JOURNAL OF NUMBER THEORY 6, 232–237 (1974)

Embedding Witt Rings of Dedekind Domains

D. B. COLEMAN

Department of Mathematics, University of Kentucky, Lexington, Kentucky 40506

Communicated by H. Zassenhaus

Received April 20, 1971

Let $W(R)$ denote Harrison's Witt ring of the commutative ring R. In case R is a field of characteristic $\neq 2$, this is the classical Witt ring based on anisotropic quadratic forms. In this note we determine under what conditions $W(R)$ is embedded in $W(S)$ for certain Dedekind domains $R \subset S$. In particular, an answer is given in case R and S are the integers in algebraic number fields K and L, respectively, with $(L: K)$ odd.

INTRODUCTION

Let R be a commutative ring with identity and let $W(R)$ denote the Witt ring given by D.K. Harrison's presentation

(i) $\langle 0\rangle = 0$
(ii) $\langle 1\rangle = 1$
(iii) $\langle ab\rangle = \langle a\rangle\langle b\rangle$
(iv) $\langle a\rangle + \langle b\rangle = \langle a+b\rangle(1 + \langle ab\rangle)$,

where the generators $\langle a\rangle = \langle a\rangle_R$ are taken for $a \in R$. In [1] a number of results on the structure of the ring $W(R)$ are given, including a description of the prime ideals of $W(R)$. Theorem 0.2. and the remark at the end of this paper indicate a connection between $W(R)$ and the diagonal quadratic forms over R. See also the last section of [1].

Here we consider the following question. If $R \to S$ is a ring injection (with 1 going to 1) under what conditions is $W(R) \to W(S)$ an injection? The main result is Theorem 1.6. which answers this question in case R and S are the algebraic integers in algebraic number fields K and L, respectively, with $(L : K)$ odd.

The following results will be needed.

THEOREM 0.1. (O. T. Springer [See 3]) *If L is a field extension of K of finite odd degree, and of characteristic $\neq 2$, then $W(K) \to W(L)$ is an injection.*

THEOREM 0.2. (D. Harrison [see 2]) *Let R be an integral domain with field of fractions K, and let $x \in W(R)$. Then $x = 0$ if and only if $W(R \to K)(x) = 0$ and $W(R \to R/a^2R)(x) = 0$ for all $0 \neq a \in R$.*

THEOREM 0.3. ([1]) *Let J be an ideal in R and let $\langle J \rangle$ denote the ideal in $W(R)$ generated by the elements $\langle a \rangle$, $a \in J$. Then $W(R)/\langle J \rangle \cong W(R/J)$.*

THEOREM 0.4. ([1]) $W(R_1 \times R_2) \cong W(R_1) \times W(R_2)$.

THEOREM 0.5. ([1]) *Let $I_0 = \{x \in R : \langle x \rangle = 0\}$. Then I_0 is the largest ideal in R such that $W(R) \to W(R/I_0)$ is an isomorphism.*

THEOREM 0.6. ([1]) *Let L be the ideal in R generated by elements of the form $ab(a + b)$, and let N denote the nil radical of R. Then $LN \subset I_0 \subset N$.*

$\mathbf{Z}$ denotes the ring of integers and $\mathbf{Z}_n$ denotes the integers modulo n.

All ring homomorphisms are assumed to preserve identity elements.

Let alg. int. $\{K\}$ denote the ring of algebraic integers in an algebraic number field K.

1. THE MAIN RESULT

LEMMA 1.1. *Let R be a local ring with maximal ideal J such that J is nil and R/J has more than two elements. Then $I_0 = J$, so that $W(R) \to W(R/J)$ is an isomorphism.*

Proof. There are units a and b in R such that $a + b$ is a unit, so 0.6. applies.

LEMMA 1.2. *Let R be a local ring with nil maximal ideal J such that $R/J \cong J/J^2 \cong \mathbf{Z}_2$ as groups. Then $I_0 = J^2$, so that $W(R) \to W(R/J^2)$ is an isomorphism and $W(R) \to W(R/J)$ is not.*

Proof. Let $x \in J$. Then $x(x + 1) \in L$ and $x + 1$ is a unit, so $x \in L$. Thus $J \subset L$ and we have $J^2 \subset LJ \subset I_0$ by 0.6.

We now produce a mapping $t : R \to \mathbf{Z}_2(C_2)$ that vanishes precisely on J^2 and such that $t(0) = 0$, $t(1) = 1$, $t(xy) = t(x)\,t(y)$ and $t(x) + t(y) = t(x + y)(1 + t(xy))$. A mapping satisfying these four definitive properties is called and *H-map* in [1]. $\mathbf{Z}_2(C_2)$ denotes the group ring of the group $C_2 = \{1, g\}$ over $\mathbf{Z}_2$. Since I_0 is the intersection of the "kernels" of all H-maps, the lemma will follow. Define t as follows:

$$t(x) = \begin{cases} 0 & \text{if } \; x \in J^2 \\ 1 + g & \text{if } \; x \in J - J^2. \\ 1 & \text{if } \; x \notin J \end{cases}$$

The verification that t is an H-map is routine. The requirement that $J/J^2 \cong \mathbf{Z}_2$ is used for the fourth condition in case x and y are both in $J - J^2$. It is easy to see that the homomorphism induced by t is an isomorphism, so in fact $W(R) \cong \mathbf{Z}_2(C_2)$ in this case.

LEMMA 1.3. *Let R and S be Dedekind domains with fields of fractions K and L, respectively, with $R \subset S$, and suppose that $W(K) \to W(L)$ is injective. Then the following statements are equivalent:*

(1) *σ: $W(R) \to W(S)$ is injective.*

(2) *$\sigma^{-1}(\langle a^2\rangle_S W(S)) = \langle a^2\rangle_R W(R)$ for all $0 \neq a \in R$.*

(3) *For each prime ideal P of R, $PS \neq S$, and if $Q_1, \ldots, Q_k$ are the primes of S that lie over P, then $W(R/P^2) \to \prod_i W(S/Q_i{}^2)$ is injective.*

Proof. If $x \in W(R)$, $x \notin \langle a^2\rangle_R W(R)$, and if $\sigma(x) \in \langle a^2\rangle_S W(S)$, then since $\langle a^2\rangle_S$ is idempotent (see [1]) it follows that $x(1 - \langle a^2\rangle_R)$ is a nonzero member of the kernel of σ. Hence (1) implies (2).

(2) implies (1). Suppose (2) holds and let $x \in \operatorname{Ker}(\sigma)$. Then by hypothesis $x \in \langle a^2\rangle_R W(R) = \operatorname{Ker}(W(R) \to W(R/a^2R))$ for all $0 \neq a \in R$. Since $W(K) \to W(L)$ is injective it follows that $x \in \operatorname{Ker}(W(R) \to W(K))$. Hence by 0.2, $x = 0$.

Using 0.3 it is easy to see that condition (2) is equivalent to

(2′) $\qquad W(R/a^2R) \to W(S/a^2S)$ is injective for all $0 \neq a \in R$.

We show the equivalence of (2′) and (3). For $0 \neq a \in R$, a not a unit, write $a^2R = P_1^{\alpha_1} \cdots P_n^{\alpha_n}$, where the P_i are prime ideals in R and each $\alpha_i \geqslant 2$. For each i, if $P_iS \neq S$ write $P_iS = Q_{i1}^{\beta_{i1}} \cdots Q_{ik_i}^{\beta_{ik_i}}$, where the Q_{ij} are primes in S. Suppose we have arranged the primes P_i such that for some $0 \leqslant m \leqslant n$, $P_iS \neq S$ if $1 \leqslant i \leqslant m$ and $P_jS = S$ if $m < j \leqslant n$. We have by the Chinese Remainder Theorem, 0.4 and Lemmas 1.1 and 1.2 that $W(R/a^2R) \cong \prod_i W(R/P_i{}^2)$. And if $m > 0$,

$$W(S/a^2S) \cong \prod_{\substack{i \leqslant m \\ i \leqslant j \leqslant k_i}} W(S/Q_{ij}^2).$$

Thus $W(R/a^2R) \to W(S/a^2S)$ is injective if and only if $m = n$ and for each i, $W(R/P_i{}^2) \to \prod_{1 \leqslant j \leqslant k_i} W(S/Q_{ij}^2)$ is injective. That is, that condition (3) holds for each P_i. Since all primes P occur over some such $a \in R$, the equivalence of (2′) and (3) follows.

LEMMA 1.4. *Let R, S, K, L be as in Lemma 1.3 and suppose further that L/K is a separable extension of odd degree. Then $W(R) \to W(S)$ is injective if and only if* (a) *$PS \neq S$ for each prime P of R and* (b) *if P is a* *prime of R that contains 2, and if $Q_1, \ldots, Q_k$ are the primes of S lying over P, then $W(R/P^2) \to \prod W(S/Q_i^2)$ is injective.*

Proof. Let P be a prime of R not containing 2 such that $PS \neq S$. Letting $PS = Q_1^{e_1} \cdots Q_k^{e_k}$ and $(S/Q_i : R/P) = f_i$ we have by separability that $(L : K) = \sum e_i f_i$. Since this degree is odd, one of the f_i must be odd, say f_1. Since $2 \notin P$ we have by 0.1 and Lemma 1.1, monomorphisms $W(R/P^2) \to W(R/P) \to W(S/Q_1) \to W(S/Q_1^2)$. Hence

$$W(R/P^2) \to \prod_i W(S/Q_i^2)$$

is a monomorphism. We are done by Lemma 1.3.

COROLLARY 1.5. *Let L be a separable field extension of K of odd degree, let R and S be Dedekind domains with fields of fractions K and L, respectively, and let $R \subset S$. If 2 is a unit in R, then $W(R) \to W(S)$ is injective if and only if $PS \neq S$ for each prime P of R.*

THEOREM 1.6. *Let K and L be algebraic number fields with $K \subset L$ and $(L : K)$ odd, and let $R = alg.\ int.\{K\}$, $S = alg.\ int.\{L\}$. Then $W(R) \to W(S)$ is injective if and only if for each prime ideal P of R such that $R/P \cong \mathbf{Z}_2$, there is a prime Q of S lying over P such that $R/P^2 \to S/Q^2$ is an isomorphism.*

Proof. Suppose P is a prime in R such that R/P is of characteristic 2 and contains more than two elements. Then for each Q_i over P, S/Q_i has more than two elements, so by Lemma 1.1 we have isomorphisms $W(R/P^2) \to W(R/P)$ and $W(S/Q_i^2) \to W(S/Q_i)$. The Witt ring of a finite field of characteristic 2 is isomorphic with $\mathbf{Z}_2$, so each $W(R/P^2) \to W(S/Q_i^2)$ is an isomorphism. Hence by Lemma 1.4, $W(R) \to W(S)$ can fail to be injective if and only if there is a prime P such that $R/P \cong \mathbf{Z}_2$ and $W(R/P^2) \to \prod_i W(S/Q_i^2)$ is not injective. (Since S is integral over R we do not have to contend with condition (a) of Lemma 1.4).

Now consider primes P with $R/P \cong \mathbf{Z}_2$. If $R/P^2 \to S/Q_i^2$ is an isomorphism for some Q_i, then surely $W(R/P^2) \to \prod W(S/Q_i^2)$ is injective. Hence the condition is sufficient.

Now suppose $R/P \cong \mathbf{Z}_2$ and no $R/P^2 \to S/Q_i^2$ is an isomorphism. If S/Q_i has more than two elements then $W(S/Q_i^2) \cong W(S/Q_i) \cong \mathbf{Z}_2$ by Lemma 1.1, so that the image of $W(R/P^2) \to W(S/Q_i^2)$ is a copy of $\mathbf{Z}_2$. If $S/Q_i \cong \mathbf{Z}_2$ then since $R/P^2 \to S/Q_i^2$ is not an isomorphism, it follows that $R/P^2 \cong \mathbf{Z}_4$ and $S/Q_i^2 \cong \mathbf{Z}_2(C_2)$. For each of R/P^2 and S/Q_i^2 must be one of these two rings with four elements and $\mathbf{Z}_2(C_2)$ cannot be mapped nontrivially into $\mathbf{Z}_4$. Hence the image of $R/P^2 \to S/Q_i^2$ is in this case a copy of $\mathbf{Z}_2$, as is the image of $W(R/P^2) \to W(S/Q_i^2$. Thus the assumption that none of the $R/P^2 \to S/Q_i^2$ is an isomorphism implies that the image of $\mathbf{Z}_2(C_2) \cong W(R/P^2) \to \prod W(S/Q_i^2)$ is a product of copies of $\mathbf{Z}_2$. Since $\mathbf{Z}_2(C_2)$ is local, the map cannot be injective and we are done by Lemma 1.4.

2. $W(\mathbf{Z}) \to W(R)$.

Let R be any Dedekind domain and let $\mathbf{Z} \to R$ be given by $n \mapsto n \cdot 1$. Let $\sigma : W(\mathbf{Z}) \to W(R)$. There is only one ideal of $W(\mathbf{Z})$ properly above $\langle 4 \rangle W(\mathbf{Z})$, namely $\langle 2 \rangle W(\mathbf{Z})$; hence $\sigma^{-1}(\langle 4 \rangle_R W(R)) = \langle 4 \rangle W(\mathbf{Z})$ if and only if $\langle 2 \rangle_R \neq \langle 8 \rangle_R$. For odd prime p, $\sigma^{-1}(\langle p^2 \rangle_R W(R)) = \langle p^2 \rangle W(\mathbf{Z})$. So using the proofs of Lemma 1.3 and Theorem 1.6 we have the following lemma, even though $\mathbf{Z} \to R$ is not necessarily injective.

LEMMA 2.1. *Let R be a Dedekind domain. Then $\langle 2 \rangle_R = \langle 8 \rangle_R$ if and only if there is no prime ideal P of R such that $R/P^2 \cong \mathbf{Z}_4$.*

Thus by Theorem 1.6 we obtain

THEOREM 2.2. *Let K be an algebraic number field with $(K : \mathbf{Q})$ odd and let $R =$ alg. int. $\{K\}$. Then the following statements are equivalent.*

(1) *$W(\mathbf{Z}) \to W(R)$ is injective.*
(2) $\langle 2 \rangle_R \neq \langle 8 \rangle_R$.
(3) *There is a prime ideal P of R such that $R/P^2 \cong \mathbf{Z}_4$.*

The kernel of $W(\mathbf{Z}) \to W(R)$ is as expected.

THEOREM 2.3. *Let $R =$ alg. int. $\{K\}$ with $(K : \mathbf{Q})$ odd. If $W(\mathbf{Z}) \xrightarrow{\sigma} W(R)$ is not injective, then* $\operatorname{Ker}(\sigma) = (\langle 2 \rangle - \langle 8 \rangle) W(\mathbf{Z})$.

Proof. Using 0.4 it is easy to see that in applying 0.2 to $\mathbf{Z}$ one need only check the conditions for primes a. Let $x \in \operatorname{Ker}(\sigma)$; since $W(\mathbf{Q}) \to W(K)$ is injective by 0.1, it follows that $W(\mathbf{Z} \to \mathbf{Q})(x) = 0$. If p is an odd prime, then $x \in \sigma^{-1}(\langle p^2 \rangle_R W(R)) = \langle p^2 \rangle W(\mathbf{Z}) (= \langle p \rangle W(\mathbf{Z}))$ as before. So by 0.2 and the remarks at the beginning of the proof, $\langle 4 \rangle x = 0$. Hence $(\langle 2 \rangle - \langle 8 \rangle) W(\mathbf{Z}) \subset \operatorname{Ker}(\sigma) \subset (1 - \langle 4 \rangle) W(\mathbf{Z})$. But since

$$\frac{(1 - \langle 4 \rangle) W(\mathbf{Z})}{(\langle 2 \rangle - \langle 8 \rangle) W(\mathbf{Z})} \cong \mathbf{Z}_2$$

and since $\langle 4 \rangle_R \neq 1$ (because $\mathbf{Z}_4$ is a homomorphic image of R by Theorem 2.2) the result follows.

Remark. Kenneth Kubota has pointed out to me that R and S need not be integrally closed for Lemma 1.3 to hold. For a field F, let $F^* = F - \{0\}$ and let F^{*2} denote the squares in F^*. Let S be an integral extension of R, where R and S are one-dimensional Noetherian domains with fields of fractions K and L, respectively. Suppose further that each residue class field R/P is finite. Then using a generalization of Lemma 1.3 Kubota proves that $W(R) \to W(S)$ is injective if and only if the following conditions hold. (i) $W(K) \to W(L)$ is injective. (ii) For each prime P of R, with $2 \in P$, there is a prime Q of S lying over P such that $(S/Q)^{*2} \cap R/P = (R/P)^{*2}$. (iii) For each prime P of R such that $R/P \cong \mathbf{Z}_2$, there is a prime Q of S lying over P such that $R/P^2 \to S/Q^2$ is an isomorphism.

Remark. Suppose S is an R-algebra with an augmentation $\rho : S \to R$; that is ρ is a ring homomorphism and $\rho \mid R$ is an isomorphism. Then since W is a functor it follows that $W(R) \to W(S)$ is injective. In particular if S is a group ring over R, this is the case.

Remark. It has been suggested by Harrison that the relation $\langle a \rangle = \langle a^3 \rangle$, which holds in $W(R)$ in many cases, might be added to the defining relations, and that the resulting ring, $\overline{W}(R)$, might be of interest. For example, 0.2 translates as follows for $R = \mathbf{Z}$. Let $a_1, \ldots, a_n$ be nonzero integers. Then $\langle a_1 \rangle + \cdots + \langle a_n \rangle = 0$ in $\overline{W}(\mathbf{Z})$ if and only if the quadratic form $a_1 x_1^2 + \cdots + a_n x_n^2$ is a sum of hyperbolic planes over $\mathbf{Q}$ and over $\mathbf{Z}_p$ for all odd primes p, and an even number of the a_i are odd. Other remarks on $\overline{W}(R)$ are found in [1].

It is easily seen that if R and S are algebraic integer rings as in 1.6, then $\overline{W}(R) \to \overline{W}(S)$ is always injective.

Acknowledgment

Thanks are due to Joel Cunningham for helpful conversations.

References

1. D. Coleman and J. Cunningham, Harrison's Witt ring of a commutative ring, *J. Algebra* **18** (1971), 549–564.
2. D. Coleman and J. Cunningham, Comparing Witt Rings, *J. Algebra* **28** (1974), 296–303.
3. F. Lorenz, "Quadratische Formen über Körpern," Lecture Notes in Mathematics No. 130, Springer-Verlag, Berlin, 1970.

Printed in Belgium