STRUCTURE OF WITT RINGS AND QUOTIENTS OF ABELIAN GROUP RINGS

BY

MANFRED KNEBUSCH, ALEX ROSENBERG AND ROGER WARE

[Reprinted from *American Journal of Mathematics*, Vol. XCIV, No. 1, January, 1972.]

STRUCTURE OF WITT RINGS AND QUOTIENTS OF ABELIAN GROUP RINGS.

By MANFRED KNEBUSCH, ALEX ROSENBERG[1] and ROGER WARE.[2]

In this paper we give a detailed exposition of some of the results announced in [18]. The primary motivation for this work is Witt's observation [31, Satz 7] that if F is a field of characteristic $\neq 2$, his ring $W(F)$ of classes of anisotropic quadratic forms may be written as $\mathbf{Z}[G]/K$ where G is an abelian group of exponent two (actually $G = F^*/F^{*2}$), $\mathbf{Z}[G]$ is the integral group ring of G, and K is an ideal of $\mathbf{Z}[G]$ generated by elements of the form $g_1 + g_2 - g_3 - g_4$ and $1 + g_5$ with g_i in G. Of course these elements can be described more explicitly, but for our purposes the only information we need about K is that any homomorphism of $\mathbf{Z}[G] \to \mathbf{Z}$ sends K to 0 or to an ideal of the form $2^n\mathbf{Z}$. In this introduction we shall call any ideal of $\mathbf{Z}[G]$ with this property "admissible."

In [26], Pfister proved certain structure theorems for $W(F)$ using his theory of multiplicative forms. His proofs were simplified in [11, 22, 23, 29, 30]. Harrison [11] and Leicht and Lorenz [22] gave important complements to Pfister's results concerning the ideal theory of $W(F)$. The main goal of our paper is to understand and generalize these structure theorems using standard techniques of commutative algebra.

In [28] and [3], Scharlau and Belskii have introduced and studied Witt and Witt-Grothendieck rings for profinite groups. Their definitions generalize the usual notions of Witt rings, $W(F)$, and Witt-Grothendieck rings, $K(F)$, of quadratic forms over fields of characteristic $\neq 2$. These rings also have the form $\mathbf{Z}[G]/K$ with G an abelian group of exponent two and K an admissible ideal of $\mathbf{Z}[G]$.

Here we are mainly interested in another generalization of $W(F)$ and $K(F)$, namely the Witt rings, $W(C, J)$, and the Witt-Grothendieck rings, $K(C, J)$ of classes of hermitian forms over a connected commutative semi-local ring C with involution J. Since J may be the identity these include the Witt and Witt-Grothendieck rings of classes of symmetric bilinear forms

Received April 26, 1971.

[1] Partially supported by NSF Grant GP-9395 and GP-25600.

[2] Partially supported by a NSF-traineeship and NSF Grant GP-23861.

defined in [16] and [17]. In 1. we show that $W(C,J)$ and $K(C,J)$ are again of the form $\mathbf{Z}[G]/K$ with G an abelian group of exponent two and K an admissible ideal of $\mathbf{Z}[G]$.

All the rings described so far are integral over $\mathbf{Z}$. Consequently, in 2. we study the ideal theory of such integral extensions. In 3. we consider the following situation: Let q be a rational prime, G an abelian q-group, and $\mathfrak{A}$ the ring of integers of the algebraic number field generated by the values of all the characters of G. If G has exponent two, $\mathfrak{A}=\mathbf{Z}$. Our aim is to characterize the rings $\mathbf{Z}[G]/K$ for which the main structure results of [26, 11, 22] remain valid. We show that this happens if and only if for all homomorphisms ψ of $\mathbf{Z}[G]$ to $\mathfrak{A}$, the ideals $\psi(K)\cap\mathbf{Z}$ are 0 or $q^n\mathbf{Z}$. We call such commutative rings *Witt rings for G*. In 3. some further properties of these rings are given. In particular, we show that if R is a Witt ring for an abelian q-group the exact sequence $0\to \operatorname{Rad} R\to R\to R/\operatorname{Rad} R\to 0$ splits as an exact sequence of abelian groups. Furthermore, we study the group of units of finite order of R. If G has exponent q, this group is generated by $\{\pm 1\}$, the image of G in R, and $1+\operatorname{Nil} R$.

We also study residue class rings of $\mathbf{Z}[G]$ where G is an arbitrary abelian torsion group (Theorem 2.14, Proposition 3.4, Theorem 3.8).

Our methods thus yield unified proofs of the structure theorems of [11, 22, 26] for $W(F)$, $W(C,J)$, $K(C,J)$ and the rings defined in [3] and [28]. For the latter case they answer questions posed on [28, p. 262]. In [19] we shall draw some conclusions for semi-local rings from our results and in [20] we shall give similar structure theorems for $W(C,J)$ and $K(C,J)$ in case C is a Dedekind domain. For this last reason we develop the theory of hermitian forms in 1. slightly more generally than needed for this present paper.

If C is a field, the proofs in [11, 22, 23, 29, 30] of the structure theorems for $W(C,J)$, with J the identity, are brief and elegant. However, in the semi-local case our methods provide a much easier approach (cf. [17, § 2], where some structure theorems have been proved by traditional methods for C semi-local and J the identity).

On the other hand, these traditional methods yield information about hermitian forms and not only about elements of Witt rings. Such information seems not always to be attainable by means of our ring purely theoretical approach.

The only result of Section 1 that is used in Sections 2 and 3 of this paper is Corollary 1.21. Indeed, it is used in the last two sections only in certain remarks and examples to provide motivation for the ideas developed

there. Thus, Sections 2 and 3 can be read independently of Section 1. In any case Corollary 1.21 is well known to hold for $W(F)$ when F is a field of characteristic not two. The methods of Section 1 are quite different from those in the last two. This section was included, however, because the structure theory of $W(C,J)$, for C a connected commutative semi-local ring, provides, at present, one of the best applications of the ring-theoretic methods of the last two sections.

We wish to thank D. K. Harrison for some discussion concerning this paper.

1. Hermitian forms over semi-local rings. Several authors have dealt with symmetric bilinear or hermitian forms over rings. For example, we cite [1], [5], [10], and [16]. In this section, which we have tried to make reasonably self contained, we develop the theory of hermitian forms as far as we need it. We have preferred giving proofs for some of the elementary initial results rather than just citing the literature since the latter is not always easily accessible.

Throughout this section all modules are assumed to be finitely generated. Let C be a ring (with identity) and J an involution of C, i.e. J is an anti-automorphism of C of period 2. If C is commutative we allow the possibility that J is the identity. For c in C we shall often write $\bar{c}$ for $J(c)$.

We define a space over (C,J) to be a pair (M,Φ) where M is a projective left C-module and $\Phi: M \times M \to C$ is a hermitian form; i.e. Φ is biadditive, $\Phi(cx,y) = c\Phi(x,y)$, and $\Phi(y,x) = \overline{\Phi(x,y)}$. Thus our spaces are special cases of the sesquilinear forms defined in [5]. Moreover, if C is comutative and J is the identity we get the spaces of [16].

If (M,Φ) is a space over (C,J) we let M^* be the set $\mathrm{Hom}_C(M,C)$ made into a left C-module via $(cf)(x) = f(x)\bar{c}$ for c in C, x in M, f in M^*. The form Φ induces a C-linear map $d_\Phi: M \to M^*$ via $d_\Phi: x \mapsto \Phi(\ ,x)$. We say Φ (or the space (M,Φ)) is non degenerate if d_Φ is bijective.

A space (M,Φ) is called a *free space* if M is a free C-module. If $B = \{x_1, \cdots, x_n\}$ is a basis for M then (M,Φ) is non degenerate if and only if the matrix $(\Phi(x_i,x_j))$ of Φ with regard to B is invertible [5, Prop. 3, p. 44].

By a *subspace* of a space (M,Φ) we mean a direct summand of M endowed with the restriction of Φ. If N is a subspace of M we set $N^\perp = \{x \in M \mid \Phi(x,N) = 0\}$. We write $M = N_1 \perp N_2$ to mean that M is the direct sum of the subspaces N_1, N_2 with $\Phi(x,y) = 0$ for all x in N_1, y in N_2. In this case we say M is the *orthogonal sum* of N_1 and N_2. A basis

$B = \{x_1, \cdots, x_n\}$ of a free space (M, Φ) is called an *orthogonal basis* if $M = Cx_1 \perp \cdots \perp Cx_n$. Note that if $x_1, \cdots, x_n$ form an orthogonal basis for a non degenrate space M then all the $\Phi(x_i, x_i)$ are units in C.

By modifying the proofs of [1, Lemmas 1.2 and 1.3, pp. 136-137] or [16, Satz 1.3.1, p. 102] one can prove the following

LEMMA 1.1. *Let (M, Φ) be a non degenerate space and N a subspace of M. Then $N^\perp$ is a subspace of M and $N = N^{\perp\perp}$. If N is non degenerate then $N^\perp$ is non degenerate and $M = N \perp N^\perp$.*

If (U, Φ) is a space over (C, J) we set $M(U) = (U \oplus U^*, \Psi)$ where Ψ is the hermitian form defined by $\Psi(u+f, v+g) = \Phi(u, v) + g(u) + \overline{f(v)}$ for $u, v \in U$ and $f, g \in U^*$. A space isometric to some $M(U)$ will be called *metabolic* (*cf.* [16], § 3). It is easy to see that metabolic spaces are non degenerate.

LEMMA 1.2. (cf. [16, Satz 3.2.1, p. 106]). *A non degenerate space (M, Φ) is metabolic if and only if M has a subspace V such that $V^\perp = V$.*

Proof. If $(M, \Phi) = M(U)$ take $V = U^*$. Conversely, if $M = U \oplus V$ is non degenerate and $V = V^\perp$ then one readily checks that $v \mapsto d_\Phi(v)\,|_U$ defines an isomorphism $V \to U^*$ and that $(U \oplus V, \Phi) \to M(U)$ via $u + v \mapsto u + d_\Phi(v)\,|_U$ is an isometry.

If Φ is the zero form on U we write $H(U)$ instead of $M(U)$ and we call a space *hyperbolic* if it is isometric to some $H(U)$. For a space (M, Φ) we often write M, and we write $-M$ to mean $(M, -\Phi)$.

LEMMA 1.3. *Let (U, Φ) be a space over (C, J). Then*

(i) $M(U) \perp M(-U) \cong H(U) \perp M(-U)$ (cf. [16, Satz 3.4.1, p. 107]).

(ii) *If U is non degenerate then* $U \perp (-U) \cong M(U)$ (cf. [16, 3.1.4, p. 106]).

(iii) *If the module U is the direct sum of two subspaces U_1, U_2 then* $M(U) \cong M(U_1) \perp M(U_2)$. (cf. [16, Satz 3.1.1, p. 105].)

Proof. (i) Let $W = \{u \perp (u+f) \mid u \in U, f \in U^*\} \subset M(U) \perp M(-U)$. Then $H(U) \to W$ via $u + f \to u \perp (u+f)$ is an isometry. Moreover, a straightforward calculation shows that $W^\perp = \{(u+f) \perp (-f - d_\Phi(u)) \mid u \in U, f \in U^*\}$ and $W \perp W^\perp = M(U) \perp M(-U)$. Finally, $M(U) \to W^\perp$ via $u + f \mapsto (u+f) \perp (-f - d_\Phi(u))$ is an isometry so we get $M(U) \perp M(-U)$

$= W \perp W^{\perp} \cong H(U) \perp M(U)$. To finish the proof of (i) notice that $H(U) \cong H(-U)$ and set $V = -U$.

(ii). Since U is non degenerate, $d_\Phi : U \to U^*$ is an isomorphism, so every element x of $M(U)$ can be written uniquely as $x = u + d_\Phi(v)$. Then $M(U) \to U \perp (-U)$ via $u + d_\Phi(v) \mapsto (u+v) \perp v$ gives the desired isometry.

(iii) If $U = U_1 \oplus U_2$ then $M(U) = (U_1 \oplus U_2 \oplus U_1^* \oplus U_2^*, \Psi)$ where

$$\Psi(u_1 + u_2 + f_1 + f_2, v_1 + v_2 + g_1 + g_2) = \Phi(u_1 + u_2, v_1 + v_2) + g_1(u_1) + g_2(u_2) + \overline{f_1(v_1)} + \overline{f_2(v_2)}.$$

Define $\phi : U_2 \to U_1^*$ by $\phi(u_2)(u_1) = \Phi(u_1, u_2)$. Then one easily checks that the mapping $M(U_1) \perp M(U_2) \to M(U)$ via

$$(u_1 + f_1) \perp (u_2 + f_2) \mapsto u_1 + u_2 + (f_1 - \phi(u_2)) + f_2$$

is an isometry.

Under the operation of $\perp$ the isometry classes of non degenerate spaces form a semi-group which we denote by $S(C,J)$. We denote the subsemi-group of isometry classes of metabolic spaces by $M(C,J)$. We shall denote the associated Grothendieck groups of these semi-groups by $K(C,J)$ and $KM(C,J)$, respectively [1, p. 9]. We recall that the elements of $K(C,J)$ can be written as $[M] - [N]$ where $[M]$ denotes the image of the isometry class of the space (M, Φ) and that $[M] = [N]$ if and only if there exists a non degenerate space M' with $M \perp M' \cong N \perp M'$ [1, Prop. 1.1, p. 10].

Now, if $[M(U)] - [M(V)] = 0$ in $K(C,J)$ then there is a space W with $M(U) \perp W \cong M(V) \perp W$. Hence by Lemma 1.3(ii)

$$M(U) \perp M(W) \cong M(U) \perp W \perp -W \cong M(V) \perp W \perp -W \cong M(V) \perp M(W)$$

so $[M(U)] - [M(V)] = 0$ in $KM(C,J)$ also. Thus the natural map $KM(C,J) \to K(C,J)$ is injective and we shall henceforth identify $KM(C,J)$ with its image in $K(C,J)$. Moreover, for any space U, $[M(U)] = [H(U)]$ by Lemma 1.3(i) so $KM(C,J)$ is generated by the hyperbolic spaces. We shall call the quotient group $K(C,J)/KM(C,J)$ the *Witt group* of (C,J) and denote it by $W(C,J)$.

We call two non degenerate spaces E, F over (C,J) *equivalent*, and write $E \sim F$, if there exist metabolic spaces M, N such that $E \perp M \cong F \perp N$. The quotient $S(C,J)/\sim$ by this equivalence relation is a group, since by Lemma 1.3(ii) we have $E \perp (-E) \sim 0$ for any non degenerate space E. Evidently the natural map $S(C,J) \to W(C,J)$ factors through our equivalence relation.

LEMMA 1.4. *The natural homomorphism from $S(C,J)/\sim$ to $W(C,J)$ is an isomorphism.*

Proof. It is surjective, since elements $-[E]$ and $[-E]$ of $K(C,J)$ have the same image in $W(C,J)$. By its universal property, $K(C,J)$ admits a canonical homomorphism $K(C,J) \to S(C,J)/\sim$ which necessarily vanishes on $KM(C,J)$. We thus get a map $W(C,J) \to S(C,J)/\sim$ which is a left inverse to $S(C,J)/\sim \to W(C,J)$, and hence the maps are inverse isomorphisms.

From now on, we shall assume that C is a commutative ring. If (E_1,Φ_1) and (E_2,Φ_2) are two spaces over (C,J) we define their tensor product to be the space $(E_1 \otimes_C E_2, \Phi)$ where $\Phi(x_1 \otimes x_2, y_1 \otimes y_2) = \Phi_1(x_1,y_1)\Phi_2(x_2,y_2)$ [5, p. 29]. Identifying $E_1^* \otimes E_2^*$ with $(E_1 \otimes E_2)^*$ [4, Prop. 4, p. 113] we have $d_{\Phi_1} \otimes d_{\Phi_2} = d_\Phi$ [5, p. 29]. Hence $E_1 \otimes E_2$ is non degenerate if both E_1 and E_2 are. Thus the tensor product makes $K(C,J)$ into a commutative ring with identity element given by the class of the space $(1) = (C,\Phi)$ where $\Phi(c_1,c_2) = c_1\bar{c}_2$.

LEMMA 1.5. (cf. [16, Satz 3.1.3, p. 106]). *Let (E,Φ_E) and (U,Φ_U) be spaces over (C,J) with E non degenerate. Then $E \otimes M(U) \cong M(E \otimes U)$.*

Proof. The subspace $V = E \otimes U^*$ of $E \otimes M(U) = E \otimes U \oplus E \otimes U^*$ fulfills the condition $V = V^\perp$ of Lemma 1.2 so $E \otimes M(U)$ is metabolic. By the proof of Lemma 1.2 we have $E \otimes M(U) \cong M(E \otimes U)$.

COROLLARY 1.6. *$KM(C,J)$ is an ideal in $K(C,J)$ and hence $W(C,J)$ is a commutative ring.*

Example 1.7. Let A be a commutative ring, $C = A \times A$ with coordinatewise operations, and J the involution $(a_1,a_2) \mapsto (a_2,a_1)$ on C. Let (M,Φ) be any non degenerate space over (C,J). Then $M = e_1M \oplus e_2M$ where $e_1 = (1,0)$, $e_2 = (0,1)$. (So e_iM is a projective A-module, $i = 1,2$.) Moreover, $\Phi(e_1M, e_1M) = \Phi(e_2M, e_2M) = 0$. Define

$$d\colon e_2M \to (e_1M)^* = \mathrm{Hom}_A(e_1M, A)$$

by $d(e_2y)(e_1x) = \Phi(e_1x, e_2y) = e_1\Phi(x,y)$. Then the non degeneracy of Φ implies that d is an isomorphism and hence induces an isomorphism of C-modules $T\colon M \to (e_1M) \times (e_1M)^*$ via $e_1x + e_2y \mapsto (e_1x, d(e_2y))$ where $C = A \times A$ acts on $e_1M \times (e_1M)^*$ coordinatewise. Now there is a natural hermitian form on $e_1M \times (e_1M)^*$, namely $\Psi((x,f),(y,g)) = (g(x),f(y))$, and T is an isometry with respect to the forms Φ, Ψ. Hence up to isometry every non degenerate space over (C,J) has the form $(U \times U^*, \Psi)$ where U

is a projective A-module, $U^* = \mathrm{Hom}_A(U, A)$, $C = A \times A$ acts coordinate-wise, and $\Psi((u,f),(v,g)) = (g(u), f(v))$. In particular, if (M,Φ) is any non degenerate space over (C,J) then M is isometric to $H(e_1 M)$ so $W(C,J) = 0$. Also, from the above we get an isomorphism from the semi-ring $P(A)$ of isomorphism classes of projective A-modules onto $S(C,J)$ which in turn induces an isomorphism $KP(A) \cong K(C,J)$, where $KP(A)$ is the Grothendieck ring of $P(A)$.

A *morphism* $\phi\colon (C,J) \to (C',J')$ *of pairs* is a ring homomorphism $\phi\colon C \to C'$ with $J' \circ \phi = \phi \circ J$. For any such ϕ and any space (E,Φ) over (C,J) we get a space $(C' \otimes_C E, \Phi')$ over (C',J') where the tensor product is taken via ϕ and $\Phi'(c' \otimes x, d' \otimes y) = c'\phi(\Phi(x,y))J'(d')$ for x, y in E and c', d' in C' [5, Prop. 2, p. 15]. Since there is a canonical isomorphism $C' \otimes_C E^* \cong (C' \otimes_C E)^*$ [4, Prop. 4, p. 113], it is readily verified that $(C' \otimes E, \Phi')$ is non degenerate (metabolic) if (E,Φ) is. Hence the assignment $(E,\Phi) \mapsto (C' \otimes_C E, \Phi')$ induces canonical ring homomorphisms $K(\phi)\colon K(C,J) \to K(C',J')$ and $W(\phi)\colon W(C,J) \to W(C',J')$.

Given a pair (C,J) the ring of J-invariant elements will be denoted by A. Then for all c in C, $c^2 - (c + \bar{c})c + c\bar{c} = 0$ with $c + \bar{c}$, $c\bar{c}$ in A so C is an integral ring extension of A. We call $c\bar{c}$ the *norm* of c and write $N(c) = c\bar{c}$. If (M,Φ) is a space over (C,J) and x is an element of M we will often write $n(x) = \Phi(x,x)$. Note that for all x in M, $n(x)$ is an element of A.

We say (C,J) is *connected* if C has no factorization $C = C_1 \times C_2$ such that $J = J_1 \times J_2$ with J_i an involution of C_i, $\mathrm{i} = 1, 2$.

LEMMA 1.8. *If (C,J) is connected then the fixed ring A has no non trivial idempotent and either C has no non trivial idempotent or $(C,J) \cong (A \times A, J')$ where $J'\colon (a_1,a_2) \mapsto (a_2,a_1)$.*

Proof. It is clear that A can have no non trivial idempotent. If $e \neq 0$, 1 is an idempotent then $eJ(e) \neq 1$ is an idempotent of A and therefore $eJ(e) = 0$. Thus $e + J(e) \neq 0$ is an idempotent of A and hence $e + J(e) = 1$. Therefore $C = Ce \oplus CJ(e)$. Define a ring homomorphism $\phi\colon A \times A \to C$ by $\phi(a_1,a_2) = a_1 e + a_2 J(e)$. Then it is easily checked that ϕ is an isomorphism and that if J' is the involution on $A \times A$ defined by $J'\colon (a_1,a_2) \mapsto (a_2,a_1)$ then $J \circ \phi = \phi \circ J'$.

For the remainder of this section, unless otherwise specified, we assume that C is a semi-local ring, i. e. that C has only finitely many maximal ideals.

LEMMA 1.9. *(C,J) admits a factorization*

$$(C, J) = (C_1, J_1) \times \cdots \times (C_t, J_t)$$

where (C_i, J_i) *is connected. The factorization induces an isomorphism of semi-rings*

$$S(C, J) \cong \prod_{i=1}^{t} S(C_i, J_i)$$

which in turn gives isomorphisms

$$K(C, J) \cong \prod_{i=1}^{t} K(C_i, J_i)$$

and

$$W(C, J) \cong \prod_{i=1}^{t} W(C_i, J_i).$$

Proof. Since C has only a finite number, s, of maximal ideals any factorization

$$(*) \qquad (C, J) = (C_1, J_1) \times \cdots \times (C_t, J_t)$$

must have length $t \leqq s$. Hence there certainly exists a factorization (*) which cannot be further refined and all the (C_i, J_i) in such a factorization must be connected and semi-local. Let e_i be the identity of C_i. Then if (M, Φ) is a space over (C, J) we can write

$$M = \coprod_{i=1}^{t} e_i M.$$

Let $\Phi_i = \Phi|_{e_i M}$. Then since $\Phi(e_i x, e_j y) = \delta_{ij} e_i \Phi(x, y) \in \delta_{ij} C_i$, it follows that $(e_i M, \Phi_i)$ is a space over (C_i, J_i). Moreover, (M, Φ) is non degenerate (metabolic) if and only if all the (Me_i, Φ_i) are. Thus

$$S(C, J) \cong \prod_{i=1}^{t} S(C_i, J_i)$$

and

$$KM(C, J) \cong \prod_{i=1}^{t} KM(C_i, J_i).$$

These isomorphisms together with the universal property of Grothendieck groups give isomorphisms

$$K(C, J) \cong \prod_{i=1}^{t} K(C_i, J_i)$$

and

$$W(C, J) \cong \prod_{i=1}^{t} W(C_i, J_i).$$

LEMMA 1.10. *If (C,J) is connected then every non degenerate space over (C,J) is free.*

Proof. If C has no non trivial idempotent then every projective C-module is free [6, Prop. 5, p. 143]. Hence by Lemma 1.8 we may assume that $C = A \times A$ with involution $(a_1, a_2) \mapsto (a_2, a_1)$. By Example 1.7, if (M,Φ) is a non degenerate space over (C,J) then $M \cong U \times U^*$ where U is a projective A-module and $U^* = \mathrm{Hom}_A(U,A)$. Since A has no non trivial idempotent, U is free over A [6, Prop. 5, p. 143] and $\mathrm{rank}\, U = \mathrm{rank}\, U^*$. Therefore $M \cong U \times U^*$ is a free $A \times A$-module.

LEMMA 1.11. *Let C be an arbitrary commutative ring with involution J and let (E,Φ) be a non degenerate space over (C,J) and let $\mathrm{Rad}\, C$ be the Jacobson radical of C. Denote both the natural maps $E \to E/(\mathrm{Rad}\, C)E$ and $C \to C/\mathrm{Rad}\, C$ by π. Then $\pi(E)$ carries a form Φ defined by*

$$\tilde{\Phi}(\pi(x),\pi(y)) = \pi(\Phi(x,y)).$$

If $(\pi(E),\tilde{\Phi})$ has an orthogonal basis $y_1,\cdots,y_n$ then there exists an orthogonal basis $x_1,\cdots,x_n$ of (E,Φ) with $\pi(x_i) = y_i$, $i = 1,\cdots,n$.

Proof. Since $(\pi(E),\tilde{\Phi})$ is the space deduced from (E,Φ) by the morphism $(C,J) \to (\pi(C),\tilde{J})$ of pairs it is also non degenerate. Let x_1 be any element of E with $\pi(x_1) = y_1$. Then $n(x_1) = \Phi(x_1,x_1)$ is mapped onto the unit $\tilde{\Phi}(y_1,y_1)$ by π and therefore is itself a unit. Hence each x in E can be written

$$x = x - \frac{\Phi(x,x_1)}{n(x_1)}x_1 + \frac{\Phi(x,x_1)}{n(x_1)}x_1$$

so that $E = Cx_1 \perp (Cx_1)^\perp$. Applying π to this decomposition we find $\pi(E) = \pi(C)y_1 \perp \pi((Cx_1)^\perp)$ so that $\pi((Cx_1)^\perp) = \pi(C)y_2 \perp \cdots \perp \pi(C)y_n$. Since $(Cx_1)^\perp$ is non degenerate by Lemma 1.1, inductions finishes the proof.

A non degenerate space (E,Φ) over (C,J) is called *proper* if the ideal of A generated by the elements $n(x)$, x in E, is all of A.

LEMMA 1.12. (cf. [16, Lemma 5.4.1, p. 111]). *Every proper free space over (C,J) has an orthogonal basis.*

Proof. In view of Lemma 1.11 it is enough to prove this in the case when $\mathrm{Rad}\, R = 0$. Then by Lemma 1.9, $(C,J) = \prod_{i=1}^{t}(C_i,J_i)$ where for $i = 1,\cdots,m$, C_i is a field with involution J_i and for $i = m+1,\cdots,t$,

$C_i = A_i \times A_i$ with A_i a field and $J_i(a,b) = (b,a)$. Let (E,Φ) be a proper free space over (C,F). Then, as in the proof of Lemma 1.9,

$$(E,\Phi) = \coprod_{i=1}^{m} (E_i,\Phi_i)$$

where (E_i,Φ_i) is a non degenerate space over (C_i,J_i). Moreover, since (E,Φ) is proper each (E_i,Φ_i) must be proper. In particular, for $i=1,\cdots,m$, Φ_i is not alternating on E_i. Hence (E_i,Φ_i) has an orthogonal basis for $i=1,\cdots,m$ [5, Th. 1, p. 90]. Now for any i with $m+1 \leqq i \leqq t$, Example 1.7 states that (E_i,Φ_i) has the form $(U \times U^*,\Psi)$ with U a vector space over A_i and $\Psi((u,f),(v,g)) = (g(u),f(v))$. Let $u_1,\cdots,u_n$ be any basis for U and $u_1^*,\cdots,u_n^*$ the dual basis for U^*. Then for $j \neq k$,

$$\Psi((u_j,u_j^*),(u_k,u_k^*)) = (u_k^*(u_j),u_j^*(u_k)) = 0$$

so that $\{(u_j,u_j^*)\}$ is an orthogonal basis for (E_i,Φ_i). Combining all these bases then gives an orthogonal basis for (E,Φ).

Our next step is to generalize [31, Satz 7] to the case of hermitian forms over semi-local rings. Let B, B' be two orthogonal bases of a free space E. We say that B and B' are *n-connectable* if there exists a finite sequence $B_1,\cdots,B_k$ of orthogonal bases of E with $B = B_1$, $B' = B_k$, and B_i differing from B_{i+1} in at most n places.

LEMMA 1.13. *Let C be an arbitrary commutative ring with involution J and let (E,Φ) be a free space over (C,J) with orthogonal bases $B = \{y_1,\cdots,y_m\}$ and $B' = \{y_1',\cdots,y_m'\}$. If $\pi(y_i) = \pi(y_i')$, $i=1,\cdots,m$, where $\pi: E \to E/(\operatorname{Rad} C)E$ is the natural map, then B is 2-connectable to B'.*

Proof. Using induction on m, it is sufficient to show that B is 2-connectable to an orthogonal basis $\{y_1',z_2,\cdots,z_m\}$ with $\pi(y_i) = \pi(z_i)$, $i=2,\cdots,m$, since then $\{z_2,\cdots,z_m\}$ and $\{y_2',\cdots,y_m'\}$ are both orthogonal bases of $(Cy_1')^{\perp}$.

By renumbering, if necessary, we have $y_1' = (1+r_1)y_1 + \sum_{i=2}^{t} r_i y_i$ with r_i in $\operatorname{Rad} C$ and $r_i \neq 0$ for $2 \leqq i \leqq t$. We now proceed by induction on t. If $y_1' = (1+r_1)y_1$, then since $1+r_1$ is a unit in C, $\{y_1',y_2,\cdots,y_m\}$ is an orthogonal basis of E which is 1-connectable to B, so that the lemma is proved in this case.

If $t \geqq 2$, let $y_1'' = (1+r_1)y_1 + r_t y_t$. Then $n(y_1'')$ is congruent to $n(y_1)$ modulo $\operatorname{Rad} C$ and hence is a unit of C. Therefore $Cy_1 \perp Cy_t = Cy_1'' \perp Cy_t''$

where $y_t'' = y_t - \dfrac{\Phi(y_t, y_1'')}{n(y_1'')} y_1''$. Now the orthogonal basis

$$B'' = \{y_1'', y_2, \cdots, y_{t-1}, y_t'', \cdots, y_m\}$$

is clearly 2-connectable to B, also $\pi(B) = \pi(B'')$, and, in terms of B'', we have $y_1' = y_1'' + \sum_{i=2}^{t-1} r_i y_i'$. Thus the proof is complete by induction on t.

LEMMA 1.14. *Assume (C, J) is connected and* $\operatorname{Rad} C = 0$. *Let (E, Φ) be a non degenerate space with orthogonal basis $B = \{x_1, \cdots, x_m\}$ and let* $y = \sum_{i=1}^{t} c_i x_i$, *with all $c_i \neq 0$, be an element of E that can be augmented to an orthogonal basis of E.*

(i) *If the pair (C, A) is not $(\boldsymbol{F}_4, \boldsymbol{F}_3)$*[3] *or $(\boldsymbol{F}_2, \boldsymbol{F}_2)$ there there is an orthogonal basis $\{y, z_2, \cdots, z_m\}$ which is 2-connectable to B.*

(ii) *If $C = \boldsymbol{F}_4$ and $A = \boldsymbol{F}_2$ then there is an orthogonal basis $\{y, z_2, \cdots, z_m\}$ which is 3-connectable to B.*

(iii) *If $C = \boldsymbol{F}_2$ there is an orthogonal basis $\{y, z_2, \cdots, z_m\}$ which is 4-connectable to B.*

Proof. Since $\operatorname{Rad} C = 0$, Lemma 1.8 shows that C is either a field or $C = A \times A$ with A a field and $J(a_1, a_2) = (a_2, a_1)$. In either case, A is a field so the assertion that an element of A is a unit is equivalent to the assertion that it is not zero.

The proof proceeds by induction on t. The case $t = 1$ is handled exactly as in Lemma 1.13. Now suppose $t > 1$ and that there exist integers i, j $1 \leqq i < j \leqq t$ with $n(c_i x_i + c_j x_j) \neq 0$. Then by the last part of Lemma 1.1 we can augment $x_i' = c_i x_i + c_j x_j$ by an element x_j' of E to yield an orthogonal basis of $Cx_i \perp Cx_j$. Then the orthogonal basis $B_1 = \{x_1, \cdots, x_i', \cdots, x_j', \cdots, x_m\}$ is 2-connectable to B and since y is a linear combination of $t-1$ elements of B_1, the induction hypothesis finishes the proof in this case.

We therefore assume that $n(c_i x_i + c_j x_j) = 0$ for all i, j with $1 \leqq i < j \leqq t$. Set $\alpha = n(y)$ and $\beta_i = N(c_i) n(x_i)$, $i = 1, \cdots, t$. Then, in the field A we have $\beta_i + \beta_j = 0$ for $i \neq j$ and $\sum_{i=1}^{t} \beta_i = \alpha \neq 0$. Hence t is odd and $\alpha = \beta_i$ for $1 \leqq i \leqq t$. Thus, for $i \neq j$, $2\alpha = \beta_i + \beta_j = 0$ so A has characteristic two. Moreover, since $N(c_i) n(x_i) = \beta_i \neq 0$ for all i, each c_i must be a unit in C. Hence making the series of changes

[3] By $\boldsymbol{F}_q$ we denote a field with q elements.

$$\{x_1, \cdots, x_m\} \to \{c_1x_1, x_2, \cdots, x_m\} \to \{c_1x_1, c_2x_2, \cdots, x_m\}$$
$$\to \cdots \to \{c_1x_1, c_2x_2, \cdots, c_tx_t, \cdots, x_m\}$$

we see that we may suppose $y = \sum_{i=1}^{t} x_i$ with $t \geqq 3$ odd, $n(x_i) = n(y) = \alpha \neq 0$ for all i, and A is a field of characteristic two. The remainder of the proof proceeds in a number of steps.

1) J is not the identity and there exists c in C with $N(c) \neq 1$ and $c + \bar{c} \neq 0$.

In this case set $x_1' = x_1 + cx_2$. Then $n(x_1') = \alpha(1 + N(c)) \neq 0$ and it is easily verified that x_1' and $x_2' = \bar{c}x_1 + x_2$ form an orthogonal basis for $Cx_1 \perp Cx_2$. Thus $B_1 = \{x_1', x_2', x_3, \cdots, x_m\}$ is 2-connected to B and in terms of B_1, $y = \frac{(1+\bar{c})}{1+N(c)} x_1' + \frac{(1+c)}{1+N(c)} x_2' + x_3 + \cdots + x_t$. Next, let $x_1'' = \frac{(1+\bar{c})}{1+N(c)} x_1' + x_3$. A routine calculation then shows that

$$n(x_1'') = \frac{\alpha(c+\bar{c})}{1+N(c)} \neq 0,$$

since $c + \bar{c} \neq 0$. Hence there is an element x_3'' of E so that $\{x_1'', x_3''\}$ is an orthogonal basis of $Cx_1' \perp Cx_3$. Then $B_2 = \{x_1'', x_2', x_3'', x_4, \cdots, x_m\}$ is 2-connectable to B, and since in terms of B_2, y is a linear combination of $t-1$ elements, the proof is finished in this case.

If $C = A \times A$ with $J(a, b) = (b, a)$ we set $c = (1, 0)$ to fulfill the hypotheses of case 1). Henceforth, therefore, we assume that C is a field.

2) C is a field and J is not the identity on C.

If c is not in A then $c + \bar{c} \neq 0$. Therefore if there is a $c \notin A$ with $N(c) \neq 1$ we are done by case 1). Hence assume $N(c) = 1$ for all $c \notin A$. Then if $a \neq 0$ is in A and $c \notin A$ we have

$$1 = N(c + a) = N(c) + (c + \bar{c})a + a^2 = 1 + (c + \bar{c})a + a^2.$$

This yields $c + \bar{c} = a$ for every $a \neq 0$ in A. Thus we are reduced to the subcase

2) (a) $A = \boldsymbol{F}_2$ and $C = \boldsymbol{F}_4$.

Here $C = A(\theta)$ with $\theta^2 + \theta + 1 = 0$. Since $t \geqq 3$ we may define elements $x_1' = x_1 + x_2 + x_3$, $x_2' = x_1 + \theta x_2 + \bar{\theta} x_3$, $x_3' = x_1 + \bar{\theta} x_2 + \theta x_3$. Then a routine calculation shows that $\{x_1', x_2', x_3'\}$ is an orthogonal basis for $Cx_1 \perp Cx_2 \perp Cx_3$. Now B is 3-connectable to $B_1 = \{x_1', x_2', x_3', x_4, \cdots, x_m\}$, and in terms of B_1, y is a sum of $t-2$ terms so again induction completes the proof.

3) C is a field and J is the identity on C.

We first prove that $t < m = \operatorname{rank} E$. Since y can be augmented to an orthogonal basis of E, there is an element z in E with $n(z) \neq 0$ and $\Phi(y, z) = 0$. Let $z = \sum_{i=1}^{m} d_i x_i$. Then $\Phi(y, z) = (\sum_{i=1}^{t} d_i)\alpha$. Since the characteristic of C is two, $0 = (\Phi(y, z))^2 = (\sum_{i=1}^{t} d_i^2\alpha)\alpha$ so that $\sum_{i=1}^{t} d_i^2\alpha = 0$. Now, if $t = m$ then $0 \neq \Phi(z, z) = \sum_{i=1}^{t} d_i^2\alpha$, a contradiction. (cf. [16, p. 113].)

3) (a) $C \neq \boldsymbol{F}_2$ and J is the identity.

Let $\alpha_m = n(x_m) \neq 0$. If $\alpha + c^2\alpha_m = 0$ for all $c \neq 0$ in C then $C - 0$ has only one element and hence $C = \boldsymbol{F}_2$. Thus there is an element c in C with $\alpha + c^2\alpha_m \neq 0$. Now set

$$x_1' = \frac{\alpha}{\alpha + c^2\alpha_m} x_1 + \frac{c\alpha}{\alpha + c^2\alpha_m} x_m \quad \text{and} \quad x_m' = \frac{c^2\alpha_m}{\alpha + c^2\alpha_m} x_1 + \frac{c\alpha}{\alpha + c^2\alpha_m} x_m.$$

Then it is easy to check that $\{x_1', x_m'\}$ is an orthogonal basis for $Cx_1 \perp Cx_2$, $x_1 = x_1' + x_m'$, and $n(x_m') = \dfrac{c^2\alpha\alpha_m}{\alpha + c^2\alpha_m} \neq \alpha$. The basis $B_1 = \{x_1', x_2', \cdots, x_m'\}$ is 2-connectable to B and in terms of B_1, $y = x_1' + x_2 + \cdots + x_t + x_m'$ which is a longer expression but has $n(x_m') \neq \alpha$. Hence $n(x_2 + x_m') \neq 0$ and therefore if $x_2'' = x_2 + x_m'$, there is an element x_m'' such that $\{x_2'', x_m''\}$ is an orthogonal basis for $Cx_2 \perp Cx_m'$. Our basis B_1 is 2-connectable to the basis $B_2 = \{x_1', x_2'', x_3, \cdots, x_{m-1}, x_m''\}$ and we have $y = x_1' + x_2'' + \cdots + x_t$. Now $n(x_2'' + x_3) = n(x_2 + x_m' + x_3) = n(x_m') \neq 0$. For $x_2''' = x_2'' + x_3$, there is an alement x_3''' such that $\{x_2''', x_3'''\}$ is an orthogonal basis of $Cx_2'' \perp Cx_3$. Now B_2 is 2-connectable to $B_3 = \{x_1', x_2''', x_3''', x_4, \cdots, x_{m-1}, x_m''\}$ and y is a linear combination of $t - 1$ elements of B_3, which completes the proof in this case.

3) (b) $C = \boldsymbol{F}_2$.

In this case we shall show that B is 4-connectable to an orthogonal basis of E containing y; so we suppose $m > 4$. Note that we still have $t < m$. Let $E' = Cx_1 \perp Cx_2 \perp Cx_3 \perp Cx_m$ and let $x' = x_1 + x_2 + x_3$. Since, in this case, $\alpha = 1$, we have $n(x') = 1$ and so by Lemma 1.1, $E' = Cx' \perp (Cx')^{\perp}$. Since x_m is in $(Cx')^{\perp}$ and $n(x_m)$ is a unit of C, the space $(Cx')^{\perp}$ is proper, and so, by Lemma 1.12, has an orthogonal basis $\{x_2', x_3', x_m'\}$. Then the orthogonal basis $B_1 = \{x', x_2', x_3', x_4, \cdots, x_{m-1}, x_m'\}$ is 4-connectable to B and $y = x' + x_4 + \cdots + x_t$ (or x' if $t = 3$) so that induction completes the proof.

THEOREM 1.15. (cf. [16, Lemma 5.5.3, p. 113], [31, Satz 7]). *Let C be a semi-local ring with involution J, (E, Φ) a proper free space over (C, J), and $B = \{x_1, \cdots, x_m\}$, $B' = \{y_1, \cdots, y_m\}$ two orthogonal bases of E.*

(i) *B and B' are 4-connectable.*

(ii) *If C has no maximal ideal $\mathfrak{m}$ with $J(\mathfrak{m}) = \mathfrak{m}$ and $C/\mathfrak{m} = \boldsymbol{F}_2$, then B and B' are 3-connectable.*

(iii) *If, in addition, C has no maximal ideal $\mathfrak{m}$ with $J(\mathfrak{m}) = \mathfrak{m}$ and $C/\mathfrak{m} = \boldsymbol{F}_4$, $A/A \cap \mathfrak{m} = \boldsymbol{F}_2$, then B and B' are 2-connectable.*

Proof. By renumbering the x's we may suppose $y_1 = \sum_{i=1}^{t} c_i x_i$ with $c_i \neq 0$. If $\operatorname{Rad} C = 0$ and (C, J) is connected, Lemma 1.14 shows that B is n-connected to an orthogonal basis $\{y_1, z_2, \cdots, z_m\}$. Here $n = 4$ if $C = \boldsymbol{F}_2$, $n = 3$ if $A = \boldsymbol{F}_2$ and $C = \boldsymbol{F}_4$, and $n = 2$ otherwise. Since $\{y_2, \cdots, y_m\}$ and $\{z_2, \cdots, z_m\}$ are orthogonal bases of the proper free space $(Cy_1)^\perp$ induction on m finishes the proof in this case.

Next, assume only $\operatorname{Rad} C = 0$. Then by Lemma 1.9,

$$(C, J) = (C_1, J_1) \times \cdots \times (C_k, J_k)$$

where (C_i, J_i) is connected and $\operatorname{Rad} C_i = 0$. Hence $E = E_1 \times \cdots \times E_k$ with E_i a proper free space over (C_i, J_i). Let e_i denote the indentity element of C_i. Then $\{e_i x_1, \cdots, e_i x_m\}$ and $\{e_i y_1, \cdots, e_i y_m\}$ are orthogonal bases of E_i. By Lemma 1.14 these bases are n-connectable with $n = 2$ or 3 or 4. By adding the connecting chains of bases, the theorem is then proved for the case $\operatorname{Rad} C = 0$.

Finally, let $\pi: E \to E/(\operatorname{Rad} C)E$ be the natural map. Then the orthogonal bases $\pi(B)$, $\pi(B')$ of $\pi(E)$ are n-connectable for $n = 2$ or 3 or 4. Let $\tilde{B}_i$ and $\tilde{B}_{i+1}$ be two adjacent bases for $\pi(E)$ occurring in the chain between $\pi(B)$ and $\pi(B')$, and let $\tilde{E}_0$ be the $C/\operatorname{Rad} C$-submodule of $\pi(E)$ generated by elements of B_i not in $\tilde{B}_{i+1}$. Thus $\tilde{E}_0$ has an orthogonal basis $\tilde{u}_h$, $h = 1, 2$, or $h = 1, 2, 3$, or $h = 1, 2, 3, 4$. Moreover, $\pi(E) = \tilde{E}_0 \perp \tilde{E}_1$ where $\tilde{E}_1$ has the orthogonal basis $\tilde{B}_i \cap \tilde{B}_{i+1} = \{\tilde{w}_j\}$. By Lemma 1.11, E has an orthogonal basis $B_i = \{u_h, w_j\}$ with $\pi(u_h) = \tilde{u}_h$ and $\pi(w_j) = \tilde{w}_j$. Now, the elements of $\tilde{B}_{i+1}$ not in $\tilde{B}_i$ must span $(\tilde{E}_1)^\perp = \tilde{E}_0$. Thus, let $\tilde{v}_h$, $h = 1, 2$; or $h = 1, 2, 3$; or $h = 1, 2, 3, 4$, be the basis of $\tilde{E}_0$ belonging to $\tilde{B}_{i+1}$. Again we can find an othogonal basis $B_{i+1} = \{v_h, w_j\}$ with $\pi(v_h) = \tilde{v}_h$ and $\pi(w_j) = \tilde{w}_j$. It thus follows that B is n-connectable, $n = 2$ or 3 or 4, to an orthogonal basis $B'' = \{y_1'', y_2'', \cdots, y_m''\}$ with $\pi(y_i'') = \pi(y_i)$. By Lemma 1.13, B'' is 2-connectable to B' so that B is n-connectable to B', $n = 2$ or 3 or 4.

It is clear from Lemma 1.14 that B and B' are 2-connectable unless $(C/\operatorname{Rad} C, \tilde{J})$ contains a direct summand $\boldsymbol{F}_2$ or a direct summand $\boldsymbol{F}_4$ with J not inducing the identity on it. In the latter case there is a maximal ideal $\mathfrak{m}$ of C with $J(\mathfrak{m}) = \mathfrak{m}$ and $C/\mathfrak{m} = \boldsymbol{F}_4$. If J induced the identity on $C/\mathfrak{m} = \boldsymbol{F}_4$ then it is clear that $\tilde{c}^2$ lies in $A/\mathfrak{m} \cap A$ for every element $\tilde{c}$ in $C/\mathfrak{m}$. Since $A/\mathfrak{m} \cap A$ is finite this would force $A/\mathfrak{m} \cap A = C/\mathfrak{m}$. Thus the hypothesis in (iii) implies that J does not induce the identity on $C/\mathfrak{m} = \boldsymbol{F}_4$ and Theorem 1.15 is completely proved.

Let A^* denote the group of units in in A and let $G = A^*/NC^*$ be the group of norm classes in A^*. For a in A^* we denote the image of a in G by $\{a\}$. Since $N(a) = a^2$ it is clear that G is an abelian group of exponent two. For a in A^* we let (a) be the proper rank one free space Cx with form $\Phi(c_1x, c_2x) = c_1\bar{c}_2a$. Note that $(a) \otimes (b) = (ab)$ and $(a) = (b)$ if and only if $\{a\} = \{b\}$ in G. Hence the assignment $\{a\} \mapsto [(a)]$ defines a ring homomorphism $\phi\colon \boldsymbol{Z}[G] \to K(C, J)$.

THEOREM 1.16 (cf. [9, p. 1366]; [16, Satz 5.5.1, p. 112]). *Let C be a semi-local ring with involution J. If the pair (C, J) is connected*[4] *then*

(i) *ϕ is surjective,*

(ii) $\operatorname{Ker}\phi$ *is additively generated by the elements* $\sum_{i=1}^{4} \{a_i\} - \sum_{i=1}^{4} \{b_i\}$ *with* $\perp_{i=1}^{4} (a_i) \cong \perp_{i=1}^{4} (b_i)$,

(iii) *If C has no maximal ideal $\mathfrak{m}$ with $J(\mathfrak{m}) = \mathfrak{m}$ such that either $C/\mathfrak{m} = \boldsymbol{F}_2$ or $C/\mathfrak{m} = \boldsymbol{F}_4$ and $A/\mathfrak{m} \cap A = \boldsymbol{F}_2$ then* $\operatorname{Ker}\phi$ *is additively generated by the elements $\{a_1\} + \{a_2\} - \{b_1\} - \{b_2\}$ with $(a_1) \perp (a_2) \cong (b_1) \perp (b_2)$.*

(iv) *If A is a field then* $\operatorname{Ker}\phi$ *is generated by the elements described in* (iii).

Proof. As before we let $[M]$ denote the image of the isometry class of a non degenerate space M in $K(C, J)$. Then for any a in A^*, $[M] = [M \perp (a)] - [(a)]$. Since both $M \perp (a)$ and (a) are proper this shows that $K(C, J)$ is generated by the images of proper spaces. Lemmas 1.10 and 1.12 apply to show that every proper space is isometric to $\perp_{i=1}^{n} (a_i)$ for a_i in A^*, so that ϕ is surjective.

Let $z = \sum_{i=1}^{s} \{a_i\} - \sum_{j=1}^{t} \{b_j\}$ lie in $\operatorname{Ker}\phi$. Then there exists a non degenerate

[4] K. J. Hertz and J. Cunningham have pointed out to us that this condition was omitted in [16] in the last statement of Lemma 5.4.1 and in some parts of § 5.5.

space N such that $\perp_{i=1}^{s}(a_i)\perp N \cong \perp_{j=1}^{t}(b_j)\perp N$. By adding (a), a in A^*, to both sides we may even assume that N is proper. Hence $N = \perp_{k=1}^{r}(c_k)$ and so $\perp_{i=1}^{s}(a_i)\perp\perp_{k=1}^{r}(c_k) \cong \perp_{j=1}^{t}(b_j)\perp\perp_{k=1}^{r}(c_k)$. In particular $s=t$, and we can suppose $z = \sum_{i=1}^{s}\{a_i\} - \sum_{i=1}^{s}\{b_j\}$ with $\perp_{i=1}^{s}(a_i) \cong \perp_{i=1}^{s}(b_i)$. Hence there exists a free space (E,Φ) with orthogonal bases $B=\{x_1,\cdots,x_s\}$, $B'=\{y_1,\cdots,y_s\}$ such that $n(x_i)=a_i$, $n(y_i)=b_i$. By Theorem 1.15, B is 4 $(3,2)$-connectable to B'. Let $B_1=B$, $B_2,\cdots,B_n=B'$ be a sequence of orthogonal bases effecting the connection, where $B_i=\{w_1^{(i)},\cdots,w_s^{(i)}\}$ and $n(w_j^{(i)})=d_j^{(i)}$. If we denote the element $\sum_{j=1}^{s}\{d_j^{(i)}\}$ of $\mathbf{Z}[G]$ by $\{B_i\}$ then

$$z = (\{B_1\}-\{B_2\})+(\{B_2\}-\{B_3\})+\cdots+(\{B_{n-1}\}-\{B_n\})$$

which proves (ii) and (iii).

Theorem 1.15 shows that the conclusion of (iv) holds with the possible exception of $A=\boldsymbol{F}_2$. In this case $G=\boldsymbol{F}_2{}^*=1$ so that $\mathbf{Z}[G]=\mathbf{Z}$. Since ϕ is surjective and $K(\boldsymbol{F}_2,\mathrm{Id})=\mathbf{Z}$ we have $\operatorname{Ker}\phi=0$ and Theorem 1.16 is proved.

COROLLARY 1.17. *Let (C,J) be as in Theorem* 1.16.

(i) *If C has no nontrivial idempotents the canonical surjection $\psi\colon \mathbf{Z}[G] \xrightarrow{\phi} K(C,J) \to W(C,J)$ has kernel generated by $\{1\}+\{-1\}$ and the elements indicated in* (ii) *or* (iii) *of Theorem* 1.16.

(ii) *If C has a nontrivial idempotent then $K(C,J)\cong\mathbf{Z}$ and $W(C,J)=0$.*

Proof. Let $\boldsymbol{H}$ denote the hyperbolic space built on the module C. If C has no non trivial idempotents all projective C-modules are free so by Lemma 1.3 (iii), $H(U)=\boldsymbol{H}\perp\boldsymbol{H}\perp\cdots\perp\boldsymbol{H}$ for all projective C-modules U. Now it is easily verified that $M((1))\cong(1)\perp(-1)$. Moreover, by Lemma 1.3 (i), $[M((1))]=[\boldsymbol{H}]$ in $K(C,J)$. Hence in $K(C,J)$, $[H(U]=n[\boldsymbol{H}]=n[(1)]+n[(-1)]$, for some natural number n. In particular, $\{1\}+\{-1\}$ is in $\operatorname{Ker}\psi$. Now suppose that $\psi(z)=0$. Then $\phi(z)$ is in $KM(C,J)$ and thus by Lemma 1.3 (i),

$$\phi(z) = [H(U)]-[H(V)] = m([(1)]+[(-1)])$$

for some integer m. Hence $\operatorname{Ker}\psi=\operatorname{Ker}\phi+\mathbf{Z}(\{1\}+\{-1\})$ which proves (i).

In the second case Lemma 1.8 shows that $(C,J) \cong (A \times A, J')$ where A is a connected semi-local ring and $J'(a,b) = (b,a)$. Example 1.7 together with the fact that projective A-modules are free finishes the proof.

Remark 1.18. In case (C,J) is not necessarily connected it can be shown that $\operatorname{Im}\phi$ is the Grothendieck ring $KF(C,J)$ of the semi-ring $SF(C,J)$ of isometry classes of *free* non degenerate spaces over (C,J). If $WF(C,J)$ is defined as $KF(C,J)/\mathbf{Z}[\boldsymbol{H}]$ and ψ is still the natural composite, it can be seen that $\operatorname{Ker}\phi$ and $\operatorname{Ker}\psi$ have the same descriptions as before.

In the cases (iii) and (iv) of Theorem 1.16 we can give a more explicit description of $\operatorname{Ker}\phi$.

LEMMA 1.19. *Suppose* $\operatorname{Ker}\phi$ *is additively generated by* $\{a_1\}+\{a_2\}-\{b_1\}-\{b_2\}$ *with* $(a_1)\perp(a_2) \cong (b_1)\perp(b_2)$. *Then as an ideal of* $\mathbf{Z}[G]$, $\operatorname{Ker}\phi$ *is generated by the elements*

$$q(a,c_1,c_2) = (1+\{a\})(1-\{N(c_1)+N(c_2)a\})$$

where (a,c_1,c_2) *runs through the triples in* $A^* \times C \times C$ *with* $N(c_1)+N(c_2)a$ *in* A^*. (cf. [16, 5.5.2, p. 112].)

Proof. By hypothesis, $\operatorname{Ker}\phi$ is generated as an ideal by elements $z = \{1\}+\{a\}-\{b\}-\{b'\}$ with $(1)\perp(a) \cong (b)\perp(b')$. Then there exist c_1, c_2 in C such that $b = N(c_1)+N(c_2)a$. Moreover, by [5, Prop. 1, p. 42], $\{a\} = \{bb'\}$ and hence $\{ab\} = \{b'\}$. Thus

$$z = (\{1\}+\{a\})(\{1\}-\{b\}) = q(a,c_1,c_2).$$

On the other hand, let (a,c_1,c_2) in $A^* \times C \times C$ be such that $b = N(c_1)+N(c_2)a$ is in A^*. Then one easily verifies that $(1)\perp(a) \cong (b)\perp(ab)$ and hence $q(a,c_1,c_2)$ lies in $\operatorname{Ker}\phi$.

Let χ be a character of G, i.e. a homomorphism from G into $\boldsymbol{C}^*$. Since G has exponent two we must have $\chi(g) = \pm 1$ for all g in G. Thus χ extends to a unique ring homomorpism $\psi_\chi\colon \mathbf{Z}[G] \to \mathbf{Z}$. The following lemma will be of importance in 3.

LEMMA 1.20. *Let* z *be an element of* $\mathbf{Z}[G]$ *of one of the following types:*

(a) $z = \sum_{i=1}^{r}\{a_i\} - \sum_{i=1}^{r}\{b_i\}$ *with* $\perp_{i=1}^{r}(a_i) \cong \perp_{i=1}^{r}(b_i)$ *and* $r \leqq 5$.

(b) $z = \{1\}+\{-1\}$.

Then, for any character χ *of* G, *we have* $\psi_\chi(z) = 0$ *or* $\pm 2^n$ *for some integer* $n \geqq 1$.

Proof. The conclusion is clear for case (b). Hence suppose z is as in (a). By [5, Prop. 1, p. 42], $\prod_{i=1}^{r}\{a_i\}=\prod_{i=1}^{r}\{b_i\}$ in G. Now fix χ and suppose s of the $\chi(\{a_i\})$ are -1 while $r-s$ of the $\chi(\{a_i\})$ are 1. Then $\sum_{i=1}^{r}\chi(\{a_i\})=r-2s$. Now $\prod_{i=1}^{r}\chi(\{a_i\})=1$ if and only if s is even, which is equivalent to $\sum_{i=1}^{r}\chi(\{a_i\})\equiv r \pmod 4$. Furthermore, $\prod_{i=1}^{r}\chi(\{a_i\})=-1$ if and only if s is odd, which is equivalent to $\sum_{i=1}^{r}\chi(\{a_i\})\equiv r-2 \pmod 4$. Thus it follows that in either case $\sum_{i=1}^{r}\chi(\{a_i\})\equiv\sum_{i=1}^{r}\chi(\{b_i\}) \pmod 4$. Hence $\psi_\chi(z)\equiv 0 \pmod 4$. But $r\leqq 5$ implies that $\psi_\chi(z)$ is an integer of absolute value $\leqq 10$. Hence $\psi_\chi(z)=0$ or ± 4 or ± 8.

COROLLARY 1.21. *Let (C,J) be a connected semi-local ring and let $R=K(C,J)$ or $W(C,J)$. Then $R\cong \boldsymbol{Z}[G]/K$ where G is an abelian group of exponent two and K is an ideal of $\boldsymbol{Z}[G]$ such that for all characters χ of G we have $\psi_\chi(K)=0$ or $2^n\boldsymbol{Z}$.*

2. Integral extensions of $\boldsymbol{Z}$ with nil torsion group. The results of 1. show that for a connected semi-local ring C with involution the commutative rings $K(C,J)$ and $W(C,J)$ are residue class rings of $\boldsymbol{Z}[G]$ where G is an abelian 2-group. This is the motivation for studying residue class rings of $\boldsymbol{Z}[G]$ for G an abelian torsion group.

Now, $\boldsymbol{Z}[G]$ is an integral extension of $\boldsymbol{Z}$ since $g^{n(g)}=1$ for all g in G, so that every element of $\boldsymbol{Z}[G]$ is a sum of integral elements [7, Cor. 2, p. 14]. Hence all residue class rings of $\boldsymbol{Z}[G]$ are also integral extensions of the image of $\boldsymbol{Z}$ they contain.

We shall use the following notations consistently throughout the remainder of the paper:

R is a commutative ring.

$\operatorname{Rad} R$ denotes the radical of R; $\operatorname{Rad} R=\cap M$ where M runs through the maximal ideals of R.

$\operatorname{Nil} R$ denotes the set of nilpotent elements of R; $\operatorname{Nil} R=\cap P$ where P runs through either the minimal prime ideals of R or all prime ideals of R [6, Prop. 13, p. 95].

R_t denotes the torsion subgroup of the additive group of R; R_t is an ideal of R.

$R_{red} = R/\mathrm{Nil}\, R$.

$\dim R =$ the Krull dimension of R [15, p. 28].

$\mathrm{Spec}\, R =$ the set of prime ideals of R topoligized by the Zariski topology [6, p. 125].

$\mathrm{Max}\, R$ and $\mathrm{Min}\, R$ denotes the subspaces of $\mathrm{Spec}\, R$ consisting of the maximal ideals and minimal prime ideals respectively.

The unadorned $\otimes$ sign will always mean $\otimes$ over $\mathbf{Z}$.

We begin by studying commutative rings for which $R_t \subset \mathrm{Nil}\, R$ since, as we shall see in 3., this is the case for certain $K(C,J)$ and $W(C,J)$.

PROPOSITION 2.1. *Let R be a commutative ring and p a rational prime. The R contains a minimal prime ideal P with $p \cdot 1_R$ in P if and only if R has non nilpotent p-torsion elements.*

Proof. Let x be a non nilpotent p-torsion element. Since x is not in $\mathrm{Nil}\, R$, there exists a minimal prime ideal P of R and an integer k with $p^k x = 0$ and x not in P. Since $p^k x$ lies in P, the element $p \cdot 1_R$ lies in P. Conversely, let P be a minimal prime ideal of R with $p \cdot 1_R$ in P. Then for the local ring R_P we have $\dim R_P = 0$ so that PR_P is a nil ideal. Since $p \cdot 1$ is in PR_P this means that there exists an integer k with $p^k \cdot 1 = 0$ in R_P so that there is an x in R, but not in P, with $p^k x = 0$. The element x is therefore not nilpotent.

COROLLARY 2.2. *$R_t \subset \mathrm{Nil}\, R$ if and only if $\mathbf{Z} \to R$ is injective and $P \cap \mathbf{Z} = 0$ for all minimal prime ideals P or R.*

Proof. If $R_t \subset \mathrm{Nil}\, R$ then $n \cdot 1_R = 0$ would imply that 1_R is nilpotent, hence $\mathbf{Z} \to R$ is injective. If $P \cap \mathbf{Z} \neq 0$ then P contains a rational prime which by Proposition 2.1 violates $R_t \subset \mathrm{Nil}\, R$. Conversely, let x be in R_t. Then $nx = 0$ for some n. But since $P \cap \mathbf{Z} = 0$, the integer n does not lie in any minimal prime ideal of R, thus x is in $\mathrm{Nil}\, R$.

Remark 2.3. Actually 2.2 can be strengthened as follows: Let $A \subset T$ be commutative rings and let T_t be the A-torsion subgroup of T. Then $T_t \subset \mathrm{Nil}\, T$ if and only if $P \cap A = 0$ for all minimal prime ideals P of T. This follows from [15, Exc. 37 (i), (iv), p. 44] by setting the ideal P used there $= 0$.

Definition 2.4. A commutative ring R is called von Neumann regular

if any one of the following equivalent conditions hold [6, Exc. 17, p. 64; Exc. 16, p. 173].

(i) For all x in R there is a y in R with $xyx = x$.

(ii) Any R-module is flat.

(iii) $\dim R = 0$ and $\operatorname{Nil} R = 0$.

(iv) $\operatorname{Spec} R$ is Hausdorff and Nil $R = 0$.

We also recall the definition of a Jacobson (or Hilbert) ring: A commutative ring is called Jacobson if each of its prime ideals is an intersection of maximal ideals.

LEMMA 2.5. *Let R be integral over $\mathbf{Z}$. Then*

(i) $\dim R \leqq 1$ *and R is Jacobson. In particular,* $\operatorname{Nil} R = \operatorname{Rad} R$.

(ii) *A prime ideal of R is maximal if and only if there is a rational prime p with $p \cdot 1_R$ in P.*

(iii) *If $R_t \subset \operatorname{Nil} R$ then $\mathbf{Z} \to R$ is injective, a prime ideal P of R is minimal if and only if $P \cap \mathbf{Z} = 0$, maximal otherwise, and every maximal ideal of R properly contains a minimal prime ideal.*

(iv) *If $R_t \subset \operatorname{Nil} R$ then* $\dim(\boldsymbol{Q} \otimes R) = 0$, $\boldsymbol{Q} \otimes \operatorname{Nil} R = \operatorname{Nil}(\boldsymbol{Q} \otimes R)$, $\boldsymbol{Q} \otimes R_{red} = (\boldsymbol{Q} \otimes R)_{red}$, *and $\boldsymbol{Q} \otimes R_{red}$ is von Neumann regular.*

(v) *For any rational prime p,* $\dim(R/pR) = 0$ *and hence R/pR is von Neumann regular if and only if* $\operatorname{Nil}(R/pR) = 0$.

Proof. Statement (i) follows from [15, Th. 48, p. 32] and [7, Prop. 5 and Cor., p. 67], while (ii) is a consequence of [7, Prop. 1, p. 36].

(iii) Assume $R_t \subset \operatorname{Nil} R$. By Corollary 2.2, $\mathbf{Z} \to R$ is injective and $P \cap \mathbf{Z} = 0$ for all minimal prime ideals P of R. Conversely, if $P \cap \mathbf{Z} = 0$ then by (ii) P cannot be maximal, whence by (i) it is a minimal prime ideal. Statement (ii) shows immediately that P is maximal if and only if $P \cap \mathbf{Z} \neq 0$. Finally, if a maximal ideal did not properly contain a minimal prime ideal then it would be a minimal prime ideal itself. But then by (ii) and Proposition 2.1, R would have non nilpotent torsion contradicting $R_t \subset \operatorname{Nil} R$.

(iv) $\boldsymbol{Q} \otimes R = S^{-1}R$ where S is the multplicative semigroup of nonzero integers. Hence the only prime ideals of $\boldsymbol{Q} \otimes R$ are $S^{-1}P$ with P a prime ideal of R such that $P \cap S = \emptyset$ [6, p. 91]. Then by (iii), $\dim(\boldsymbol{Q} \otimes R) = 0$. Since $\boldsymbol{Q}$ is a flat $\mathbf{Z}$-module and the elements of $\boldsymbol{Q} \otimes R$ have the form $1/n \otimes x$, it is clear that $\boldsymbol{Q} \otimes \operatorname{Nil} R \subset \operatorname{Nil}(\boldsymbol{Q} \otimes R)$. Conversely, if $(1/n \otimes x)^k = 0$

then x^k is in $R_t \subset \mathrm{Nil}\, R$. Thus $\boldsymbol{Q} \otimes \mathrm{Nil}\, R = \mathrm{Nil}(\boldsymbol{Q} \otimes R)$. Tensoring the exact sequence $0 \to \mathrm{Nil}\, R \to R \to R_{red} \to 0$ with $\boldsymbol{Q}$ then shows $\boldsymbol{Q} \otimes R_{red} = (\boldsymbol{Q} \otimes R)_{red}$. The final part follows from Definition 2.4 (iii).

(v) By (ii), $\dim(R/pR) = 0$ so that the result follows from Definition 2.4 (iii).

Example 2.6(i). If G is an abelian torsion group, we saw that $R = \boldsymbol{Z}[G]$ is an integral extension of $\boldsymbol{Z}$ and since R is a free $\boldsymbol{Z}$-module, $R_t = 0$. Thus Lemma 2.5 applies to R. Now it is well known that if F is any field of characteristic not dividing any of the orders of elements of G, then $F \otimes R = F[G]$ is von Neumann regular [14, Th. 26, p. 117]. Hence $\boldsymbol{Q} \otimes \mathrm{Nil}\, R = 0$ and so $\mathrm{Nil}\, R = 0$ since $R_t = 0$. Similarly, if p is a rational prime not dividing the order of any element of G, the ring R/pR is von Neumann regular.

(ii) Let $R \to R'$ be a surjection of rings. By the right exactness of the tensor product, $F \otimes R \to F \otimes R'$ is still a surjection for any commutative ring F. Now Definition 2.4(i) is clearly preserved under surjection so that $F \otimes R'$ is von Neumann regular if $F \otimes R$ is. In particular, therefore if $\boldsymbol{Q} \otimes R$ or R/pR is von Neumann regular the same is true for $\boldsymbol{Q} \otimes R'$ or R'/pR'. If (C, J) is a connected semi-local ring with involution, Theorem 1.16 shows that $K(C, J)$ and $W(C, J)$ are surjective images of $\boldsymbol{Z}[G]$ with G an abelian 2-group. Thus the rings $\boldsymbol{Q} \otimes K(C, J)$ and $\boldsymbol{Q} \otimes W(C, J)$ as well as the rings $K(C, J)/pK(C, J)$ and $W(C, J)/pW(C, J)$ for any odd rational prime p, are von Neumann regular.

Lemma 2.8 below will be used both here and in [20]. We first prove

LEMMA 2.7. *If $S \subset T$ are commutative rings with T integral over S and $\mathfrak{a}$ an ideal of S, then* $\mathrm{Ker}(S/\mathfrak{a} \to T/\mathfrak{a}T)$ *is nil.*

Proof. Since $\mathrm{Nil}(S/\mathfrak{a})$ is the intersection of all its prime ideals, we show that any prime ideal P of S containing $\mathfrak{a}$ also contains $\mathfrak{a}T \cap S$. By [7, Cor. 2, p. 38] there is a prime ideal P' of T with $P' \cap S = P$ and $P' \supset \mathfrak{a}T$. Hence $P \supset \mathfrak{a}T \cap S$.

LEMMA 2.8. *Let $S \subset T$ be commutative rings with T integral over S and p a rational prime.*

(i) *If* $\mathrm{Nil}(T/pT) = 0$ *and the abelian group T/S has zero p-torsion, then* $\mathrm{Nil}(S/pS) = 0$.

(ii) *If T has zero p-torsion and* $\mathrm{Nil}(S/pS) = 0$, *then T/S has zero p-torsion.*

Proof. For any abelian group X, we let $X[p]$ denote the subgroup of elements of order p. Then tensoring the exact sequence $0 \to S \to T \to T/S \to 0$ over $\mathbf{Z}$ with $\mathbf{Z}/p\mathbf{Z}$ and noting $\mathbf{Z}/p\mathbf{Z} \otimes X = X/pX$ and $\mathrm{Tor}_1^{\mathbf{Z}}(\mathbf{Z}/p\mathbf{Z}, X) = X[p]$ [8, p. 129], we get an exact sequence

$$T[p] \to (T/S)[p] \to S/pS \to T/pT.$$

This yields (i). Now Lemma 2.7 shows that $\mathrm{Ker}(S/pS \to T/pT)$ is nil so that with the hypothesis of (ii) the sequence $0 \to (T/S)[p] \to 0$ is exact, which proves (ii).

For any commutative ring R we denote the image $1 \otimes R$ of R in $\boldsymbol{Q} \otimes R$ by $\bar{R} \cong R/R_t$ and the integral closure of $\bar{R}$ in $Q \otimes R$ by $\tilde{R}$.

PROPOSITION 2.9. *Let R be integral over $\mathbf{Z}$ and p a rational prime such that $\mathrm{Nil}(R/pR) = 0$. Then $\tilde{R}/\bar{R}$ has zero p-torsion.*

Proof. By Lemma 2.5(v), R/pR is von Neumann regular. By Example 2.6(ii) it then follows that $\mathrm{Nil}(\bar{R}/p\bar{R}) = 0$. Then Lemma 2.8(ii) completes the proof since $\tilde{R}$ is torsion free.

Remark. One can also prove the following analogous proposition: Let R be a commutative ring with $R_t \subset \mathrm{Nil}\, R$ and $\mathrm{Nil}(R/pR) = 0$ for some rational prime p. Then $\tilde{R}/\bar{R}$ has zero p-torsion.

Example. If R is the group ring of a finite abelian group of order n then $n(\tilde{R}/\bar{R}) = 0$ [2, Cor. 1.2, p. 560].

COROLLARY 2.10. *Let R be integral over $\mathbf{Z}$ and p a rational prime such that $\mathrm{Nil}(R/pR) = 0$. If e is an idempotent of $\boldsymbol{Q} \otimes R$ then there exists an integer n with $(n, p) = 1$ and an element x in R with $e = 1/n \otimes x$.*

Proof. Clearly e is in $\tilde{R}$. Since $\tilde{R}/\bar{R}$ is torsion, Proposition 2.9 shows that the order, n, of the class of e in $\tilde{R}/\bar{R}$ is prime to p. Thus ne lies in $\bar{R} = 1 \otimes R$.

Remark 2.11. Proposition 2.8 can also be used to give a proof of the following theorem of Rosenberg-Ware [27]: Let $E \supset F$ be a galois extension of fields of odd degree m with galois group $\mathfrak{G}$. If J is the identity we write $W(C)$ for $W(C, J)$. Then $W(E)^{\mathfrak{G}} = W(F)$, where the operation of $\mathfrak{G}$ on $W(E)$ arises from the functorial properties of $W(\ )$. For the proof we note first that if $\mathrm{Tr} = \sum_{\sigma \text{ in } \mathfrak{G}} \sigma$ then $\mathrm{Tr}(W(E)) \subset W(F)$ [21]. Thus for an element ξ of $W(E)^{\mathfrak{G}}$ we have that $m\xi$ lies in $W(F)$. Hence $W(E)^{\mathfrak{G}}/W(F)$ is an m-torsion group and so if it is not zero it has non zero p-torsion for some

odd prime p. Now it is known [26, Satz 10], and we shall show in 3., that $W(E)$ has only 2-torsion. Moreover, by Example 2.6(ii), $\mathrm{Nil}(W(F)/pW(F)) = 0$. Thus Lemma 2.8(ii) shows that $W(E)^{\mathfrak{G}}/W(F)$ has zero p-torsion. The contradiction forces $W(E)^{\mathfrak{G}} = W(F)$.

The following theorem in conjunction with Corollary 2.10 represent the main result of 2.

THEOREM 2.12. *Let R be an integral extension of $\mathbf{Z}$ such that $R_t \subset \mathrm{Nil}\, R$ and M a maximal ideal of R such that $M \cap \mathbf{Z} = p\mathbf{Z}$. If every idempotent e of $\mathbf{Q} \otimes R$ can we written as $1/n \otimes x$ with $(p, n) = 1$ and x in R, then M properly contains a unique minimal prime ideal.*

Proof. By Lemma 2.5(iii) M properly contains at least one minimal prime ideal. The rest of the proof is a series of reductions.

First we note that it suffices to treat the case $R_t = \mathrm{Nil}\, R = 0$. For if $\mathrm{Nil}\, R \cap \mathbf{Z} \neq 0$ then 1 is in $R_t \subset \mathrm{Nil}\, R$, which is absurd. Thus $\mathbf{Z}$ embeds into R_{red}. It is easily checked that if $\bar{M} = M/\mathrm{Nil}\, R$ then $\bar{M} \cap \mathbf{Z} = M \cap \mathbf{Z} = p\mathbf{Z}$. By Lemma 2.5(iv), $\mathbf{Q} \otimes R_{red} = (\mathbf{Q} \otimes R)_{red}$ and so by [6, Cor. 1, p. 132] the idempotents of $\mathbf{Q} \otimes R_{red}$ are images of idempotents of $\mathbf{Q} \otimes R$. Thus the hypotheses of Theorem 2.12 are inherited by R_{red} and $\bar{M}$. Finally, since $\mathrm{Nil}\, R$ is in every prime ideal of R, if $\bar{M}$ contains a unique minimal prime ideal, M does also.

Assuming now $\mathrm{Nil}\, R = R_t = 0$ we reduce to the case where $[\mathbf{Q} \otimes R : \mathbf{Q}]$ is finite. Thus $R \to \mathbf{Q} \otimes R$ is an injection and we identify R with $1 \otimes R$. Suppose M contains two distinct minimal prime ideals P_1 and P_2. Let $x \in P_1$, $x \notin P_2$. Since x is integral over $\mathbf{Z}$, the subalgebra $A = \mathbf{Q}[x]$ of $\mathbf{Q} \otimes R$ generated by x has finite dimension over $\mathbf{Q}$. By Lemma 2.5(iv), $\mathrm{Nil}(\mathbf{Q} \otimes R) = 0$, so that A is a direct product of fields. Let $e_1, \cdots, e_k$ be the primitive idempotents of A. We can write $e_i = m_i^{-1} y_i$ with $(m_i, p) = 1$ and y_i in R. Then $y_i = m e_i$ is in A. Let $R_0 = \mathbf{Z}[x, y_1, \cdots, y_k]$. Evidently $\mathbf{Q} \otimes R_0 = \mathbf{Q} R_0 = A$ so that $[\mathbf{Q} \otimes R_0 : \mathbf{Q}]$ is finite. Since the only idempotents of A are sums of the e_i, it is easily verified that all the idempotents of $A = \mathbf{Q} \otimes R_0$ can be written as $m^{-1} y$ with $(m, p) = 1$ and y in R_0. Now by [7, Cor. 1, p. 36] $M \cap R_0 = M_0$ is maximal in R_0 and $(M \cap R_0) \cap \mathbf{Z} = M \cap \mathbf{Z} = p\mathbf{Z}$. Clearly $P_1 \cap R_0 \neq P_2 \cap R_0$.

Hence we are finally reduced to the case where $[\mathbf{Q} \otimes R : \mathbf{Q}]$ is finite, $\mathrm{Nil}\, R = R_t = 0$ and the maximal ideal contains two distinct minimal prime ideals P_1, P_2. Let T be the multiplicative semigroup of integers generated by all rational primes distinct from p. Clearly $M \cap T = \emptyset$, so that in $T^{-1}R \subset \mathbf{Q} \otimes R$,

the ideal $T^{-1}M$ is maximal and contains the distinct minimal prime ideals $T^{-1}P_1$ and $T^{-1}P_2$. But $T^{-1}R$ contains all the idempotents of $\boldsymbol{Q} \otimes R$ which is a direct product of fields. Hence $T^{-1}R$ is a direct product of integral domains: $T^{-1}R = D_1 \times D_2 \times \cdots \times D_k$. Since R is integral over $\boldsymbol{Z}$, it follows that each D_i is integral over $T^{-1}\boldsymbol{Z}$ [7, Prop. 16, p. 22]. Hence $\dim D_i = 1$ [15, Th. 48, p. 32]. Now prime ideals of $T^{-1}R$ must contain all but one of the identity elements of the D_i. Since the non zero prime ideals in D_i are maximal, the only non maximal prime ideals of $T^{-1}R$ are $\underset{i \neq i_0}{\times} D_i$. Thus $T^{-1}P_1$, $T^{-1}P_2$ cannot both be in $T^{-1}M$. Hence M contains precisely one minimal prime ideal.

In the case of group rings we can prove a converse of Theorem 2.12. We first need

LEMMA 2.13. *Let G be an abelian q-group, where q is a rational prime. Then M_0, the kernel of the augmentation map $\boldsymbol{Z}[G] \to \boldsymbol{Z}$ followed by reduction modulo q is the unique maximal ideal of $\boldsymbol{Z}[G]$ containing q.*

Proof. It is clear that M_0 is a maximal ideal containing q. Conversely, let M be a maximal ideal of $\boldsymbol{Z}[G]$ containing q. Then $\boldsymbol{Z}[G]/M$ is a field of charactersitic q and so, since every element g of G satisfies an equation of the form $g^{q^n} = 1$, G is mapped to the identity of $\boldsymbol{Z}[G]/M$. Hence the kernel of the augmentation map is contained in M and thus $M = M_0$.

THEOREM 2.14. *Let G be an abelian torsion group, M a maximal ideal of $\boldsymbol{Z}[G]$ and p the rational prime with $M \cap \boldsymbol{Z} = p\boldsymbol{Z}$. Then the following are equivalent:*

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

(ii) *p does not divide the order of any element of G.*

Proof. The implication (ii) $\Rightarrow$ (i) follows from Theorem 2.12, Example 2.6, and Corollary 2.10.

Conversely, suppose (i) holds. Let g be an element of order p in G and H the subgroup of G generated by g. Set $M' = \boldsymbol{Z}[H] \cap M$. By Lemma 2.13, M' is the unique maximal ideal of $\boldsymbol{Z}[H]$ containing p. Hence by [7, Cor. 2, p. 38], M' contains all the minimal prime ideals of $\boldsymbol{Z}[H]$. But the integral group algebra of any non trivial abelian torsion group contains more than one minimal prime ideal since it is not a domain and the intersection of the minimal prime ideals is zero by Example 2.6. Thus M' contains at least two distinct minimal prime ideals of $\boldsymbol{Z}[H]$. Now $\boldsymbol{Z}[G]$ is a free, whence flat $\boldsymbol{Z}[H]$-module. Hence by [24, Th. 4, p. 33] for any

prime ideal P' in M' there is a prime ideal P in M with $P \cap \mathbf{Z}[H] = P'$ (i.e. the Going Down Theorem holds). Hence there must exist two distinct prime ideals in M. This contradiction shows that G has no elements of order p, proving (ii).

3. Residue class rings of $\mathbf{Z}[G]$ for G an abelian torsion group. Throughout this section G denotes an abelian torsion group, K a proper ideal of the integral group ring $\mathbf{Z}[G]$, and R the residue class ring $\mathbf{Z}[G]/K$. The letters p and q will always denote rational prime numbers. Let χ be a character of G, i.e. a homomorphism of G into the field of complex numbers. For each g in G, the element $\chi(g)$ is a root of unity. For a given group G, let $\mathfrak{L}$ be the field generated over $\mathbf{Q}$ by all the $\chi(g)$ and let $\mathfrak{A}$ be the integral closure of $\mathbf{Z}$ in $\mathfrak{L}$. Every character χ gives rise in an obvious way to a ring homomorphism ψ_χ of $\mathbf{Z}[G]$ into $\mathfrak{A}$ and, conversely, by restricting a ring homomorphism ψ, of $\mathbf{Z}[G]$ into $\mathfrak{A}$, to G, we obtain a character χ of G with $\psi = \psi_\chi$. The ideal K gives rise to ideals $\psi_\chi(K)$ in $\psi_\chi(\mathbf{Z}[G])$. The main aim of this section is to characterize structural properties of R in terms of the $\psi_\chi(K)$.

LEMMA 3.1. *The minimal prime ideals of $\mathbf{Z}[G]$ are the kernels P_χ of the $\psi_\chi: \mathbf{Z}[G] \to \mathfrak{A}$. The maximal ideals of $\mathbf{Z}[G]$ are of the form $M_{\chi,\mathfrak{p}} = \psi_\chi^{-1}(\mathfrak{p})$ where $\mathfrak{p}$ is a non zero prime ideal (i.e. maximal ideal) of $\mathfrak{A}$.*

Proof. By Lemma 2.5(iii) and Example 2.6, a prime ideal P of $\mathbf{Z}[G]$ is a minimal prime ideal if and only if $P \cap \mathbf{Z} = 0$. Since ψ_χ is a monomorphism on $\mathbf{Z}$ it is clear that the P_χ are minimal prime ideals. Conversely, for any prime ideal P of $\mathbf{Z}[G]$ such that $P \cap \mathbf{Z} = 0$ the quotient field $\mathfrak{L}'$ of $\mathbf{Z}[G]/P$ is a field of algebraic numbers, which we can assume embedded in $\mathbf{C}$. Thus the map $g \mapsto g + P$ is a character χ and so $\mathfrak{L}' \subset \mathfrak{L}$. It is clear that $P = \operatorname{Ker} \psi_\chi$.

By [7, Prop. 1, p. 36], $\mathfrak{p} \cap \mathbf{Z} \neq 0$ for any non zero prime ideal $\mathfrak{p}$ of $\mathfrak{A}$. But clearly $M_{\chi,\mathfrak{p}} \supset \mathfrak{p} \cap \mathbf{Z} \neq 0$ and so again by Lemma 2.5(iii) and Example 2.6, the $M_{\chi,\mathfrak{p}}$ are maximal ideals for all χ and $\mathfrak{p}$. Conversel. let M be a maximal ideal of $\mathbf{Z}[G]$. By Lemma 2.5(iii), M properly contains a minimal prime ideal P_χ. Then ψ_χ yields an isomorphism of $\mathbf{Z}[G]/P_\chi$ onto a subring $\mathfrak{A}_\chi$ of $\mathfrak{A}$. Let $\psi_\chi(M) = \mathfrak{p}'$, a maximal ideal of $\mathfrak{A}_\chi$. By [7, Th. 1, p. 38, Prop. 1, p. 36] there is a maximal ideal $\mathfrak{p}$ of A with $\mathfrak{p}' = \mathfrak{A}_\chi \cap \mathfrak{p}$. Clearly, $M_{\chi,\mathfrak{p}} = M$.

Remark 3.2. The preceding takes on a particularly simple form if G is a group of exponent 2. For then $g^2 = 1$, forces $\chi(g) = \pm 1$ for all χ

and g so that $\mathfrak{Q} = \boldsymbol{Q}$ and $\mathfrak{P} = \boldsymbol{Z}$. Thus for all minimal prime ideals P of $\boldsymbol{Z}[G]$, we have $\boldsymbol{Z}[G]/P = \boldsymbol{Z}$. Since the only ring automorphism of $\boldsymbol{Z}$ is the identity, a homomorphism of $\boldsymbol{Z}[G]$ onto $\boldsymbol{Z}$ is completely determined by its kernel. Thus, in this case, there is a bijective correspondence between the characters χ of G and the minimal prime ideals of $\boldsymbol{Z}[G]$. Furthermore, all maximal ideals of $\boldsymbol{Z}$ being of the form $p\boldsymbol{Z}$, we have $M_{\chi,\mathfrak{p}} = P_\chi + p\boldsymbol{Z}$.

LEMMA 3.3. *Let $R = \boldsymbol{Z}[G]/K$. Then R is Jacobson,* $\operatorname{Nil} R = \operatorname{Rad} R$ *and* $R_t \supset \operatorname{Nil} R$.

Proof. The first two statements follow from Lemma 2.5(i). By Example 2.6, $\boldsymbol{Q} \otimes R$ is von Neumann regular. Thus $\operatorname{Nil}(\boldsymbol{Q} \otimes R) = 0$, which shows $\boldsymbol{Q} \otimes \operatorname{Nil} R = 0$, i.e. $\operatorname{Nil}(R) \subset R_t$.

PROPOSITION 3.4. *$R_t = \operatorname{Nil} R$ 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 are minimal prime ideals.*

Proof. If $R_t = \operatorname{Nil} R$, Lemma 2.5(iii) shows that no maximal prime ideal is a minimal prime ideal. The condition $R_t = R$ is equivalent to $\boldsymbol{Z} \to R$ not being injective. In that case R contains $\boldsymbol{Z}/n\boldsymbol{Z}$ for some n and since $\dim(\boldsymbol{Z}/n\boldsymbol{Z}) = 0$, [15, Th. 48, p. 32] shows that then all maximal ideals of R are minimal prime ideals. For the converses, we first note that if no maximal ideal of R is a minimal prime ideal, $\boldsymbol{Z} \to R$ is injective and thus by Lemma 2.5(ii), $P \cap \boldsymbol{Z} = 0$ for all minimal prime ideals of R. Then Corollary 2.2 shows that $R_t \subset \operatorname{Nil} R$, which together with Lemma 3.3 proves $R_t = \operatorname{Nil} R$. If all maximal ideals of R are minimal prime ideals and $\boldsymbol{Z} \to R$ is an injection then again [15, Th. 48, p. 32] yields a contradiction; thus $\boldsymbol{Z} \to R$ has a non zero kernel and $R_t = R$.

Using Lemma 3.1 we easily obtain the following more explicit formulation of the case $R_t = R$ in Proposition 3.4:

COROLLARY 3.5. *The following conditions are equivalent*

(i) $R_t = R$

(ii) $K \cap \boldsymbol{Z} \neq 0$

(iii) $\dim R = 0$

(iv) *For all characters χ of G, we have $\psi_\chi(K) \neq 0$.*

The first main result of this section deals with the existence of p-torsion in R. We need

LEMMA 3.6. *For any character* χ *we have* $\psi_\chi(K) \cap \mathbf{Z} = (K + P_\chi) \cap \mathbf{Z}$.

Proof. Since ψ_χ is the identity on $\mathbf{Z}$, it is clear that the right hand side is contained in the left hand side. If n lies in $\psi_\chi(K) \cap \mathbf{Z}$, then $n = \psi_\chi(x)$ or $n = x + y$ where x lies in K and y in P_χ. Thus the left hand side is in the right hand side.

COROLLARY 3.7. $(K + P_\chi) \cap \mathbf{Z} \neq 0$ *if and only if* $K \not\subset P_\chi$.

Proof. Since 0 is a prime ideal of $\mathfrak{A}$, if $\psi_\chi(K) \cap \mathbf{Z} = 0$, then $\psi_\chi(K) = 0$ [7, Cor. 1, p. 36]. Thus if $K \not\subset P_\chi$, then $\psi_\chi(K) \cap \mathbf{Z} = (K + P_\chi) \cap \mathbf{Z} \neq 0$. The reverse implication is clear.

THEOREM 3.8. *Let* p *be a rational prime not dividing the order of any element of* G. *Then the following are equivalent:*

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

(ii) R *contains a minimal prime ideal* $\bar{M}$ *with* $R/\bar{M}$ *a field of characteristic* p.

(iii) R *has non nilpotent* p*-torsion.*

(iv) R *has non zero* p*-torsion.*

Proof. According to Lemma 3.1 and Corollary 3.7, (i) is equivalent to (i′): There exists a minimal prime ideal P of $\mathbf{Z}[G]$ with

$$0 \neq (P + K) \cap \mathbf{Z} \subset p\mathbf{Z}.$$

(i′) $\Rightarrow$ (ii). By [7, Cor. 2, p. 38] there exists a maximal ideal M of $\mathbf{Z}[G]$ with $M \supset P + K$ and $M \cap \mathbf{Z} = p\mathbf{Z}$. By Theorem 2.14, P is the unique minimal prime ideal of $\mathbf{Z}[G]$ in M. By Corollary 3.7, $K \not\subset P$, thus $\bar{M} = M/K$ is a minimal prime ideal of R which contains p and is also maximal in R.

(ii) $\Rightarrow$ (i′). This implication is valid without any hypothesis on p. Let M be the inverse image of $\bar{M}$ in $\mathbf{Z}[G]$. For all minimal prime ideals P of $\mathbf{Z}[G]$ in M we must have $K \not\subset P$. Thus by Corollary 3.7,

$$0 \neq (K + P) \cap \mathbf{Z} \subset M \cap \mathbf{Z} = p\mathbf{Z}.$$

(ii) $\Leftrightarrow$ (iii). By Proposition 2.1, (iii) is equivalent to the existence of a minimal prime ideal of R which contains p. By Lemma 2.5(ii) this ideal is maximal.

(iii) $\Leftrightarrow$ (iv). The implication (iii) $\Rightarrow$ (iv) is trivial. To prove (iv) $\Rightarrow$ (iii) we shall assume that all p-torsion elements are nilpotent and show that this implies that the p-torsion is 0. Let x in $\operatorname{Nil} R$ be such that

$p^r x = 0$. Then there exists a finitely generated, whence finite, subgroup H of G with x in $R_1 = \mathbf{Z}[H]/\mathbf{Z}[H] \cap K$. By hypothesis p is prime to the order of H. By Example 2.6, $\mathrm{Nil}(R_1/pR_1) = 0$. Thus the image of x in R_1/pR_1 is 0, i.e. there is an element y in R_1 with $py = x$. Clearly, y is p-torsion and so by hypothesis lies in $\mathrm{Nil}\, R_1$. Hence the p-torsion element x is infinitely divisible by p in the finitely generated abelian group R_1. Therefore $x = 0$ as desired.

Assume now that G is a q-group for q a rational prime. By Lemma 2.13, $\mathbf{Z}[G]$ contains a unique maximal ideal M_0 with $M_0 \cap \mathbf{Z} = q\mathbf{Z}$. Any maximal ideal of $\mathbf{Z}[G]$ distinct from M_0 contains a unique minimal prime ideal by Theorem 2.14. By [7, Cor. 2, p. 38] and Lemma 2.5(iii), M_0 contains all minimal prime ideals of $\mathbf{Z}[G]$.

Before stating the next theorem we introduce some notation for an arbitrary commutative ring R. Let $Y \subset \mathrm{Spec}\, R$, the set of prime ideals of R. Let $I(Y) = \bigcap_{P \in Y} P$. For any ideal $\mathfrak{a}$ we let $\sqrt{\mathfrak{a}}$ denote the radical of $\mathfrak{a}$. It is well known that $\sqrt{\mathfrak{a}}$ is the intersection of all prime ideals (all prime ideals minimal over $\mathfrak{a}$) containing $\mathfrak{a}$ [6, Cor. 1, p. 95].

THEOREM 3.9. *Let G be an abelian q-group. For any ideal K of $\mathbf{Z}[G]$ the following are equivalent:*

(i) *Let $M \neq M_0$ be a maximal ideal of $\mathbf{Z}[G]$ and P_χ a minimal prime ideal of $\mathbf{Z}[G]$ in M. If $K \subset M$, then $K \subset P_\chi$.*

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

(iii) $R = \mathbf{Z}[G]/K$ *has only* q*-torsion.*

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

(v) $\sqrt{K} = I(Y)$ *with* $Y \subset \mathrm{Min}(\mathbf{Z}[G])$, *the set of minimal prime ideals of* $\mathbf{Z}[G]$, *with the convention that* $I(\emptyset) = M_0$.

Proof. Statement (ii) is false if and only if there exists a characted χ of G with $0 \neq \psi_\chi(K) \cap \mathbf{Z} \subset p\mathbf{Z}$ with $p \neq q$ since a non zero ideal of $\mathbf{Z}$ is not in $p\mathbf{Z}$ for all $p \neq q$ if and oniy if it is the form $q^r\mathbf{Z}$. With this remark the equivalence of (i) and (ii) follows from the equivalence of (i) and (ii) in Theorem 3.8 and the equivalence of (ii) and (iii) follows from the equivalence of (i) and (iii) of Theorem 3.8.

(i) $\Rightarrow$ (iv). Let Q be a prime ideal of $\mathbf{Z}[G]$ containing K. If Q is a maximal and distinct from M_0, then by (i), K is in a minimal prime ideal of $\mathbf{Z}[G]$ which, as we noted above, all lie in M_0. In any case $K \subset M_0$. Now

the set of zero divisors in R is a union of prime ideals [15, 2., p. 3]. By (iii), none of these prime ideals can contain $p \neq q$ thus their inverse images in $\boldsymbol{Z}[G]$ either are minimal prime ideals or M_0. In either case, they lie in $\bar{M}_0$ which proves (iv).

(iv) $\Rightarrow$ (v). To prove (v) it is enough to show that if $P \neq M_0$ is a prime ideal minimal over K then P is a minimal prime ideal of $\boldsymbol{Z}[G]$. Let $\bar{P} = P/K$. Then $\bar{P}$ is a minmal prime ideal of R and hence consists entirely of zero divisors [15, Th. 84, p. 51]. By (iv) this means $\bar{P} \subsetneq \bar{M}_0$ whence $P \subsetneq M_0$ and so P is a minimal prime ideal of $\boldsymbol{Z}[G]$.

(v) $\Rightarrow$ (i). Clearly both (i) and (v) hold for K if and only if they are valid for $\sqrt{K}$. Hence we may assume that $K = \sqrt{K}$. Now $\boldsymbol{Z}[G]/I(Y)$ is embedded in $\prod_{P \in Y} \boldsymbol{Z}[G]/P$, which, since by Lemma 2.5(iii) $P \cap \boldsymbol{Z} = 0$, is a product of torsion free domains. The implication (v) $\Rightarrow$ (i) now follows from the implication (iii) $\Rightarrow$ (i) which has already been proved.

COROLLARY 3.10. *Let K satisfy the conditions of Theorem 3.9, then R is connected (i.e. has not idempotents except 0 and 1), and $R_t \neq 0$ if and only if $\bar{M}_0$ consists entirely of zero divisors.*

Proof. Let $e \neq 0$ or 1 be an idempotent of R. Then both e and $(1-e)$ are zero divisors and so by Theorem 3.9(iv) lie in $\bar{M}_0$. This is impossible, and so either $e = 0$ or $e = 1$. If $R_t \neq 0$ then by Theorem 3.9(iii) $q \cdot 1_R$ is a zero divisor in R. Now the set of zero divisors is a union of prime ideals in $\bar{M}_0$ by Theorem 3.9(iv). None of the non-maximal prime ideals of R contain q so that $\bar{M}_0$ itself must consist entirely of zero divisors. Conversely, if $\bar{M}_0$ consists entirely of zero divisors, $q \cdot 1_R$ is one which means $R_t \neq 0$.

Example 3.11. Let $R = K(C, J)$ *or* $W(C, J)$ with C a semi-local ring with involution and containing no non trivial idempotent. By Corollary 1.21 we see that Theorem 3.9 and Corollary 3.10 apply to R with $q = 2$. As pointed out in the Introduction, Theorem 3.9 and Corollary 3.10 also apply when R is the Witt or the Witt-Grothendieck of a profinite group as defined in [3] and [28]. In particular R is a connected Jacobson ring with $\operatorname{Rad} R = \operatorname{Nil} R \subset R_t$ which is a 2-group (Lemma 3.3, Corollary 3.10 and Theorem 3.9(iii)). The ideal $\bar{M}_0$ consists of classes of forms of even rank since this set is a maximal ideal containing 2. Thus no hermitian form of odd rank is a zero divisor in $K(C, J)$ or $W(C, J)$. (Theorem 3.9(iv)). For C a field, J the identity and $R = W(C, J)$ these results can also be found in [23, 26, 30]. Furthermore $R/\bar{P} \cong \boldsymbol{Z}$ for all non maximal prime ideals $\bar{P}$ of R (Remark 3.2).

Any maximal ideal $\bar{M}$ of R distinct from $\bar{M}_0$ contains exactly one minimal prime ideal $\bar{P}$ (Theorems 2.4 and 3.9(i)) and thus $\bar{M} = \bar{P} + \mathbf{Z}$ with p an odd rational prime. On the other hand, $\bar{M}_0 = \bar{P} + 2\mathbf{Z}$ for all minimal prime ideals $\bar{P}$ of R (cf. [11, 22] in case C is a field, J the identity and $R = W(C, J)$).

Example 3.11 leads us to the following

Definition 3.12. Let R be a commutative ring with $R \cong \mathbf{Z}[G]/K$ where G is an abelian q-group and K is an ideal of $\mathbf{Z}[G]$ satisfying condition (ii) of Theorem 3.9. Then R is called a *Witt ring for* G.

Remarks 3.13. (i) Let R be a Witt ring for G and H a subgroup of G. The subring $R_H \cong \mathbf{Z}[H]/\mathbf{Z}[H] \cap K$ then is a Witt ring for H since by Theorem 3.9(iii) its only possible torsion is q-torsion and so $K \cap \mathbf{Z}[H]$ satisfies condition (iii) of Theorem 3.9.

(ii) Since $\sqrt{\sqrt{K}} = \sqrt{K}$, an ideal K in $\mathbf{Z}[G]$ satisfies the conditions of Theorem 3.9 if and only if $\sqrt{K}$ does. Hence R is a Witt ring for G if and only if R_{red} is.

(iii) If R is a Witt ring for G and $R \cong \mathbf{Z}[G']/K'$ for some other abelian q-group G' then since the only possible torsion in R is q-torsion, Theorem 3.9 shows that R is also a Witt ring for G'. Hence a commutative ring is a Witt ring for some abelian q-group if and only if R_t is q-torsion and R is additively generated by a q-group of units of R.

PROPOSITION 3.14. *Let* $R = \mathbf{Z}[G]/K$ *be a Witt ring for* G. *Then* $\operatorname{Nil} R = 0$ *if and only if* $K = I(Y)$ *with* $Y \subset \operatorname{Min}(\mathbf{Z}[G])(I(\emptyset) = M_0)$. *There is a bijection between the closed subsets* Y *or* $\operatorname{Min}(\mathbf{Z}[G])$ *and the reduced Witt rings for* G *given by* $Y \leftrightarrow \mathbf{Z}[G]/I(Y)$.

Proof. This is immediate keeping in mind $\operatorname{Nil} R = \sqrt{K}/K$, Theorem 3.9(v), and the fact that if $\bar{Y}$ is the closure of Y in $\operatorname{Min}(\mathbf{Z}[G])$ then $I(\bar{Y}) = I(Y)$ [6, Prop. 11(iii), p. 126].

Next we show that if R is a Witt ring for G, we either have $R_t = \operatorname{Nil} R$ or $R_t = R$.

PROPOSITION 3.15. *Let* $R = \mathbf{Z}[G]/K$ *where* G *is an abelian* q*-group. Then* $R_t = \operatorname{Nil} R$ *if and only if* $K \cap \mathbf{Z} = 0$ *and* R *is a Witt ring for* G. *In this case* R *contains non maximal prime ideals.*

Proof. If $R_t = \operatorname{Nil} R$, then by Lemma 2.5(iii), $K \cap \mathbf{Z} = 0$ and every maximal ideal of R properly contains a minimal prime ideal so (i) of

Theorem 3.9 holds. Conversely, if $K \cap \mathbf{Z} = 0$ and the conditions of Theorem 3.9 hold, then by Corollary 3.5, R has non maximal prime ideals (which are necessarily minimal) and by Theorem 3.9(v) all minimal prime ideals are properly contained in $\bar{M}_0 = M_0/K$. Hence, if $\bar{P}$ is any minmal prime ideal of R, then $\bar{P}$ cannot be maximal so by Propisition 3.4, $R_t = \operatorname{Nil} R$.

PROPOSITION 3.16. *Let $R = \mathbf{Z}[G]/K$ where G is an abelian q-group. Then the following are equivalent:*

(i) *$R = R_t$ is a q-group and hence R is a Witt ring for G.*

(ii) *$\psi_\chi(K) \cap \mathbf{Z} = q^n{}_\chi\mathbf{Z}$ for all characters χ of G.*

(iii) *R is local with unique prime ideal $\bar{M}_0 = M_0/K$.*

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

Proof. The equivalence of (i) and (iv) is immediate.

(i) $\Rightarrow$ (ii). This follows from Theorem 3.9 and Corollary 3.5.

(ii) $\Rightarrow$ (iii). By Corollary 3.5, $\dim R = 0$ and hence by Theorem 3.9(i), R can contain no maximal ideal distinct from $\bar{M}_0$.

(iii) $\Rightarrow$ (i). By the hypothesis $\bar{M}_0 = \operatorname{Nil} R$ whence $(q \cdot 1_R)^n = q^n \cdot 1_R = 0$ for some natural number n. Hence $R = R_t$ is a q-group.

In case C is a field of characteristic $\neq 2$, J is the identity, and $R = W(C, J)$ it is shown in [26, Satz 22, Satz 17] that the conditions of Proposition 3.15 are equivalent to C being formally real and those of Proposition 3.16 to C not being formally real. We shall return to these matters in [19].

PROPOSITION 3.17. *Let R be a Witt ring for some abelian q-group with $R \neq R_t$. If $\bar{R}$ denotes the subring $1 \otimes R \cong R_{red}$ of $\mathbf{Q} \otimes R$ and $\tilde{R}$ the integral closure of $\bar{R}$ in $\mathbf{Q} \otimes R$, then $\tilde{R}/\bar{R}$ is a q-group.*

Proof. By Example 2.6(ii), $\operatorname{Nil}(R/pR) = 0$ for all $p \neq q$. The result then follows from Proposition 2.9.

A detailed topological study of $\tilde{R}$ in case G has exponent two appears in [19].

The following proposition may be of some interest because of our results on the relationship between $\operatorname{Nil} R$ and R_t. We shall make no use of it in the sequel.

PROPOSITION. *Let G be an abelian q-group and $R = \mathbf{Z}[G]/K$ be an*

arbitrary quotient of $\mathbf{Z}[G]$. *If* $K \not\subset M_0$ *then any q-torsion element of* R *is nilpotent. If* $K \subset M_0$, *any q-torsion element of* R *in* M_0 *is nilpotent.*

Proof. Let $\bar{x}$ be a q-torsion element in R. If x is any inverse image of $\bar{x}$ in $\mathbf{Z}[G]$, there is an integer n such that $q^n x$ lies in K. If Q is any prime ideal of $\mathbf{Z}[G]$ which contains K we have $q^n x$ is in Q. It follows from Lemma 2.13 that if $Q \not\supset M_0$ then x is in Q. Hence, in the first case $\bar{x}$ is in all the prime ideals of R and so is nilpotent. In the second case, assume $\bar{x}$ is in $\bar{M}_0$, then again $\bar{x}$ is in all prime ideals of R and so is nilpotent.

We end this section by considering the abelian group structure of $R/\mathrm{Nil}\, R$ and the units of finite order in R where R is a Witt ring for G. First we note

LEMMA 3.18. *Let* $\mathfrak{F}$ *be a not necessarily finite algebraic extension field of* $\boldsymbol{Q}$ *and* $\mathfrak{A}$ *the integral closure of* $\mathbf{Z}$ *in* $\mathfrak{F}$. *Then* $\mathfrak{A}$ *is a free* $\mathbf{Z}$*-module.*

Proof. We can write $\mathfrak{F} = \bigcup_1^\infty \mathfrak{F}_i$ where the $\mathfrak{F}_i$ are finite dimensional algebraic extension fields of $\boldsymbol{Q}$ with $\boldsymbol{Q} = \mathfrak{F}_1 \subset \mathfrak{F}_2 \cdots \subset \mathfrak{F}_i \subset \mathfrak{F}_{i+1} \subset \cdots$. Let $\mathfrak{A}_i$ be the integral closure of $\mathbf{Z}$ in $\mathfrak{F}_i$. Then it is clear that $\mathfrak{A} = \bigcup_1^\infty \mathfrak{A}_i$. Moreover, it is easily checked that $\mathfrak{A}_{i+1}/\mathfrak{A}_i$ is torsion free. Therefore the $\mathbf{Z}$-module $\mathfrak{A}_{i+1}/\mathfrak{A}_i$ is finitely generated and torsion free and so is free. Thus the map $\mathfrak{A}_{i+1} \to \mathfrak{A}_{i+1}/\mathfrak{A}_i$ splits and we have $\mathfrak{A}_{i+1} = C_i \oplus \mathfrak{A}_i$. Let B_i be a basis of C_i over $\mathbf{Z}$. Clearly, $1 \cup \bigcup_1^\infty B_i$ is a basis of $\mathfrak{A}$ over $\mathbf{Z}$.

PROPOSITION 3.19. *Let* R *be a Witt ring for* G *with* $R_t \neq R$. *Then* R_{red} *is a free abelian group and thus the exact sequence of abelian groups*

$$0 \to \mathrm{Nil}\, R \to R \to R_{red} \to 0$$

splits.

Proof. Let $\bar{P}$ be a minmal prime ideal of $R = \mathbf{Z}[G]/K$ and P its inverse image in $\mathbf{Z}[G]$. By Lemma 3.1, there is a character χ of G and a homomorphism $\psi_\chi : \mathbf{Z}[G] \to \mathfrak{A}$ with $P = P_\chi$. Thus the natural homomorphism $R \to R/\bar{P}$ is induced by ψ_χ. Let $X = \mathrm{Min}\, R$. For each r in R we define a function $f : X \to \mathfrak{A}$ by $f(\bar{P}) = \psi_\chi(r_0)$ where r_0 is an inverse image of r in $\mathbf{Z}[G]$. Since $r_0 = \sum a_i g_i$ and there is some m with $g_i^m = 1$ it is clear that $r \mapsto f$ yields an embedding of $R/\bigcap \bar{P} = R_{red}$ into $F(X, \mathfrak{A})$ the ring of finite valued functions from X to $\mathfrak{A}$. By Lemma 3.18, $\mathfrak{A}$ is a free abelian group. By composing a nite valued function from X to $\mathfrak{A}$ with the coordinate

projections of $\mathfrak{A}$ to the elements of some basis, it is easily verified that $F(X, \mathfrak{A})$ is isomorphic as abelian group to a direct sum of copies of $F(X, \mathbf{Z})$. By [25], $F(X, \mathbf{Z})$ is a free abelian group and so $F(X, \mathfrak{A})$ and R_{red} are also.

Remark 3.20. If G is a group of exponent two and R a Witt ring for G, it follows that $\mathfrak{A} = Z$ and thus $R_{red} \subset \mathbf{Z}^X$ for X the set of all homomorphisms from R to $\mathbf{Z}$. Hence in this case we obtain a split exact sequence of abelian groups

$$0 \to \operatorname{Nil} R \to R \to \mathbf{Z}^X.$$

In case $R = W(C, J)$ with C a formally real field and J the identity there is a bijection between the orderings of C and the minimal prime ideals, $\bar{P} = P/K$, of R [11], [22] and the map $R \to R/\bar{P} \cong \mathbf{Z}$ is given by attaching to each quadratic form over C its signature with regard to the ordering of C corresponding to $\bar{P}$ [11, 22]. The above exact sequence then reduces to [26, Satz 22], [22, Satz 2], [29, Th. 2.1].

If R is a Witt ring for G, the homomorphism of R to $\mathfrak{A}$ are induced by the ψ_χ of $\mathbf{Z}[G]$ to $\mathfrak{A}$ which vanish on K. Let ϕ denote such a homomorphism from R to $\mathfrak{A}$ then $\operatorname{Ker} \phi = P_\chi/K$ for some χ and it is clear that $\cap \operatorname{Ker} \phi = \operatorname{Nil} R$.

LEMMA 3.21. *Let R be a Witt ring for an abelian q-group G.*

(i) *All elements of the form $1 + y$ with y in $\operatorname{Nil} R$ are units of q-power order.*

(ii) *Let $R \neq R_t$. Then x in R is a unit of finite order if and only if for every homomorphism $\phi: R \to \mathfrak{A}$, the element $\phi(x)$ is a root of unity. If x is a unit of finite order then its order is of the form q^m or $2q^m$.*

(iii) *If $R = R_t$, all units have finite order nq^m with $n \mid q - 1$.*

Proof. (i) If y lies in $\operatorname{Nil} R$, there exist integers k and l with $y^k = q^l y = 0$ by Lemma 3.3 and Theorem 3.9. Since q is prime, the binomial coefficients $\binom{q^r}{i}$ are divisible by q for $0 < i < q$ and thus $(1 + y)^{q^r} = 1 + qx_r y + y^{q^r}$. Hence if $q^r > k$ we find $(1 + y)^{q^r} = 1 + qx_r y$. Now, an induction on l shows that for any w in R, $(1 + qw)^{q^l} = 1 + q^{l+1} w' w$ for w' in R. Therefore, if $q^r > k$ we have $(1 + y)^{q^{r+l-1}} = 1$.

(ii) If x is a unit of finite order it is clear that all its images $\phi(x)$ in $\mathfrak{A}$ are roots of unity. Since $\mathfrak{A}$ is the ring of integers of a (possible infinite) number field generated by q-power roots of unity, the roots of unity in $\mathfrak{A}$

have orders $2q^m$ or q^m [12, p. 536]. Now assume that for all $\phi: R \to \mathfrak{A}$ the element $\phi(x)$ is a root of unity. Since x is the image of an element $\sum a_i g_i$ in $\boldsymbol{Z}[G]$ and $\phi(x) = \sum a_i \chi(g_i)$ for some character χ, it is clear that there are only finitely many values that $\phi(x)$ can assume for a fixed x in R. Thus, taking the lowest common multiples of all the orders of the $\phi(x)$ there is an integer t of the form q^m or $2q^m$ with $(\phi(x))^t = 1$ for all $\phi: R \to \mathfrak{A}$. Hence $x^t - 1$ lies in $\cap \operatorname{Ker} \phi = \operatorname{Nil} R$. Thus $x^t = 1 + y$ in $\operatorname{Nil} R$ and so by (i) is a unit of q-power order.

(iii) In case $R_t = R$, Proposition 3.15 shows that $\operatorname{Nil} R = \bar{M}_0$. If x is a unit in R, the coset $x + \bar{M}_0$ is a unit in $R/\bar{M}_0 = \boldsymbol{F}_q$ and so $x^{q-1} = 1 + y$ in $\bar{M}_0 = \operatorname{Nil} R$. The proof is then completed by (i).

Remark 3.22. If $q = 2$ all the units of finite order of R have 2-power order. Furthermore, if G has exponent two, $\mathfrak{A} = \boldsymbol{Z}$ as was already noted in Remark 3.2. If $R_t \neq R$ and x is a unit in R, then $\phi(x) = \pm 1$ for all $\phi: R \to \mathfrak{A}$ and thus by Lemma 3.21(ii) *all* units of R have finite order. Keeping in mind Remark 3.20 for the case $R = W(C, J)$ with C a formally real field and J the identity, Lemma 3.21(ii) reduces to [26, Satz 24].

THEOREM 3.23. *Let $R \neq R_t$ be a Witt ring for an abelian group of exponent q. Let $\bar{g}$ denote the image of an element g of G in R. Then x in R is a unit of finite order if and only if $x = \pm \bar{g}(1 + y)$ with y in* $\operatorname{Nil} R$.

Proof. If $x = \pm \bar{g}(1 + y)$, then $x^{2q} = (1 + y)^{2q} = 1 + y'$ with y' in $\operatorname{Nil} R$, and so by Lemma 3.21(i), x is a unit of finite order.

To prove the converse it suffices to treat the case when $\operatorname{Nil} R = 0$. For, le x be a unit of finite order in R. If $x + \operatorname{Nil} R = \pm \tilde{g}$, where $\tilde{g}$ denotes thei mage of g in R_{red}, then $x = \pm \bar{g} + z$ with z in $\operatorname{Nil} R$. Thus $x = \pm \bar{g}(1 + \bar{g}^{-1} z)$. Hence we assume for the remainder of the proof that $\operatorname{Nil} R = 0$.

Since G has exponent q, the field $\mathfrak{Q}$ generated over $\boldsymbol{Q}$ by all $\chi(g)$ is the field of the q-th-roots of unity. Now the roots of unity of $\mathfrak{Q}$ have order dividing $2q$ if q is odd and order dividing 2 if $q = 2$ [12, p. 536]. It follows that for x a unit of finite order of $R = R_{red}$, we always have $x^{2q} = 1$ if q is odd and $x^2 = 1$ if $q = 2$, since $R \subset \prod \phi(R)$ where ϕ runs through all homomorphisms of R into $\mathfrak{A} \subset \mathfrak{Q}$. Thus for q odd, x has order 1, 2, q or $2q$, and for $q = 2$, the element x has order 1 or 2. In the former case a unit of order $2q$ is a product of a unit of order 2 and a unit of order q and since the set $\{\pm \bar{g}\}$ is multiplicatively closed, it clearly suffices to treat three cases: x a unit of order q with q odd, x a unit of order 2 with $q = 2$, and x a unit of order 2 with q odd.

Assume first that x has order q, an odd prime. Let $x = \sum a_i \bar{g}_i$ with a_i in $\boldsymbol{Z}$. We show that if $g = \prod g_i^{a_i}$ then $\bar{g} = x$. To prove this it suffices to show $\phi(\bar{g}) = \phi(x)$ for all $\phi: R \to \mathfrak{A}$ since $\cap \operatorname{Ker} \phi = \operatorname{Nil} R = 0$. Let ϕ be such a homomorphism and let ζ be a primitive q-th root of unity in $\mathfrak{Q}$. Let $\phi(x) = \zeta^m$ and $\phi(\bar{g}_i) = \zeta^{n_i}$ with $0 \leqq m, n_i \leqq q-1$. Then $\zeta^m = \sum a_i \zeta^{n_i}$. Now $1, \zeta, \cdots, \zeta^{q-2}$ are linearly independent over $\boldsymbol{Q}$ and $0 = \sum_0^{q-1} \zeta^j$. From this it easily follows that $\sum_0^{q-1} k_j \zeta^j = 0$ with k_j in $\boldsymbol{Q}$ implies $k_0 = k_1 = \cdots = k_{q-1} = k$. Thus, if k_j denotes the sum of the a_i for which $n_i = j$, there exists an integer k with $k_j = k$ if $j \neq m$ and $k_m - 1 = k$. Hence

$$\sum n_i a_i = k(0 + 1 + 2 + \cdots + q-1) + m = \frac{kq(q-1)}{2} + m.$$

Since q is odd this is congruent to m modulo q. Thus

$$\phi(\bar{g}) = \phi(\prod \bar{g}_i^{a_i}) = \zeta^{\sum n_i a_i} = \zeta^m = \phi(x).$$

Next, let $q = 2$. We put $x = b_1 + \cdots + b_n$ with $b_i = \pm \bar{g}_i$. Since for all $\phi: R \to \mathfrak{A} = \boldsymbol{Z}$, the b_i and x_i have value ± 1 we must have $n = 2l + 1$. For a fixed ϕ, we then renumber the b_i so that $\phi(b_i) = 1$, $i = 1, 2, \cdots, l$, and $\phi(b_i) = -1$, $i = l+1, l+2, \cdots, 2l$. Hence $\phi(b_{2l+1}) = \phi(x)$ which in turns yields $\phi(x) = \phi((-1)^l b_1 b_2 \cdots b_{2l+1})$ for all $\phi: R \to \mathfrak{A}$. Hence $x = (-1)^l b_1 b_2 \cdots b_{2l+1}$, an element of the form $\pm \bar{g}$.

Finally, let q be odd and suppose x has order 2. Since $\operatorname{Nil} R = R_t = 0$ we have $R \cong R \otimes 1$ embedded in $\boldsymbol{Q} \otimes R$. The element $\frac{x+1}{2} = z$ of $\boldsymbol{Q} \otimes R$ is readily verified to be idempotent and, therefore, lies in $\tilde{R}$, the integral closure of R in $\boldsymbol{Q} \otimes R$. But $2z$ lies in R and by Proposition 3.17, $\tilde{R}/R$ is a q-group. Thus z lies in R. Since R is a Witt ring for a q-group, Corollary 3.10 shows that $z = 0$ or 1. This forces $x = \pm 1$ which completes the proof of the theorem.

Remark 3.24. If $R = \boldsymbol{Z}[G]$, for G an abelian group of exponent q, Theorem 3.23 is a special case of [13, p. 237] which asserts that if V is a ring of algebraic integers and G an abelian torsion group, the units of the group ring $V[G]$ of finite order all have the form ϵg with ϵ a unit of V.

UNIVERSITÄT DES SAARLANDES, SAARBRÜCKEN, WEST GERMANY,
CORNELL UNIVERSITY,
AND
NORTHWESTERN UNIVERSITY.

REFERENCES.

[1] H. Bass, "Lectures on topics in algebraic K-theory," *Tata Inst. Fund. Res.*, Bombay, 1967.

[2] ———, *Algebraic K-theory*, Benjamin, New York, 1968.

[3] A. A. Belskii, "Cohomological Witt rings," *Math. USSR-Izvestija*, vol. 2 (1968), pp. 1101-1115.

[4] N. Bourbaki, *Algèbre*, Chap. 2, 3rd ed., Act. Sc. Ind. 1236, Hermann, Paris, 1962.

[5] ———, *Algèbre*, Chap. 9, Act. Sc. Ind. 1272, Hermann, Paris, 1959.

[6] ———, *Algèbre commutative*, Chap. 1-2, Act. Sc. Ind. 1290, Hermann, Paris, 1961.

[7] ———, *Algèbre commutative*, Chap. 5, Act. Sc. Ind. 1308, Hermann, Paris, 1964.

[8] H. Cartan and S. Eilenberg, *Homological algebra*, Princeton University Press, Princeton, 1956.

[9] A. Delzant, "Définition des classes de Stiefel-Whitney d'un module quadratique de characteristique differente de 2," *C. R. Acad. Sc. Paris*, vol. 255 (1962), pp. 1366-1368.

[10] A. Fröhlich and A. M. McEvett, "Forms over rings with involution," *Journal of Algebra*, vol. 12 (1969), pp. 79-104.

[11] D. K. Harrison, "Witt rings," Lecture notes, Department of Mathematics, University of Kentucky, Lexington, Kentucky, 1970.

[12] H. Hasse, *Zahlentheorie*, 2. erweiterte Auflage, Akademie Verlag, Berlin, 1963.

[13] Graham Higman, "The units of group rings," *Proceedings of the London Mathematical Society* (2), vol. 46 (1940), pp. 231-248.

[14] I. Kaplansky, *Fields and rings*, The University of Chicago Press, Chicago, 1969.

[15] ———, *Commutative rings*, Allyn and Bacon, Boston, 1970.

[16] M. Knebusch, *Grothendieck- und Wittringe von nichtausgearteten symmetrischen Bilinearformen*, Sitzber. Heidelberg Akad. Wiss. 1969/1970, pp. 93-157.

[17] ———, "Runde Formen über semi-lokalen Ringen," *Mathematische Annalen*, vol. 193 (1971), pp. 21-34.

[18] M. Knebusch, A. Rosenberg and R. Ware, "Structure of Witt rings, quotients of abelian group rings, and orderings of fields," *Bulletin of the American Mathematical Society*, vol. 77 (1971), pp. 205-210.

[19] ———, "Signatures on semi-local rings," to appear in *Journal of Algebra*.

[20] ———, "Grothendieck and Witt rings of hermitian forms over Dedekind rings," to appear in *Pacific Journal of Mathematics*.

[21] M. Knebusch and W. Scharlau, "Über das Verhalten der Witt-Gruppe bei galoischen Körpererweiterungen," *Mathematische Annalen*, vol. 193 (1971), pp. 189-196.

[22] J. Leicht and F. Lorenz, "Die Primideale des Wittschen Ringes," *Invent. Math.*, vol. 10 (1970), pp. 82-88.

[23] F. Lorenz, "Quadratische Formen über Körpern," Springer Lecture Notes 130, 1970.

[24] H. Matsumura, *Commutative algebra*, Benjamin, New York, 1970.

[25] G. Nöbeling, "Verallgemeinerung eines Satzes von Herrn E. Specker," *Invent. Math.*, vol. 6 (1968), pp. 41-55.

[26] A. Pfister, "Quadratische Formen in beliebigen Körpern," *Invent. Math.*, vol. 1 (1966), pp. 116-132.

[27] A. Rosenberg and R. Ware, "The zero-dimensional Galois cohomology of Witt rings," *Invent. Math.*, vol. 11 (1970), pp. 65-72.

[28] W. Sharlau, "Quadratische Formen und Galois-Cohomologie," *Invert. Math.*, vol. 4 (1967), pp. 238-264.

[29] ———, "Induction theorems and the structure of the Witt group," *Invent. Math.*, vol. 11 (1970), pp. 37-44.

[30] ———, "Quadratic forms," *Queen's paper in pure and applied mathematics*, No. 22, Queen's University, Kingston, Ontario, 1969.

[31] E. Witt, "Theorie der quadratischen Formen in beliebigen Körpern, *J. Reine Angew. Math.*, vol. 176 (1937), pp. 31-44.

Corrections.

p. 120, line -5: Interchange "ring" and "purely"
p. 127, line 4 of Lemma 1.11: tilde is omitted from a capital phi. Also the tildes are too small.
p. 131, line 12: There should be no apostrophe on x_2 in the braces.
p. 132, line -10: A tilde is omitted on B_i
p. 133, line 2: The italic "O" should be Roman.
p. 140: It is hard to tell the difference between the R's with a tilde on top and a bar on top.
p. 146, line 3 of Proof of Theorem 3.9: "Oniy" should be "Only"
p. 146, line -3: "a" at the end of the line should be deleted
p. 147, line 7: The bar beside the P at the beginning of the line should be over the P.
p. 150, line -1: "Nite" should be "finite"
p. 151, line 15: "homomorphism" should be plural
p. 151, line -7: It should read "q^r" not "q" in "$0 < i < q$"
p. 152, line -15: "le" should be "let"
p. 152, line -14: "thei mge" should be "the image"