} = \mathbb{Z}\left[p\sqrt{d}\right]$. We shall distinguish between the unramified case (when $p$ does not divide the discriminant of $K$, so $p \nmid 2d$) and the ramified one (when $p \mid 2d$).

If $p \mid 2d$, then either $p = 2$, so that $W\mathcal{O} \to WK$ is not injective by [1, Theorem 5.2] or $2 \nmid p$ and $p \mid d$, in which case $W\mathcal{O} \to WK$ is injective by [7, Theorem 2.2]. The unramified case is more subtle:

THEOREM 2. *Let $p$ be an odd prime with $p \nmid d$ and let $\mathcal{O} = \mathbb{Z}[p\sqrt{d}]$, where $d \not\equiv 1 (\mathrm{mod}\, 4)$. Let $m$ be the order of the image of fundamental unit $\varepsilon$ in the multiplicative group $(\mathcal{O}_K/p\mathcal{O}_K)^\times$. If $4 \mid m$, then set $n = m/4$. Then*

$$a_n \equiv 0 \pmod{p}, \quad b_n \not\equiv 0 \pmod{p}.$$

PROOF. Let $R = \mathcal{O}_K/p\mathcal{O}_K$. The multiplicative group $R^\times$ is cyclic of order $p^2 - 1$ if $p$ is inert, that is if $\left(\frac{d}{p}\right) = -1$, and isomorphic to $\mathbb{F}_p^\times \times \mathbb{F}_p^\times$ if $p$ splits, that is if $\left(\frac{d}{p}\right) = 1$. In either case, the order $m$ of $\varepsilon$ in $R^\times$ is well-defined. By hypothesis, $4 \mid m$.

Set $n = m/4$. Then $\varepsilon^{2n} = \varepsilon^{m/2}$. Since $m/2$ is even (because $m$ is divisible by 4), we have $\varepsilon^{m/2} \neq 1$ and its square is $\varepsilon^m = 1$. Hence $\varepsilon^{m/2}$ is an element of order 2 in $R^\times$. In any field of characteristic not 2, the only element of order 2 is $-1$. In the split case, the group is a product, and the element of order 2 is $(-1, -1)$. In either case, $\varepsilon^{m/2} = -1$ (where $-1$ denotes the element $(-1, \ldots, -1)$ in the product, or the field element $-1$). Thus $\varepsilon^{2n} = -1$.

Now write $\varepsilon^n = a_n + b_n\sqrt{d}$ in $\mathcal{O}_K$. Reducing modulo $p$ gives an element in $R$. The equality $\varepsilon^{2n} = -1$ becomes

$$(a_n + b_n\sqrt{d})^2 \equiv -1 \pmod{p}.$$

Expanding, $a_n^2 + db_n^2 + 2a_nb_n\sqrt{d} \equiv -1$. Since the representation of elements of $R$ in the basis $\{1, \sqrt{d}\}$ is unique (mod $p$), we compare coefficients:

$$a_n^2 + db_n^2 \equiv -1, \quad 2a_nb_n \equiv 0 \pmod{p}.$$

Because $p$ is odd, the second congruence gives $a_nb_n \equiv 0 \pmod{p}$. If $b_n \equiv 0 \pmod{p}$, then the first congruence gives $a_n^2 \equiv -1 \pmod{p}$, which would imply that $-1$ is a square modulo $p$. But then $\varepsilon^n \equiv a_n$ would be a rational integer,

and its norm would be $a_n^2$, which is $\pm 1$. However, if $b_n \equiv 0$, then $\varepsilon^n \equiv \pm 1$ (since the only units in $\mathbb{Z}$ are $\pm 1$). Then $\varepsilon^{2n} \equiv 1$, contradicting $\varepsilon^{2n} \equiv -1$. Therefore $b_n \not\equiv 0 \pmod{p}$. Hence $a_n \equiv 0 \pmod{p}$ from the product condition.

Thus we have $a_n \equiv 0$ and $b_n \not\equiv 0 \pmod{p}$, which finishes the proof. □

EXAMPLE 1. The condition that the order $m$ of $\varepsilon$ in $(\mathcal{O}_K/p\mathcal{O}_K)^\times$ is divisible by 4 is a concrete arithmetic condition that can be checked for given $d$ and $p$. It is satisfied for many primes:

- for $d = 2$, $p = 3$: $\varepsilon = 1 + \sqrt{2}$ has order 8 in $\mathbb{F}_9^\times$ (since $p$ is inert), so $m = 8$ is divisible by 4;
- for $d = 2$, $p = 17$: 17 splits, $\varepsilon$ has order 16 in $\mathbb{F}_{17}^\times$, so $m = 16$ is divisible by 4;
- for $d = 3$, $p = 7$: 7 is inert, $\varepsilon = 2 + \sqrt{3}$ has order 8 in $\mathbb{F}_{49}^\times$, which again is divisible by 4.

Thus the theorem provides infinitely many odd conductor examples for each real quadratic field: by the Chebotarev Density Theorem there are infinitely many primes for which the order of $\varepsilon$ is a multiple of 4.

REMARK 1. The condition provided by Theorem 2 is sufficient for the existence of suitable $n$, but far from necessary. For example, let $K = \mathbb{Q}\left(\sqrt{2}\right)$ and $p = 7$. The order of $\varepsilon = 1 + \sqrt{2}$ modulo 7 is 6, which is not divisible by 4, but for $n = 3$ we get $\varepsilon^3 = 7 + 5\sqrt{2}$, so that $a_3 = 7 \equiv 0 \pmod{7}$ and $b_3 = 5 \not\equiv 0 \pmod{7}$.

The case of imaginary quadratic number fields seems to be more complicated. Recall that except for $d = 1$ and $d = 3$, the ring of integers $\mathcal{O}_K$ of the field $K = \mathbb{Q}\left(\sqrt{-d}\right)$ contains only 2 units, namely 1 and $-1$, so there is no hope of applying Theorem 1 here. The case of the Gaussian field $\mathbb{Q}\left(\sqrt{-1}\right)$, whose ring of integers contains 4 units, has been completely described by Ciemała and Szymiczek. The Eisenstein field $\mathbb{Q}\left(\sqrt{-3}\right)$ is considerably more involved and the methods developed for the Gaussian field do not seem to be transferable here.

## References


[1] M. Ciemała and K. Szymiczek, *On injectivity of natural homomorphisms of Witt rings*, Ann. Math. Sil. **21** (2007), 15–30.

[2] T.C. Craven, A. Rosenberg, and R. Ware, *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.

[3] P. Gładki and M. Pulikowski, *Natural homomorphisms of Witt rings of a certain cubic order*, Int. J. Number Theory **19** (2023), no. 9, 2015–2020.

[4] P. Gładki and M. Pulikowski, *On natural homomorphisms of Witt rings of orders in pure number fields*, Math. Slovaca, to appear.

[5] M. Knebusch, *Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen*, S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl. 1969/70, Abh. 3, Springer-Verlag, Berlin–Heidelberg, 1970, pp. 5–69.
[6] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Ergeb. Math. Grenzgeb., Band 73. Springer-Verlag, New York–Heidelberg, 1973.
[7] B. Rothkegel, *Witt functor of a quadratic order*, Math. Slovaca **68** (2018), no. 6, 1339–1342.

Institute of Mathematics
University of Silesia in Katowice
ul. Bankowa 14
40-007 Katowice
Poland
e-mail: pawel.gladki@us.edu.pl
e-mail: mateusz.pulikowski@us.edu.pl