JOURNAL OF ALGEBRA 28, 296–303 (1974)

Comparing Witt Rings

D. B. COLEMAN AND JOEL CUNNINGHAM

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

Communicated by A. Fröhlich

Received September 4, 1972

INTRODUCTION

In [2] Harrison's Witt ring of a commutative ring R was defined, and the prime ideal structure for this ring was given in terms of the orderings of integral domain factor rings of R. Also in [2] some results were given which for special cases relate Harrison's Witt ring, which we here denote by $H(R)$, with the more standard Witt ring $W(R)$ based on inner product spaces over R. Note that we have changed notation from that used in [2] where we denoted Harrison's Witt ring as $W(R)$ and the inner product space Witt ring as Witt(R).

Recall that for R a commutative ring, $H(R)$ is the ring given by generators $\langle a\rangle$, $a \in R$, and relations $\langle 0\rangle = 0$, $\langle ab\rangle = \langle a\rangle\langle b\rangle$, and $\langle a\rangle + \langle b\rangle = \langle a + b\rangle + \langle (a + b)ab\rangle$. It is shown in [4] that for F a field with characteristic not 2, $H(F)$ is the classical Witt ring of F.

In the first section of this paper a proof is given that if R is any integral domain with quotient field K, then the map

$$H(R) \to H(K) \times \prod_{a\neq 0} H(R/a^2R)$$

is one-to-one. This result is due to D. K. Harrison and his students K. J. Hertz and D. A. Schoenfeld. The proof involves two results which are of independent interest. This result answers affirmatively the conjecture we made in [2, p. 560].

In the second section we consider $H^*(R)$, the subring of $H(R)$ generated by elements $\langle a\rangle$, where a is a unit of R, and $W^*(R)$, the subring of $W(R)$ composed of Witt classes of diagonal inner product spaces. We note that for any field F, $H(F) = H^*(F) \simeq W^*(F) = W(F)$. The main result is that $W^*(R) \simeq H^*(R)$ for any Dedekind domain R. From this we get that $W(R) \simeq H^*(R)$ for any semilocal principal ideal domain in which 2 is a unit. Such a result gives a set of generators for $W(R)$ along with relations that involve elements from the larger ring $H(R)$.

1

It was conjectured in [2] that for $x \in H(Z)$, $x = 0$ if and only if

$$H(Z \hookrightarrow Q)(x) = 0, \qquad H(Z \to Z/pZ)(x) = 0$$

for all odd primes p, and $H(Z \to Z/4Z)(x) = 0$ (Z denotes the integers). Harrison, Hertz and Schoenfeld developed methods which show that the conjecture is true, and that the theorem of this section holds in case 2 is a unit. The proof depends on two results of independent interest. The first is that H preserves localizations at multiplicative sets. The second is that H preserves direct limits of directed families of rings. Since these do not appear in print we give proofs for them here. We assume that these proofs are much like those given by Harrison, Hertz and Schoenfeld.

An H-map is a mapping $t\colon R \to S$ of commutative rings satisfying $t(0) = 0$, $t(ab) = t(a)\,t(b)$ and $t(a) + t(b) = t(a + b) + t((a + b)ab)$. Thus $\langle\ \rangle\colon R \to H(R)$ is a universal H-map.

Lemma 1.1 (Schoenfeld). *If S is a multiplicative subset of a commutative ring R, then $\langle S\rangle$ is a multiplicative subset of $H(R)$, and $H(S^{-1}R)$ is isomorphic to $\langle S\rangle^{-1}H(R)$ under an isomorphism taking $\langle r/s\rangle \mapsto \langle r\rangle/\langle s\rangle$ for $r \in R$, $s \in S$.*

Proof. For convenience assume that $1 \in S$. Clearly $\langle S\rangle$ is a multiplicative subset of $H(R)$. We will use $\langle\ \rangle$ to denote the canonical H-map for both $H(R)$ and $H(S^{-1}R)$.

Note that $t\colon R \to H(S^{-1}R)$ given by $t(r) = \langle r/1\rangle$ is an H-map, so there is a ring homomorphism $\mu\colon H(R) \to H(S^{-1}R)$ with $\mu(\langle r\rangle) = \langle r/1\rangle$. If $s \in S$, then $\mu(\langle s\rangle)$ is a unit in $H(S^{-1}R)$, so there is a homomorphism $\theta\colon \langle S\rangle^{-1}H(R) \to H(S^{-1}R)$ such that $\theta(\langle r\rangle/\langle s\rangle) = \langle r/s\rangle$.

To construct an inverse for θ we need to note that for any $s \in S$, $\langle s^2\rangle$ is an idempotent in $H(R)$ [2, (2.1)] so that $1/\langle s^2\rangle$ is an idempotent unit in $\langle S\rangle^{-1}H(R)$, hence $1/\langle s^2\rangle = 1$.

Define $h\colon S^{-1}R \to \langle S\rangle^{-1}H(R)$ by $h(r/s) = \langle r\rangle/\langle s\rangle$. One checks easily that h is well-defined, $h(0) = 0$, and that h preserves multiplication. For any r/s, r'/s' in $S^{-1}R$,

$$h\left(\frac{r}{s}\right) + h\left(\frac{r'}{s'}\right) = \frac{\langle rs'\rangle + \langle r's\rangle}{\langle ss'\rangle} = \frac{\langle rs' + r's\rangle}{\langle ss'\rangle} + \frac{\langle (rs' + r's)\,rr'\rangle}{\langle ss'\rangle^2}$$

$$= h\left(\frac{r}{s} + \frac{r'}{s'}\right) + h\left(\left(\frac{r}{s} + \frac{r'}{s'}\right)\frac{rr'}{ss'}\right).$$

Hence h is an H-map and induces a ring homomorphism $\varphi\colon H(S^{-1}R) \to \langle S\rangle^{-1}H(R)$ which is the inverse of θ. ∎

LEMMA 1.2 (Hertz). *If D is a directed set and $\{A_d\}_{d\in D}$ is a directed family of rings over D, then*

$$H(\varinjlim_{d\in D} A_d) \cong \varinjlim_{d\in D} H(A_d)$$

under an isomorphism such that $\langle[a]\rangle \mapsto [\langle a\rangle]$.

Proof. We have a partially ordered set $(D, \leqslant)$ such that for any $d, e \in D$, there is $f \in D$ with $d \leqslant f$ and $e \leqslant f$; and we have connecting homomorphisms $\varphi_{ed} : A_d \to A_e$ for $d \leqslant e$, with $\varphi_{dd} = 1_{A_d}$ and $\varphi_{fe} \circ \varphi_{ed} = \varphi_{fd}$ for $d \leqslant e \leqslant f$. It follows that $\{H(A_d): d \in D\}$ is a directed family with connecting homomorphisms $\{H(\varphi_{ed}): d \leqslant e\}$. So $\varinjlim_{d\in D} H(A_d)$ makes sense. For $d \in D$, $a \in A_d$, $x \in H(A_d)$, we denote by $[a]$ the element of $\varinjlim A_d$ corresponding to a and by $[x]$ the element of $\varinjlim H(A_d)$ corresponding to x.

Define t: $\varinjlim A_d \to \varinjlim H(A_d)$ by $t([a]) = [\langle a\rangle_{A_d}]$ for $a \in A_d$. One easily checks that t is an H-map, so it induces a ring homomorphism $\theta{:}H(\varinjlim A_d) \to \varinjlim H(A_d)$ with $\theta(\langle[a]\rangle) = [\langle a\rangle]$. Now for $d \in D$ let $\gamma_d : A_d \to \varinjlim A_d$ be the map $a \mapsto [a]$. Then for any $d \leqslant e$, $H(\gamma_e) \circ H(\varphi_{ed}) = H(\gamma_d)$. So by the universality of $\varinjlim H(A_d)$ there is a ring homomorphism φ: $\varinjlim H(A_d) \to H(\varinjlim A_d)$ such that for each $d \in D$, $H(\gamma_d) = \varphi \circ \gamma_d'$, where γ_d': $H(A_d) \to \varinjlim H(A_d)$ takes $x \mapsto [x]$. Hence $\varphi([\langle a\rangle_{A_d}]) = \langle[a]\rangle$ so that φ is the inverse of θ. ∎

PROPOSITION 1.3. *Let R be a commutative ring and let $a \in R$, $a \neq 0$. Let ν_{a^2}: $R \to R/a^2R$ be the natural map, and let $\gamma_{a^2} : R \to S^{-1}R$ be the canonical map, where $S = \{a^{2n}: n \geqslant 0\}$. Then* (1) $\mathrm{Ker}(H(\nu_{a^2})) = \langle a^2\rangle H(R)$ *and* (2) $\mathrm{Ker}(H(\gamma_{a^2})) = (1 - \langle a^2\rangle) H(R)$.

Proof. (1) follows from (3.1) of [2]. Note that if θ: $H(S^{-1}R) \to \langle S\rangle^{-1}H(R)$ is the isomorphism of Lemma (1.1) and η is the canonical map

$$H(R) \to \langle S\rangle^{-1} H(R),$$

then $\eta = \theta \circ H(\gamma_{a^2})$. So $\mathrm{Ker}(H(\gamma_{a^2})) = \mathrm{Ker}(\eta) = \{x \in H(R): \langle s\rangle x = 0$ for some $s \in S\} = \{x \in H(R): \langle a^2\rangle x = 0\} = (1 - \langle a^2\rangle) H(R)$. This last equality is because $\langle a^2\rangle$ is idempotent. This proves (2). ∎

Note 1.4. Let A be an integral domain with quotient field K and let $\mathscr{S}$ be the collection of all finitely generated multiplicative subsets of A that contain 1; i.e., all subsets $S = \{s_1^{m_1} \cdots s_n^{m_n}: m_i \geqslant 0\}$, for fixed nonzero elements $s_1, \ldots, s_n$ from A. Then $(\mathscr{S}, \subset)$ is a directed set and $\{S^{-1}A\}_{S\in\mathscr{S}}$ is a directed family of rings with connecting maps the inclusions. Since $K = \varinjlim_{S \in \mathscr{S}} S^{-1}A$, we have by Lemmas (1.2) and (1.3) that

$$H(K) \cong \varinjlim H(S^{-1}A) \cong \varinjlim \langle S\rangle^{-1} H(A)$$

via $\langle a/s\rangle \mapsto [\langle a/s\rangle] \mapsto [\langle a\rangle/\langle s\rangle]$. ∎

THEOREM 1.5. *Let A be a domain with quotient field K. Then $H(A) \to H(K) \times \prod_{a\neq 0} H(A/a^2A)$ is one-to-one.*

Proof. Let $i\colon A \to K$ be inclusion and $\nu_{a^2} : A \to A/a^2A$. We wish to show that the kernel of $H(i) \times \prod_{a\neq 0} H(\nu_{a^2})$ is zero. Let x be in this kernel. Then $H(i)(x) = 0$; so since

$$\begin{tikzcd} H(K) \arrow[rr] & & \varinjlim H(S^{-1}A) \\ & H(A) \arrow[ul] \arrow[ur] & \end{tikzcd}$$

commutes, there is $T \in \mathscr{S}$ such that $H(A \to T^{-1}A)(x) = 0$. If such a T is generated by $a_1, \ldots, a_n$, then letting $a = a_1 \cdots a_n$ and $S = \{a^{2k}\colon k \geqslant 0\}$, we see that $T^{-1}A = S^{-1}A$. Hence $x \in \operatorname{Ker}(H(A \to S^{-1}A)) = (1 - \langle a^2\rangle)\, H(A)$, this last equality by (1.3). But also $x \in \operatorname{Ker}(\nu_{a^2}) = \langle a^2\rangle\, H(A)$. So since $\langle a^2\rangle$is idempotent, $x = 0$. ∎

COROLLARY 1.6. *If D is a Dedekind domain with quotient field K, then $H(D) \to H(K) \times \prod H(D/P^2)$ is one-to-one, where P ranges over all nonzero prime ideals of D.*

Proof. Let $0 \neq a \in D$. Then there are prime ideals $P_1, \ldots, P_n$ and positive integers $e_1, \ldots, e_n$ such that $a^2D = P_1^{2e_1} \cdots P_n^{2e_n}$. Now it is easy to see from [2, (3.5)] that $H(D/P_i^{2e_i}) \to H(D/P_i^2)$ is an isomorphism. Hence since $D/a^2D \cong \prod_i D/P_i^{2e_i}$, we have by [2, (3.7)] an isomorphism $H(D/a^2D) \to \prod_i H(D/P_i^2)$. We are done by Theorem (1.5) and the commutative diagram

$$\begin{tikzcd} & H(D) \arrow[dl] \arrow[dr] & \\ H(D/a^2D) \arrow[rr, "\cong"] & & \prod_i H(D/P_i^2). \end{tikzcd}$$ ∎

It follows from [2, (3.6)] that if p is an odd rational prime, then $H(Z/p^2Z) \to H(Z/pZ)$ is an isomorphism. Thus the conjecture mentioned in the beginning of this section follows.

2

For any commutative ring R, $W(R)$ will denote the Witt ring based on inner product spaces over R. We will recall briefly how $W(R)$ is formed. For more detail, see [3, 5, 6, 7]. Let $X = (X, \beta)$ be an inner product space over R; i.e., X is a finitely generated projective R-module and $\beta: X \times X \to R$ is a symmetric bilinear form such that $x \to \beta(x, \ )$ is an isomorphism between X and $\mathrm{Hom}_R(X, R)$. We let $[X]$ denote the Witt class determined by X. Recall that $[X] = [X']$ if and only if there are metabolic (or split) spaces Y and Y' such that the orthogonal sums $X \perp Y$ and $X' \perp Y'$ are isometric. An inner product space is *metabolic* if it has an R-module direct summand that is its own orthogonal complement. The ring $W(R)$ consists of Witt classes of inner product spaces with addition induced by orthogonal direct sum and multiplication by tensor product.

In [2, Sect. 6] it was noted that if R is a local ring in which 2 is a unit, and with nil maximal ideal, then $H(R)$ and $W(R)$ are isomorphic, but for any Prüfer domain R not a field, the rings $H(R)$ and $W(R)$ are not isomorphic. We will see, however, that for a Dedekind domain R, the subring $W^*(R)$ of $W(R)$ consisting of Witt classes of diagonalizable spaces is isomorphic with a similar subring of $H(R)$.

For a unit a in the ring R, let $[a]$ denote the Witt class of the one-dimensional form $h_a : R \times R \to R$, where $h_a(x, y) = axy$. Thus $W^*(R)$ is the subring generated by the elements $[a]$.

Let $H^*(R)$ denote the subring of $H(R)$ generated by elements $\langle a \rangle$, where a is a unit in R. It is natural to ask whether there is an isomorphism $W^*(R) \to H^*(R)$ that takes $[a] \mapsto \langle a \rangle$ for units a.

Using (6.1) and (6.2) from [2], it is easy to see that if R is a local ring in which 2 is a unit, and such that for any unit a and non-unit x, $a^2 + x$ is a square in R, then we have the isomorphism $W^*(R) \to H^*(R)$. Note, however, that $W^*(Z/4Z) \ncong H^*(Z/4Z)$.

We now proceed with the Dedekind case.

LEMMA 2.1. *If K is any field, there is an isomorphism φ: $W(K) \to H(K)$ such that $\varphi([a]) = \langle a \rangle$ for all nonzero $a \in K$.*

Proof. If K has characteristic $\neq 2$, this is Harrison's characterization of $W(K)$ [4].

Assume K has characteristic 2. It is known that if H is the hyperbolic plane with form $h_1 \perp h_{-1}$, then for any inner product space X over K, $X \perp H$ is diagonalizable [1, p. 90]. Thus $W^*(K) = W(K)$. So to show that $[a] \mapsto \langle a \rangle$ induces a homomorphism φ: $W(K) \to H(K)$ it suffices to show that if $a_1, \dots, a_n, b_1, \dots, b_n$ are nonzero members of K with $h_{a_1} \perp \cdots \perp h_{a_n} \cong$

$h_{b_1} \perp \cdots \perp h_{b_n}$, then $\langle a_1 \rangle + \cdots + \langle a_n \rangle = \langle b_1 \rangle + \cdots + \langle b_n \rangle$ in $H(K)$. But the 2×2 theorem (see for example [6]) says that the given isometry is the composition of isometries $h_{c_1} \perp \cdots \perp h_{c_n} \cong h_{c_1'} \perp \cdots \perp h_{c_n'}$, where $c_i = c_i'$ for all but at most two values of i. Harrison proved in [4] that if $h_{a_1} \perp h_{a_2} \cong h_{b_1} \perp h_{b_2}$, then $\langle a_1 \rangle + \langle a_2 \rangle = \langle b_1 \rangle + \langle b_2 \rangle$. (There he is at characteristic $\neq 2$, but the argument carries over without change). Thus the mapping φ is well-defined, and is clearly a ring surjection.

The elements $[a]$, with $a \in K$, satisfy the defining relations of $H(K)$, defining $[0] = 0$. Thus there is a homomorphism $H(K) \to W(K)$ that is the inverse of φ. ∎

THEOREM 2.2. *If R is a Dedekind domain, then $W^*(R) \cong H^*(R)$ under an isomorphism taking $[a] \mapsto \langle a \rangle$ for units $a \in R$.*

Proof. Suppose that $a_1, \ldots, a_n$ are units in R such that $\langle a_1 \rangle + \cdots + \langle a_n \rangle = 0$ in $H(R)$. Letting K denote the quotient field of R, $\langle a_1 \rangle + \cdots + \langle a_n \rangle = 0$ in $H(K)$. By (2.1), we have $[a_1] + \cdots + [a_n] = 0$ in $W(K)$. But for Dedekind domains, $W(R) \to W(K)$ is injective [5, p. 47]. Thus there is a ring surjection $\psi\colon H^*(R) \to W^*(R)$ such that $\psi(\langle a \rangle) = [a]$ if a is a unit. We show that ψ is injective. Suppose $a_1, \ldots, a_n$ are units such that $[a_1] + \cdots + [a_n] = 0$ in $W(R)$. To show that $\langle a_1 \rangle + \cdots + \langle a_n \rangle = 0$ in $H(R)$ it suffices by (1.6) to show that $\langle a_1 \rangle + \cdots + \langle a_n \rangle = 0$ in $H(K)$ and in $H(R/P^2)$ for each prime ideal P of R, The isomorphism between $H(K)$ and $W(K)$ takes care of $H(K)$. For the primes ideals we consider two cases.

Case 1. R/P has more than two elements. In this case there are units a and b in R/P^2 such that $a + b$ is also a unit. Hence the natural mapping $H(R/P^2) \to H(R/P)$ is an isomorphism [2, (3.5)]. Since $[a_1] + \cdots + [a_n]$ in $W(R)$ maps to $\langle a_1 \rangle + \cdots + \langle a_n \rangle$ in $H(R/P)$ under $W(R) \to W(R/P) \cong H(R/P)$, we have $\langle a_1 \rangle + \cdots + \langle a_n \rangle = 0$ in $H(R/P)$, hence in $H(R/P^2)$.

Case 2. $R/P \cong Z_2 = Z/2Z$. In this case $H(R/P^2) \cong Z_2(C_2)$, the group ring of the group $C_2 = \{1, g\}$ of order 2 over Z_2. The isomorphism is induced by $\langle x \rangle \mapsto 1 + g$, where P/P^2 is generated by x, and $\langle a \rangle \mapsto 1$ if a is a unit in R/P^2. Thus $H^*(R/P^2) \cong Z_2$. Hence for units $a_1, \ldots, a_n$ in R, $\langle a_1 \rangle + \cdots + \langle a_n \rangle = 0$ in $H(R/P^2)$ if and only if n is even. Our assumption that $[a_1] + \cdots + [a_n] = 0$ in $W(R)$, hence in $W(K)$, insures that n is even. Hence $\langle a_1 \rangle + \cdots + \langle a_n \rangle = 0$ in $H(R/P^2)$.

The following result is probably known to specialists but we have not seen it in this form. However cf. [7, (1, 3.4)] and [5, (5.4.1)]. ∎

PROPOSITION 2.3. *If R is a semilocal ring in which 2 is a unit, and over* *which every finitely generated projective module is free, then* $W(R) = W^*(R)$. *In fact every inner product space over R has an orthogonal basis.*

Proof. Let X be an inner product space over R. It is well-known that there are units $a_1, \ldots, a_n$ in R such that $X \cong [a_1] \perp \cdots \perp [a_n] \perp Y$, where $Y = (Y, \beta)$ is an inner product space with $\beta(y, y)$ a nonunit for all $y \in Y$. (See [7, (1, 3.3)]). So it suffices to show that $Y = 0$. Just suppose $Y \neq 0$. By hypothesis, Y is free, say with basis $e_1, \ldots, e_k$, $k > 0$. Let $e_1^{\#}, \ldots, e_k^{\#}$ be a dual basis for $e_1, \ldots, e_k$; i.e., another basis for Y such that $\beta(e_i, e_j^{\#}) = \delta_{ij}$ (see [7, (1, 2.6)]).

Let $P_1, \ldots, P_m$ be the maximal ideals of R. For each i, there is $x_i \in Y$ such that $\beta(x_i, x_i) \notin P_i$. Because otherwise

$$2 = 2\beta(e_1, e_1^{\#}) = \beta(e_1 + e_1^{\#}, e_1 + e_1^{\#}) - \beta(e_1, e_1) - \beta(e_1^{\#}, e_1^{\#})$$

is in P_i, contradicting the hypothesis that 2 is a unit. Write

$$x_i = a_{i_1}e_1 + \cdots + a_{ik}e_k, \qquad a_{ij} \in R.$$

By the Chinese Remainder Theorem, there is for each $j = 1, \ldots, k$, some $b_j \in R$ such that $b_j \equiv a_{ij} (\text{mod } P_i)$ for all i. Let $y = b_1e_1 + \cdots + b_ke_k$. Then for each i,

$$\beta(y, y) \equiv \beta(x_i, x_i) \not\equiv 0 \ (\text{mod } P_i).$$

Hence $\beta(y, y)$ is a unit, a contradiction. ∎

Every semilocal Dedekind domain is a PID. Since every finitely generated projective over a PID is free, (2.2) and (2.3) give the following.

COROLLARY 2.4. *If R is a semilocal principal ideal domain in which* 2 *is a unit, then* $W(R) = W^*(R) \cong H^*(R)$. ∎

Note, however, that if R is the semilocal ring Z_{21}, then $H^*(R) \cong W^*(R)$ and $W(R) \cong H(R)$, but $H^*(R) \subsetneqq H(R)$. In fact $H(R) \cong Z_4 \times Z_4$ and $H^*(R)$ has eight elements. In general one can check, using [3, (6.5)] and [2, (3.7)], that if R is any finite product of fields, then $W^*(R) \cong H^*(R)$. Note also that $Z_{21} \cong Z_7 \times Z_3$ illustrates that neither H^* nor W^* preserves finite products.

REFERENCES

1. N. BOURBAKI, "Algèbre," Chap. 9, Act. Sc. Ind. 1272, Hermann, Paris, 1959.
2. D. B. COLEMAN AND J. CUNNINGHAM, Harrison's Witt ring of a commutative ring, *J. Algebra* 18 (1971), 549–563.

3. A. Fröhlich and A. McEvett, Forms over rings with involution, *J. Algebra* 12 (1969), 79–104.
4. D. K. Harrison, "Witt Rings," Lecture notes, Department of Mathematics, University of Kentucky, 1970.
5. M. Knebusch, "Grothendieck–und Wittringe von nichtausgearteten symmetrischen Bilinearformen, Sitzber. Akad. Wiss., Math. Nat. Kl. (Heidelberg) 3 (1969/70), 1–69.
6. M. Knebusch, A. Rosenberg, and R. Ware, Structure of Witt rings and quotients of abelian group rings, *Amer. J. Math.* **94** (1972), 119–155.
7. J. Milnor, D. Husemoller, Symmetric Bilinear Forms, "Ergebnisse der Mathematik," Vol. 73, Springer, Berlin, 1973.