STRUCTURE OF WITT RINGS, QUOTIENTS OF ABELIAN GROUP RINGS, AND ORDERINGS OF FIELDS

BY

MANFRED KNEBUSCH, ALEX ROSENBERG, AND
ROGER WARE

Reprinted from the
BULLETIN OF THE AMERICAN MATHEMATICAL SOCIETY
March, 1971, Vol. 77, No. 2
Pp. 205-210

BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 77, Number 2, March 1971

STRUCTURE OF WITT RINGS, QUOTIENTS OF ABELIAN GROUP RINGS, AND ORDERINGS OF FIELDS

BY MANFRED KNEBUSCH, ALEX ROSENBERG[1] AND ROGER WARE[2]

Communicated October 19, 1970

1. **Introduction.** In 1937 Witt [9] defined a commutative ring $W(F)$ whose elements are equivalence classes of anisotropic quadratic forms over a field F of characteristic not 2. There is also the Witt-Grothendieck ring $WG(F)$ which is generated by equivalence classes of quadratic forms and which maps surjectively onto $W(F)$. These constructions were extended to an arbitrary pro-finite group, $\mathfrak{G}$, in [1] and [6] yielding commutative rings $W(\mathfrak{G})$ and $WG(\mathfrak{G})$. In case $\mathfrak{G}$ is the galois group of a separable algebraic closure of F we have $W(\mathfrak{G})=W(F)$ and $WG(\mathfrak{G})=WG(F)$. All these rings have the form $\boldsymbol{Z}[G]/K$ where G is an abelian group of exponent two and K is an ideal which under any homomorphism of $\boldsymbol{Z}[G]$ to $\boldsymbol{Z}$ is mapped to 0 or $\boldsymbol{Z}2^n$. If C is a connected semilocal commutative ring, the same is true for the Witt ring $W(C)$ and the Witt-Grothendieck ring $WG(C)$ of symmetric bilinear forms over C as defined in [2], and also for the similarly defined rings $W(C, J)$ and $WG(C, J)$ of hermitian forms over C with respect to some involution J.

In [5], Pfister proved certain structure theorems for $W(F)$ using his theory of multiplicative forms. Simpler proofs have been given in [3], [7], [8]. We show that these results depend only on the fact that $W(F)\cong\boldsymbol{Z}[G]/K$, with K as above. Thus we obtain unified proofs for all the Witt and Witt-Grothendieck rings mentioned.

Detailed proofs will appear elsewhere.

2. **Homomorphic images of group rings.** Let G be an abelian torsion group. The characters χ of G correspond bijectively with the homomorphisms ψ_χ of $\boldsymbol{Z}[G]$ into some ring A of algebraic integers generated by roots of unity. (If G has exponent 2, then $A=\boldsymbol{Z}$.) The minimal prime ideals of $\boldsymbol{Z}[G]$ are the kernels of the homomorphisms $\psi_\chi:\boldsymbol{Z}[G]\to A$. The other prime ideals are the inverse images under the ψ_χ of the maximal ideals of A and are maximal.

AMS 1970 *subject classifications*. Primary 15A63, 16A26, 13A15; Secondary 13D15, 13F05, 20C15.

Key words and phrases. Witt ring, quadratic forms, hermitian forms, torsion of Witt rings, orderings of a field, group rings of abelian torsion groups.

[1] Partially supported by N.S.F. Grant GP-9395.

[2] Partially supported by an N.S.F. traineeship.

THEOREM 1. *If M is a maximal ideal of $\mathbf{Z}[G]$ the following are equivalent*:

(1) *M contains a unique minimal prime ideal.*

(2) *The rational prime p such that $M\cap\mathbf{Z}=\mathbf{Z}p$ does not occur as the order of any element of G.*

In the sequel K is a proper ideal of $\mathbf{Z}[G]$ and R denotes $\mathbf{Z}[G]/K$.

PROPOSITION 2. *The nil radical,* Nil R, *is contained in the torsion subgroup, R^t. We have $R^t=\text{Nil } R$ if and only if no maximal ideal of R is a minimal prime ideal and $R^t=R$ if and only if all maximal ideals of R are minimal prime ideals.*

THEOREM 3. *If p is a rational prime which does not occur as the order of any element of G, the following are equivalent*:

(1) *R has nonzero p-torsion.*

(2) *R has nonnilpotent p-torsion.*

(3) *R contains a minimal prime ideal $\overline{M}$ such that $R/\overline{M}$ is a field of characteristic p.*

(4) *There exists a character χ of G with $0\neq\psi_\chi(K)\cap\mathbf{Z}\subset\mathbf{Z}p$.*

In addition, suppose now that G is an abelian q-group for some rational prime q. Then $\mathbf{Z}[G]$ contains a unique prime ideal M_0 which contains q.

COROLLARY 4. *The following are equivalent*:

(1) *R^t is q-primary.*

(2) *Let M be a maximal ideal of R which does not contain q, then M is not a minimal prime ideal.*

(3) *For all characters χ of G, $\psi_\chi(K)\cap\mathbf{Z}=0$ or $\mathbf{Z}q^{n(\chi)}$.*

(4) *$K\subset M_0$ and all the zero divisors of R lie in $\overline{M}_0=M_0/K$.*

THEOREM 5. *$R^t\subset\text{Nil } R$ if and only if $K\cap\mathbf{Z}=0$ and one (hence all) of* (1), (2), (3), (4) *of Corollary* 4 *hold.*

THEOREM 6. *If K satisfies the conditions of Theorem* 5,

(1) *$R^t=\text{Nil } R$,*

(2) *$R^t\neq 0$ if and only if $\overline{M}_0$ consists entirely of zero divisors,*

(3) *R is connected.*

THEOREM 7. *The following are equivalent*:

(1) *For all characters χ we have $\psi_\chi(K)\cap\mathbf{Z}=\mathbf{Z}q^{n(\chi)}$.*

(2) *$R=R^t$ is a q-torsion group.*

(3) *$K\cap\mathbf{Z}=\mathbf{Z}q^n$.*

(4) *$M_0\supset K$ and $\overline{M}_0$ is the unique prime ideal of R.*

These results apply to the rings mentioned in §1 with $q=2$. In particular, Theorems 5 and 6 yield the results of [5, §3] for Witt rings of formally real fields and Theorem 7 those of [5, §5] for Witt rings of nonreal fields.

By studying subrings of the rings described in Theorems 5–7 and using the results of [2] for symmetric bilinear forms over a Dedekind ring C and similar results for hermitian forms over C with respect to some involution J of C, we obtain analogous structure theorems for the rings $W(C)$, $WG(C)$, $W(C, J)$ and $WG(C, J)$. In particular, all these rings have only two-torsion, $R^t = \mathrm{Nil}\, R$ in which case no maximal ideal is a minimal prime ideal or $R^t = R$ in which case R contains a unique prime ideal. The forms of even dimension are the unique prime ideal containing two which contains all zero divisors of R. Finally, any maximal ideal of R which contains an odd rational prime contains a unique minimal prime ideal of R.

3. **Topological considerations and orderings on fields.** Throughout this section G will be a group of exponent 2 and $R = \mathbf{Z}[G]/K$ with K satisfying the equivalent conditions of Theorem 5. The images in R of elements g in G will be written $\bar{g}$. For a field F let $\dot{F} = F - \{0\}$. Then $W(F) = \mathbf{Z}[\dot{F}/\dot{F}^2]/K$ with K satisfying the conditions of Corollary 4. In this case K satisfies the conditions of Theorem 5 if and only if F is a formally real field.

THEOREM 8. *Let X be the set of minimal prime ideals of R. Then*

(a) *in the Zariski topology X is compact, Hausdorff, totally disconnected.*

(b) *X is homeomorphic to* $\mathrm{Spec}(\mathbf{Q} \otimes_{\mathbf{Z}} R)$ *and $\mathbf{Q} \otimes_{\mathbf{Z}} R \cong C(X, \mathbf{Q})$ the ring of $\mathbf{Q}$-valued continuous functions on X where $\mathbf{Q}$ has the discrete topology.*

(c) *For each P in X we have $R/P \cong \mathbf{Z}$ and $R_{red} = R/\mathrm{Nil}(R) \subset C(X, \mathbf{Z}) \subset C(X, \mathbf{Q})$ with $C(X, \mathbf{Z})/R_{red}$ being a 2-primary torsion group and $C(X, \mathbf{Z})$ being the integral closure of R_{red} in $\mathbf{Q} \otimes_{\mathbf{Z}} R$.*

(d) *By a theorem of Nöbeling [4], R_{red} is a free abelian group and hence we have a split exact sequence*

$$0 \to \mathrm{Nil}(R) \to R \to R_{red} \to 0$$

of abelian groups.

Harrison (unpublished) and Lorenz-Leicht [3] have shown that the set of orderings on a field F is in bijective correspondence with X

when $R=W(F)$. Thus the set of orderings on a field can be topologized to yield a compact totally disconnected Hausdorff space.

Let F be an ordered field with ordering $<$, $F_<$ a real closure of F with regard to $<$, and $\sigma_<$ the natural map $W(F)\rightarrow W(F_<)$. Since $W(F_<)\cong \mathbf{Z}$ (Sylvester's law of inertia), Ker $\sigma_< = P_<$ is a prime ideal of $W(F)$. Let the character $\chi_< \in \mathrm{Hom}(\dot F/\dot F^2, \pm 1)$ be defined by

$$\begin{aligned}\chi_<(aF^2) &= 1 \quad \text{if } a > 0,\\ &= -1 \quad \text{if } a < 0.\end{aligned}$$

PROPOSITION 9. *For u in R the following statements are equivalent*:

(a) *u is a unit in R.*

(b) *$u\equiv \pm 1$ mod P for all P in X.*

(c) *$u=\pm \bar g + s$ with g in G and s nilpotent.*

COROLLARY 10 (PFISTER [5]). *Let F be a formally real field and $R=W(F)$. Then u is a unit in R if and only if $\sigma_<(u)=\pm 1$ for all orderings $<$ on F.*

Let E denote the family of all open-and-closed subsets of X.

DEFINITION. Harrison's subbasis H of E is the system of sets

$$W(a) = \{P \in X \mid a \equiv -1 \pmod P\}$$

where a runs over the elements $\pm\bar g$ of R.

If F is a formally real field and $R=W(F)$ then identifying X with the set of orderings on F one sees that the elements of H are exactly the sets

$$W(a) = \{<\text{on } F \mid a < 0\}, \qquad a \in \dot F.$$

PROPOSITION 11. *Regarding R_{red} as a subring of $C(X, \mathbf{Z})$ we have*

$$R_{red} = \mathbf{Z}\cdot 1 + \sum_{U\in H} \mathbf{Z}\cdot 2f_U$$

where f_U is the characteristic function of $U\subset X$.

Following Bel'skiĭ [1] we call $R=\mathbf{Z}[G]/K$ a *small Witt ring* if there exists g in G with $1+g$ in K. Note that for F a field, $W(F)$ is of this type.

THEOREM 12. *For a small Witt ring R the following statements are equivalent*:

(a) *$E=H$.*

(b) (*Approximation.*) *Given any two disjoint closed subsets Y_1, Y_2 of X there exists g in G such that $\bar g\equiv -1 \pmod P$ for all P in Y_1 and $\bar g \equiv 1 \pmod P$ for all P in Y_2.*

(c) $R_{red} = \boldsymbol{Z}\cdot 1 + C(X, 2\boldsymbol{Z})$.

COROLLARY 13. *For a formally real field F the following statements are equivalent:*

(a) *If U is an open-and-closed subset of orderings on F then there exists a in* $\dot{F}$ *such that* $<$ *is in U if and only if* $a<0$.

(b) *Given two disjoint closed subsets* Y_1, Y_2 *of orderings on F there exists a in* $\dot{F}$ *such that* $a<0$ *for* $<$ *in* Y_1 *and* $a>0$ *for* $<$ *in* Y_2.

(c) $W(F)_{red} = \boldsymbol{Z}\cdot 1 + C(X, 2\boldsymbol{Z})$.

PROPOSITION 14. *Suppose F is a field with* $\dot{F}/\dot{F}^2$ *finite of order* 2^n. *Then there are at most* 2^{n-1} *orderings of F.*

If F is a field having orderings $<_1, \cdots, <_n$ we denote by σ the natural map $W(F) \to W(F_{<_1}) \times \cdots \times W(F_{<_n}) = \boldsymbol{Z} \times \cdots \times \boldsymbol{Z}$ via $r \to (\sigma_{<_1}(r), \cdots, \sigma_{<_n}(r))$.

THEOREM 15. *Let* $<_1, \cdots, <_n$ *be orderings on a field F. Then the following statements are equivalent:*

(a) *For each i there exists a in* $\dot{F}$ *such that* $a <_i 0$ *and* $0 <_j a$ *for* $j \neq i$.

(b) $\chi_{<_1}, \cdots, \chi_{<_n}$ *are linearly independent elements of* $\mathrm{Hom}(\dot{F}/\dot{F}^2, \pm 1)$.

(c) $\mathrm{Im}\,\sigma = \{(b_1, \cdots, b_n) \mid b_i \equiv b_j \pmod 2$ *for all* $i, j\}$.

If F is the field $\boldsymbol{R}((x))((y))$ of iterated formal power series in 2 variables over the real field, F has four orderings, $W(F) = W(F)_{red}$ is the group algebra of the Klein four group, and the conditions of Theorem 15 fail.

COROLLARY 16. *Suppose F is a field with* $\dot{F}/\dot{F}^2$ *finite of order* 2^n. *If condition* (a) *of Theorem* 15 *holds for the orderings on F then there are at most n orderings on F.*

REFERENCES

1. A. A. Bel'skiĭ, *Cohomological Witt rings*, Izv. Akad. Nauk SSSR Ser. Mat. **32** (1968), 1147–1161 = Math. USSR Izv. 2 (1968), 1101–1115. MR **39** #5666.

2. M. Knebusch, *Grothendieck-und Wittringe von nichtausgearteten symmetrischen Bilinearformen*, S.-B. Heidelberger Akad. Wiss. Math.-Natur. Kl. **1969**, 93–157.

3. F. Lorenz und J. Leicht, *Die Primideale des Wittschen Ringes*, Invent. Math. **10** (1970), 82–88.

4. G. Nöbeling, *Verallgemeinerung eines Satzes von Herrn E. Specker*, Invent. Math. **6** (1968), 41–55. MR **38** #233.

5. A. Pfister, *Quadratische Formen in beliebigen Körpern*, Invent. Math. **1** (1966), 116–132. MR **34** #169.

6. W. Scharlau, *Quadratische Formen und Galois-Cohomologie*, Invent. Math. **4** (1967), 238–264. MR **37** #1442.

7. ———, *Zur Pfisterschen Theorie der quadratischen Formen*, Invent. Math. **6** (1969), 327–328. MR **39** #2793.

8. ———, *Induction theorems and the Witt group*, Invent. Math. **11** (1970), 37–44.

9. E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern*, J. Reine Angew. Math. **176** (1937), 31–44.

MATHEMATISCHES INSTITUT, UNIVERSITÄT DES SAARLANDES, SAARBRÜCKEN, GERMANY

CORNELL UNIVERSITY, ITHACA, NEW YORK 14850

NORTHWESTERN UNIVERSITY, EVANSTON, ILLINOIS 60202