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, \( G \), in [1] and [6] yielding commutative rings \( W(G) \) and \( WG(G) \). In case \( G \) is the galois group of a separable algebraic closure of \( F \) we have \( W(G) = W(F) \) and \( WG(G) = WG(F) \). All these rings have the form \( \mathbb{Z}[G]/K \) where \( G \) is an abelian group of exponent two and \( K \) is an ideal which under any homomorphism of \( \mathbb{Z}[G] \) to \( \mathbb{Z} \) is mapped to 0 or \( \mathbb{Z}/2^n \). 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 \( W(F) \cong \mathbb{Z}[G]/K \), 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 \( \chi \) of \( G \) correspond bijectively with the homomorphisms \( \psi_\chi \) of \( \mathbb{Z}[G] \) into some ring \( A \) of algebraic integers generated by roots of unity. (If \( G \) has exponent 2, then \( A = \mathbb{Z} \).) The minimal prime ideals of \( \mathbb{Z}[G] \) are the kernels of the homomorphisms \( \psi_\chi : \mathbb{Z}[G] \to A \). The other prime ideals are the inverse images under the \( \psi_\chi \) of the maximal ideals of \( A \) and are maximal.
Theorem 1. If $M$ is a maximal ideal of $\mathbb{Z}[G]$ the following are equivalent:

1. $M$ contains a unique minimal prime ideal.
2. The rational prime $p$ such that $M \cap \mathbb{Z} = \mathbb{Z}p$ does not occur as the order of any element of $G$.

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

Proposition 2. The nil radical, $\text{Nil } R$, 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 $\chi$ of $G$ with $0 \neq \psi_x(K) \cap \mathbb{Z} \subset \mathbb{Z}p$.

In addition, suppose now that $G$ is an abelian $q$-group for some rational prime $q$. Then $\mathbb{Z}[G]$ 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 $\chi$ of $G$, $\psi_x(K) \cap \mathbb{Z} = 0$ or $\mathbb{Z}q^n(x)$.
4. $K \subseteq M_0$ and all the zero divisors of $R$ lie in $\overline{M}_0 = M_0/K$.

Theorem 5. $R^t \subseteq \text{Nil } R$ if and only if $K \cap \mathbb{Z} = 0$ 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 $\chi$ we have $\psi_x(K) \cap \mathbb{Z} = \mathbb{Z}q^n(x)$.
2. $R = R^t$ is a $q$-torsion group.
3. $K \cap \mathbb{Z} = \mathbb{Z}q^n$.
4. $M_0 \supseteq K$ 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 \( \mathcal{C} \) and similar results for hermitian forms over \( \mathcal{C} \) with respect to some involution \( J \) of \( \mathcal{C} \), we obtain analogous structure theorems for the rings \( W(\mathcal{C}), W_G(\mathcal{C}), W(\mathcal{C}, J) \) and \( W_G(\mathcal{C}, J) \). In particular, all these rings have only two-torsion, \( R^* = \text{Nil } R \) in which case no maximal ideal is a minimal prime ideal or \( R^* = R \) 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 \( R = \mathbb{Z}[G]/K \) 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 \( \bar{F} = F - \{0\} \). Then \( W(F) = \mathbb{Z}[\bar{F}/F^2]/K \) 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 \( \text{Spec}(\mathcal{Q} \otimes \mathbb{Z} R) \) and \( \mathcal{Q} \otimes \mathbb{Z} R \cong C(X, \mathcal{Q}) \) the ring of \( \mathcal{Q} \)-valued continuous functions on \( X \) where \( \mathcal{Q} \) has the discrete topology.

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

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

\[
0 \rightarrow \text{Nil}(R) \rightarrow R \rightarrow R_{\text{red}} \rightarrow 0
\]

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 \( < \), \( F_\sigma \) a real closure of \( F \) with regard to \( < \), and \( \sigma < \) the natural map \( W(F) \to W(F_\sigma) \). Since \( W(F_\sigma) \cong Z \) (Sylvester's law of inertia), \( \ker \sigma_< = P_\sigma \) is a prime ideal of \( W(F) \). Let the character \( \chi_< \in \text{Hom}(\hat{F}/\hat{F}^2, \pm 1) \) be defined by

\[
\chi_<(aF^\pm) = \begin{cases} 
1 & \text{if } a > 0, \\
-1 & \text{if } a < 0.
\end{cases}
\]

**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

\[
W(a) = \{ P \in X \mid a \equiv -1 \mod P \}
\]

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

\[
W(a) = \{ \sigma < F \mid a < 0 \}, \quad a \in \hat{F}.
\]

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

\[
R_{\text{red}} = Z \cdot 1 + \sum_{U \in H} Z \cdot 2f_U
\]

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

Following Bel'skiï [1] we call \( R = Z[G]/K \) 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) \( \text{(Approximation.)} \) Given any two disjoint closed subsets \( Y_1, Y_2 \) of \( X \) there exists \( g \) in \( G \) such that \( \bar{g} \equiv -1 \mod P \) for all \( P \) in \( Y_1 \) and \( \bar{g} \equiv 1 \mod P \) for all \( P \) in \( Y_2 \).
(c) \( R_{\text{red}} = \mathbb{Z} \cdot 1 + C(X, 2\mathbb{Z}) \).

**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 \( \hat{F} \) 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 \( \hat{F} \) such that \( a < 0 \) for \( < \) in \( Y_1 \) and \( a > 0 \) for \( < \) in \( Y_2 \).

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

**Proposition 14.** Suppose \( F \) is a field with \( \hat{F}/\hat{F}^2 \) finite of order \( 2^n \). Then there are at most \( 2^{n-1} \) orderings of \( F \).

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

**Theorem 15.** Let \( <_1, \ldots, <_n \) be orderings on a field \( F \). Then the following statements are equivalent:

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

(b) \( \chi_{<_1}, \ldots, \chi_{<_n} \) are linearly independent elements of \( \text{Hom}(\hat{F}/\hat{F}^2, \pm 1) \).

(c) \( \text{Im} \sigma = \{ (b_1, \ldots, b_n) | b_i \equiv b_j \pmod{2} \text{ for all } i, j \} \).

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

**Corollary 16.** Suppose \( F \) is a field with \( \hat{F}/\hat{F}^2 \) 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**


**MATHEMATISCHES INSTITUT, UNIVERSITÄT DES SAARLANDES, SAARBRÜCKEN, GERMANY**

**CORNELL UNIVERSITY, ITHACA, NEW YORK 14850**

**NORTHWESTERN UNIVERSITY, EVANSTON, ILLINOIS 60202**