7815362

HERSHBERGER, BESSIE LOU
ORTHOGONAL GEOMETRY OVER RINGS WITH STABILITY
CONDITIONS.

THE UNIVERSITY OF OKLAHOMA, PH.D., 1977

THE UNIVERSITY OF OKLAHOMA

GRADUATE COLLEGE

ORTHOGONAL GEOMETRY OVER RINGS WITH STABILITY CONDITIONS

A DISSERTATION

SUBMITTED TO THE GRADUATE FACULTY

in partial fulfillment of the requirements for the

degree of

DOCTOR OF PHILOSOPHY

BY

BESSIE LOU HERSHBERGER

Norman, Oklahoma

1977

ORTHOGONAL GEOMETRY OVER RINGS WITH STABILITY CONDITIONS

APPROVED BY

Robert A Morris

A B Schwarzkopf

Stanley B. Eliason

Harold V. Huneke

DISSERTATION COMMITTEE

ACKNOWLEDGEMENTS

I would like to express gratitude to Dr. Bernard R. McDonald for his guidance, invaluable suggestions and kind encouragement during the writing of this dissertation.

TABLE OF CONTENTS

ORTHOGONAL GEOMETRY OVER RINGS WITH STABILITY CONDITIONS

CHAPTER I

INTRODUCTION

Historically, H. Bass described a "stable range condition" on a ring and when the stable range is 1, he was able to classify completely the normal subgroups of the general linear group in any dimension. In contrast, the study of the orthogonal group and the Witt ring over a general coefficient ring has progressed slowly through increasingly more general rings, e.g., first fields, then local rings, then semilocal rings. Our approach was to discover an equational condition analogous to stable range which would allow duplication of the classical results.

In Chapter II, a ring is defined to be _full_, _of type_ ⟨m,n⟩, if it satisfies certain polynomial-type conditions. Examples of rings which are ⟨m,n⟩-full are shown to include large enough fields, semi-local rings whose residue fields are full of type ⟨m,n⟩, and von Neumann regular rings. We show that every commutative ring can be embedded in an ⟨m,n⟩-full ring.

Chapter III concerns inner product spaces over a ring R which is full of type ⟨1,3⟩ and has 2 a unit. We show that such an inner product space always has an orthogonal basis and that Witt Cancellation holds. For a space with hyperbolic rank $\geqslant 1$, we determine generators of the orthogonal group and show that the Eichler subgroup equals the commutator subgroup of the orthogonal group.

Chapter IV deals with the normal subgroups of the orthogonal group $O(V)$ where V is a free symmetric inner-product space over a $\langle 1,3\rangle$-full ring R and V has hyperbolic rank $\geqslant 1$. The main result is that G is a normal subgroup of $O(V)$ if and only if there is an ideal A of R with $\Omega(V,A) \leq G \leq O(V,A)$.

The final chapter defines the Witt ring $W(R)$ of free symmetric inner product spaces over a $\langle 1,3\rangle$-full ring R having 2 a unit. Generators and relations of $W(R)$ are given and its prime ideals are classified. For a ring which is full of type $\langle 3,3\rangle$ and has 2 a unit, we show using round forms that the generators of the torsion part of the Witt ring have the form $(1,-a)$ where a is a unit and a sum of squares.

Throughout, rings are commutative with identity. Let R^* denote the group of units of a ring R.

CHAPTER II

RING THEORETIC RESULTS

In this chapter, equational conditions on a ring are defined which allow the development of the theory of free symmetric inner product spaces, the orthogonal group, and the Witt ring. Examples of rings which satisfy these conditions are shown to include "sufficiently large" fields, semi-local rings with "large enough" residue fields, and von Neumann regular rings.

(II.1) Definition. Let m be an integer $\geqslant 1$ and n an integer $\geqslant 2$. A ring R is full of type $\langle m,n\rangle$, or $\langle m,n\rangle$-full, if for every $m \times n$ matrix $A = [a_{ij}]$ over R with unimodular rows, there exist an α in R (dependent on A) and units $u_1, u_2, \cdots, u_m$ of R such that

$$A\begin{bmatrix} 1 \\ \alpha \\ \alpha^2 \\ \vdots \\ \alpha^{n-1} \end{bmatrix} = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_m \end{bmatrix} .$$

Rings of the above type have "many" units, i.e., are "full" of units--hence the terminology.

R is strongly full of type $\langle m,n\rangle$ if α may be chosen to be a unit.

Finally, R is (strongly) full if R is (strongly) full of type $\langle m,n\rangle$ for all positive integers m, n. (This generalizes the definition of a full ring used in [29].) Certainly any strongly full ring is full.

To illustrate the definition, we will consider some specific types of fullness and indicate the types of results they give.

(1) Suppose R is full of type $\langle 1,2\rangle$. Then for any two elements a, b of R such that the ideal generated by a and b is all of R (the notation for this is $(a,b) = R$), there exists an α in R with $a + \alpha b$ a unit. This is Bass's definition of stable range 1 (see [7]). Bass showed in [7] that for a free module V over a ring with stable range 1 (i.e., a ring which is full of type $\langle 1,2\rangle$), the normal subgroup structure of GL(V) behaves in the classical fashion.

(2) Suppose R is full of type $\langle 1,3\rangle$. Then for three elements a, b, c of R such that $(a,b,c) = R$, there is an element α of R with $a + b\alpha + c\alpha^2$ a unit. We show this condition is sufficient to insure that every free inner product space over R has an orthogonal basis, Witt cancellation holds, generators and relations for the Witt ring over R are known, and if hyperbolic rank $\geqslant 1$, then the Eichler subgroup is equal to the commutator subgroup of the orthogonal group.

(3) Suppose R is strongly full of type $\langle 1,3\rangle$. Then for any three elements a, b, c of R such that $(a,b,c) = R$, there is a unit α in R satisfying $a + b\alpha + c\alpha^2$ is a unit. For a free module V over R, where R is of type $\langle 1,3\rangle$, with certain additional hypotheses, we show the normal subgroups of O(V), the orthogonal group of V, are nested between congruence subgroups.

(4) Suppose R is full of type $\langle 3,3\rangle$. This says that if $[a_{ij}]_{3\times 3}$ is a matrix over R with $(a_{11},a_{12},a_{13}) = (a_{21},a_{22},a_{23})$

$= (a_{31},a_{32},a_{33}) = R$, then there is an α in R such that $a_{11} + a_{12}\alpha + a_{13}\alpha^2$, $a_{21} + a_{22}\alpha + a_{23}\alpha^2$, and $a_{31} + a_{32}\alpha + a_{33}\alpha^2$ are all units. We show this condition is enough to determine generators of the torsion part of the Witt ring.

Certain relations between types of fullness should be noted:

Any ring which is full of type $\langle m,n\rangle$ is full of type $\langle s,t\rangle$ for $1 \leq s \leq m$, $1 \leq t \leq n$.

A ring R is called <u>n-stable</u> for a positive integer n if for every set of n + 1 elements $\alpha, \beta_1, \beta_2, \cdots, \beta_n$ in R with $(\alpha,\beta_1,\cdots,\beta_n) = R$, then there exist $\omega_1,\cdots,\omega_n$ in R with $\alpha + \beta_1\omega_1 + \cdots + \beta_n\omega_n = \text{unit}$. A ring R is <u>stable</u> if R is n-stable for every $n \geqslant 1$. It is straightforward to check that if R is 1-stable, then R is n-stable for $n \geqslant 1$, and if R is n-stable then R is m-stable for $1 \leq m \leq n$. Thus, 1-stable implies stable. Clearly, if R is $\langle 1,3\rangle$-full, then R is 1-stable, hence R is stable.

The following lemma gives a useful equivalent condition to $\langle 1,3\rangle$-full.

(II.2) <u>Lemma</u> R is $\langle 1,3\rangle$-full if and only if for any set of 2n + 1 elements $\alpha, \beta_1, \cdots, \beta_n, \delta_1, \cdots, \delta_n$ in R with $(\alpha,\beta_1,\cdots,\beta_n,\delta_1,\cdots,\delta_n) = R$, there exist $\omega_1,\omega_2,\cdots,\omega_n$ in R with

$$\alpha + \beta_1\omega_1 + \beta_2\omega_2 + \cdots + \beta_n\omega_n + \delta_1\omega_1^2 + \cdots + \delta_n\omega_n^2 = \text{unit}.$$

<u>Proof</u> One direction is trivial. So suppose $(\alpha,\beta_1,\cdots,\beta_n,\delta_1,\cdots,\delta_n) = R$. Then for suitable $a, b_1,\cdots, b_n, d_1,\cdots, d_n$, $a\alpha + \sum b_i\beta_i + \sum d_i\delta_i = 1$. Since R is $\langle 1,3\rangle$-full, it is stable, so there is a $\bar{b}$ in R with $\alpha + \bar{b}(\sum_i b_i\beta_i + \sum_i d_i\delta_i) = \text{unit}$.

Let $\hat{b}_i = \bar{b}b_i$, $\hat{d}_i = \bar{b}d_i$. Then

$$(\alpha + \sum_{i=1}^{n-1} \hat{b}_i\beta_i + \sum_{i=1}^{n-1} \hat{d}_i\delta_i) + \hat{b}_n\beta_n + \hat{d}_n\delta_n = \text{unit}.$$

Since R is $\langle 1,3\rangle$-full, there is an element, say ω_n, with

$$[\alpha + \sum_{i=1}^{n-1} (\hat{b}_i\beta_i + \hat{d}_i\delta_i)] + \omega_n\beta_n + \omega_n{}^2\delta_n = \text{unit}.$$

Now reassociate, and repeat the argument on $\hat{b}_{n-1}\beta_{n-1} + \hat{d}_{n-1}\delta_{n-1}$ to manufacture ω_{n-1}. After n steps, we have $\omega_1,\cdots,\omega_n$ with $\alpha + \sum\beta_i\omega_i + \sum\delta_i\omega_i{}^2$ = unit.

A minor application of (II.2) is the following lemma which in turn will be applied in (III.6).

(II.3) <u>Lemma</u> Let R be a ring which is full of type $\langle 1,3\rangle$ and let A be a proper ideal of R. Then R/A is full of type $\langle 1,3\rangle$.

<u>Proof</u> Let $\bar{x}$ denote the image of x under the canonical mapping R → R/A. Suppose $(\bar{x},\bar{y},\bar{z})$ = R/A. Then there exist $\bar{a}$, $\bar{b}$, $\bar{c}$ in R/A such that $\bar{a}\bar{x} + \bar{b}\bar{y} + \bar{c}\bar{z} = \bar{1}$. This implies that there is a k in A with ax + by + cz - k = 1. Thus (x,y,k,z,k) = R. By (II.2) there exist ω_1, ω_2 in R such that $x + \omega_1 y + \omega_2 k + \omega_1{}^2 z + \omega_2{}^2 k = v$ a unit in R. Then $\bar{x} + \bar{\omega}_1\bar{y} + \bar{\omega}_2\bar{k} + \bar{\omega}_1{}^2\bar{z} + \bar{\omega}_2{}^2\bar{k} = \bar{x} + \bar{\omega}_1\bar{y} + \bar{\omega}_1^2\bar{z} = \bar{v}$. Since v is a unit, $\bar{v}$ is a unit.

Now some examples of some types of full rings will be given. Since the class of full rings of type $\langle m,n\rangle$ is defined equationally, we have the following result.

(II.4) <u>Proposition</u> (a) If R_λ is (strongly) full of type $\langle m,n\rangle$ for each λ in an index set Λ, then the product $\prod_\lambda R_\lambda$ is (strongly) full of type $\langle m,n\rangle$.

(b) If $\{R_\lambda\}$ is a directed system of (strongly) full rings of type $\langle m,n\rangle$, then the direct limit $\varinjlim R_\lambda$ is (strongly) full of type $\langle m,n\rangle$.

As an application of (II.4) we have: If each finitely generated subring S of R is contained in some (strongly) full subring of type $\langle m,n\rangle$, then R (being a direct limit of such rings) is (strongly) full of type $\langle m,n\rangle$.

(II.5) Proposition Let R be (strongly) $\langle m,n\rangle$-full where $n \geqslant 2$ and let A be a proper ideal of R. Then

(a) R/A is (strongly) full of type $\langle m,n-1\rangle$.

(b) The canonical ring morphism π: $R \to R/A$ induces a surjective group morphism $R^* \to (R/A)^*$. Indeed, $R^* \to (R/A)^*$ is surjective for every A if and only if 1 is in the stable range of R, i.e., R is $\langle 1,2\rangle$-full.

Proof Let $[\bar{a}_{ij}]$ be an m x (n-1) matrix over R/A having unimodular rows. There are $\bar{r}_{ij}$ in R/A with

$$\textstyle\sum_{j=1}^{n-1} \bar{r}_{ij}\bar{a}_{ij} = \bar{1} \qquad (1 \leq i \leq m)$$

Let r_{ij} and a_{ij} be in R with $r_{ij} \to \bar{r}_{ij}$ and $a_{ij} \to \bar{a}_{ij}$ under the canonical morphism $R \to R/A$. Then, there exist $a_1,\cdots,a_m$ in A with

$$\textstyle\sum_{j=1}^{n-1} r_{ij}a_{ij} + a_i = 1, \qquad (1 \leq i \leq m).$$

Thus

$$\begin{bmatrix} a_{11} & \cdots & a_{1,n-1} & a_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \cdots & a_{m,n-1} & a_m \end{bmatrix}$$

has unimodular rows. Since R is full of type $\langle m,n\rangle$, there is an α with

$$\sum_{j=1}^{n-1} a_{ij}\alpha^{j-1} - a_1\alpha^{n-1} = v_i \qquad (1 \leqslant i \leqslant m)$$

where v_i is a unit. If $\alpha \to \bar{\alpha}$ under $R \to R/A$, then $\sum_{j=1}^{n-1} \bar{a}_{ij}\bar{\alpha}^{j-1} = \bar{v}_i$, where $\bar{v}_i$ is a unit in R/A. This gives (a).

(b) Let $\bar{u}$ be a unit in R/A. Then there is a $\bar{v}$ in R/A with $\bar{u}\bar{v} = 1$. Let u and v be preimages for $\bar{u}$ and $\bar{v}$, respectively, under $R \to R/A$. For some a in A, uv + a = 1. Since (u,a) = R and R is stable, there is an element b of R with u + ba = w and w is a unit. Then if $w \to \bar{w}$ under $R \to R/A$, $\bar{w}$ is a unit, and $\bar{w} = \bar{u} + \bar{b}\bar{a} = \bar{u}$.

(II.6') Proposition A field k with more than m(n-1) elements is $\langle m,n \rangle$-full.

Proof. Suppose $[a_{ij}]$ is an $m \times n$ matrix over k with a non-zero entry in each row. In order for all m entries of $[a_{ij}][1, \alpha, \alpha^2, \cdots, \alpha^{n-1}]^t$ to be non-zero, α cannot be a zero of any of the m polynomials $a_{i1} + a_{i2}X + \cdots + a_{in}X^{n-1}$. A polynomial of degree n - 1 over a field has at most n - 1 zeroes. Thus, there are at most m(n - 1) elements of k which will not meet the requirement for α.

In particular, (II.6) says that a field with 2 a unit is full of type $\langle 1,3 \rangle$, and a field where 2, 3 and 5 are units is full of type $\langle 3,3 \rangle$. Obviously, an infinite field is full.

(II.7) Theorem Let Rad(R) denote the Jacobson radical of R and let A be an ideal of R contained in Rad(R). If R/A is $\langle m,n \rangle$-full, then R is $\langle m,n \rangle$-full.

Proof Let $[a_{ij}]$ be an $m \times n$ matrix over R with unimodular rows. Let π: $R \to R/A$ be the canonical map. Since R/A is $\langle m,n \rangle$-full, there is an $\bar{\alpha}$ in R/A with

$$[\pi(a_{ij})][1, \bar{\alpha}, \cdots, \bar{\alpha}^{n-1}]^t = [\bar{u}_1, \bar{u}_2, \cdots, \bar{u}_m]^t$$

where $\bar{u}_i$ is a unit, $1 \leqslant i \leqslant m$. Let $\alpha, u_1, \cdots, u_m$ be in R with $\pi(\alpha) = \bar{\alpha}$, $\pi(u_i) = \bar{u}_i$. Then

$$[a_{ij}][1, \alpha, \cdots, \alpha^{n-1}]^t = [u_1 + j_1, \cdots, u_m + j_m]^t$$

where j_i is in A, $1 \leqslant i \leqslant m$. Since $\pi(u_i) = \bar{u}_i$ is a unit, there exist y_i in R and t_i in A with $(u_i + j_i)y_i = 1 + t_i$, $1 \leqslant i \leqslant m$. Since $1 + t_i$ is a unit for each i, $u_i + j_i$ is a unit.

Corollary A semi-local ring R having $|R/M| \geqslant m(n - 1)$ for each maximal ideal M is $\langle m,n \rangle$-full.

Proof $R/\text{Rad}(R) = \prod R/M$ where the product runs over the finitely-many maximal ideals of R. Applying (II.6) and (II.7) gives the result.

Note, in particular, that a semi-local ring with 2 a unit is full of type $\langle 1,3 \rangle$, and if 2, 3 and 5 are units, it is full of type $\langle 3,3 \rangle$.

We next show that von Neumann regular rings are full of type $\langle 1,3 \rangle$ (or type $\langle m,n \rangle$ for larger m and n when certain additional hypotheses are given) and thus also stable. This involves the Pierce representation of a von Neumann ring as a ring of cross-sections of a sheaf of fields over a Boolean space. (See [33], pp. 4-41.)

(II.9) Theorem The ring of cross-sections of a sheaf of $\langle m,n \rangle$-full rings over a Boolean space is $\langle m,n \rangle$-full.

Proof Let Σ be a sheaf of full rings over a Boolean space X. Let R denote the ring of cross-sections. Suppose $[\sigma_{ij}]$ is an $m \times n$ matrix over R with $(\sigma_{i1},\sigma_{i2},\cdots,\sigma_{in}) = R$ for each i, $1 \leqslant i \leqslant m$. Then there exist $\beta_{i1}, \beta_{i2}, \cdots, \beta_{in}$ in R with $\sum_{j=1}^{n} \beta_{ij}\sigma_{ij} = 1$. Then, for each point x in the base space X, $\sum_{j=1}^{n} \beta_{ij}(x)\sigma_{ij}(x) = 1_x$ in the stalk R_x above x. That is, $(\sigma_{i1}(x), \sigma_{i2}(x), \cdots, \sigma_{in}(x)) = R_x$ for each i. Since R_x is $\langle m,n \rangle$-full, there is an α_x in R_x with

$$[\sigma_{ij}(x)][1, \alpha_x, \cdots, \alpha_x^{n-1}]^t = [u_{1x}, u_{2x}, \cdots, u_{mx}]^t,$$

where u_{ix} is a unit in R_x, $(1 \leqslant i \leqslant m)$.

By 3.2(b) and Lemma 3.3 of [33], there exist τ, u_i and v_i in R with $\tau(x) = \alpha_x$, $u_i(x) = u_{ix}$ and $v_i(x) = u_{ix}^{-1}$. Then

$$(v_i(\sigma_{i1} + \sigma_{i2}\tau + \sigma_{i3}\tau^2 + \cdots + \sigma_{in}\tau^{n-1}))(x) = 1_x$$

and by 3.2(e) of [33] there is an open neighborhood N_{ix} of x in X such that

$$(v_i(\sigma_{i1} + \sigma_{i2}\tau + \cdots + \sigma_{in}\tau^{n-1})(y) = 1_y$$

for all y in N_{ix}. Let $N_x = \bigcap_{i=1}^{n} N_{ix}$. Then

$$(v_i(\sigma_{i1} + \sigma_{i2}\tau + \cdots + \sigma_{in}\tau^{n-1}))(y) = 1_y \quad \text{for all } i$$

and for all y in N_x. The family $\{N_x\}_{x \in X}$ cover X and by the partition property there is a finite disjoint subcollection of open-closed subsets which cover X. By patching together the appropriate sections above each of these sets, we obtain a $\bar{\tau}$ in R with

$$\sigma_{ij} + \sigma_{i2}\bar{\tau} + \cdots + \sigma_{in}\bar{\tau}^{n-1} = \text{unit} \quad \text{for each } i$$

That is, $[\sigma_{ij}][1,\bar{\tau},\bar{\tau}^2,\cdots,\bar{\tau}^{n-1}]^t$ is a column of units.

Using the fact that a von Neumann regular ring may be represented as the ring of cross sections of a sheaf of fields over a Boolean space gives the following corollaries.

(II.10) Corollary A von Neumann regular ring having 2 a unit is full of type $\langle 1,3\rangle$.

(II.11) Corollary A von Neumann regular ring with 2, 3, and 5 being units is full of type $\langle 3,3\rangle$.

(II.12) Theorem A zero-dimensional ring having 2 a unit is full of type $\langle 1,3\rangle$. A zero-dimensional ring in which 2, 3, and 5 are units is full of type $\langle 3,3\rangle$.

Proof Goodearl and Warfield in [16] show that a commutative ring R is zero-dimensional if and only if Rad(R) is nil and R/Rad(R) is von Neumann regular. Combining (II.7) with (II.11) gives the theorem.

For an example of a ring which is not stable, hence not full of type $\langle m,n\rangle$ for any $m \geqslant 1$, $n \geqslant 2$, consider R[X], the polynomial ring over a commutative ring R. Let $\alpha = 1 + X$ and $\beta = X^2$. Then $(\alpha,\beta) = R[X]$ since $1 = (1 + X)(1 - X) + X^2$. However, by checking degrees, there is no polynomial f with $(1 + X) + X^2 f$ a unit in R[X].

On the other hand, we have the following

(II.13) Proposition If R is full of type $\langle m,n\rangle$, then the formal power series, R[[X]], is full of type $\langle m,n\rangle$.

Proof Let $[f_{ij}]$ be an $m \times n$ matrix over R[[X]] with $(f_{i1},f_{i2},\cdots,f_{in}) = R[[X]]$ for $1 \leqslant i \leqslant m$. Then there are α_{ij}, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, in R[[X]] with $\alpha_{i1}f_{i1} + \alpha_{i2}f_{i2} + \cdots + \alpha_{in}f_{in} = 1$. Then $1 = \alpha^o_{i1}f^o_{i1} + \alpha^o_{i2}f^o_{i2} + \cdots + \alpha^o_{in}f^o_{in}$, where α^o_{ij} is the constant coefficient of α_{ij}, etc. That is, $[f^o_{ij}]$ is an $m \times n$ matrix over R with unimodular rows. Since R is $\langle m,n\rangle$-full, there is an α in R with

$$[f^o_{ij}][1,\alpha,\alpha^2,\cdots,\alpha^{n-1}]^t = [u_1,u_2,\cdots,u_m]^t$$

where u_i is a unit, $1 \leqslant i \leqslant m$. Then α and u_i are elements of R[[X]] and

$$[f_{ij}][1,\alpha,\alpha^2,\cdots,\alpha^{n-1}] = [g_1,g_2,\cdots,g_m]^t$$

where g_i has u_i for its constant coefficient. Since a power series is a unit if and only if its constant coefficient is a unit, each g_i is a unit.

As the following examples will show, the requirement that R be strongly full of type $\langle m,n\rangle$ is not much more stringent than requiring the ring to be full of type $\langle m,n\rangle$.

(II.14) Proposition A field k with more than $m(n - 1) + 1$ elements is strongly full of type $\langle m,n\rangle$.

Proof In the proof of (II.6), the additional choice $\alpha = 0$ now must be avoided.

(II.15) Corollary A field such that both 2 and 3 are units is strongly full of type $\langle 1,3\rangle$.

(II.16) Theorem If R/Rad(R) is strongly full of type $\langle m,n\rangle$, then R is strongly full of type $\langle m,n\rangle$.

Proof Let π: $R \to R/\mathrm{Rad}(R)$ be the canonical map. Suppose $[a_{ij}]$ is an $m \times n$ matrix over R with unimodular rows. Then $[\pi a_{ij}]$ is an $m \times n$ matrix over R/Rad(R) with unimodular rows. There exists a unit $\bar{\alpha}$ of R/Rad(R) with $[\pi a_{ij}][1,\bar{\alpha},\bar{\alpha}^2,\cdots,\bar{\alpha}^{n-1}]^t = [\bar{u}_1,\bar{u}_2,\cdots,\bar{u}_m]^t$ where $\bar{u}_i$ is a unit, $1 \leqslant i \leqslant m$. Since the morphism $R^* \to (R/\mathrm{Rad}(R))^*$ induced by π is surjective, there is a unit α in R with $\pi(\alpha) = \bar{\alpha}$. Thus

$$[a_{ij}][1,\alpha,\cdots,\alpha^{n-1}]^t = [u_1 + j_1,\cdots,u_m + j_m]^t$$

where u_i is in R and j_i is in Rad(R). Now $\pi(u_i + j_i) = \bar{u}_i$ is a unit in

R/Rad(R) implies there is an x_i in R with $(u_i + j_i)x_i = 1 + t_i$, for some t_i in Rad(R). Since $1 + t_i$ is a unit, $u_i + j_i$ is a unit for each i, and the proof is done.

(II.17) Corollary A semi-local ring R having $|R/M| \geqslant m(n - 1) + 1$ for each maximal ideal M is strongly full of type $\langle m,n\rangle$.

In particular, a semi-local ring in which 2 and 3 are both units is strongly full of type $\langle 1,3\rangle$.

(II.18) Theorem Let Σ be a sheaf of rings, each of which is strongly full of type $\langle m,n\rangle$, over a Boolean space. The ring of cross sections of Σ is strongly full of type $\langle m,n\rangle$.

Proof The proof is only a little more detailed than the proof of (II.9). Let R denote the ring of cross sections. Suppose $[\sigma_{ij}]$ is an $m \times n$ matrix over R with unimodular rows. Then there exist β_{ij}, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, in R with $\sum_{j=1}^{n} \beta_{ij}(x)\sigma_{ij}(x) = 1_x$ in the stalk R_x above x, for each point x in X. That is, $[\sigma_{ij}(x)]$ is an $m \times n$ matrix over R_x with unimodular rows. Then there exists a unit α_x in R_x, with

$$[\sigma_{ij}(x)][1,\alpha_x,\cdots,\alpha_x^{n-1}]^t = [u_{1x},u_{2x},\cdots,u_{mx}]^t,$$

where u_{ix} is a unit in R_x, $1 \leqslant i \leqslant m$. By 3.2(b) and Lemma 3.3 of [33], there exist σ, τ, u_i, v_i in R with $\tau(x) = \alpha_x$, $\sigma(x) = \alpha_x^{-1}$, $u_i(x) = u_{ix}$ and $v_i(x) = u_{ix}^{-1}$. Then $(v_i(\sigma_{i1} + \sigma_{i2}\tau + \cdots + \sigma_{in}\tau^{n-1}))(x) = 1_x$ and $\sigma\tau(x) = 1_x$. By 3.2(e) of [33] there is an open neighborhood N_{ix} of x in X such that $(v_i(\sigma_{i1} + \sigma_{i2}\tau + \cdots + \sigma_{in}\tau^{n-1}))(y) = 1_y$ for all y in N_{ix}, and there is an open neighborhood O_x of x such that $\sigma\tau(y) = 1_y$ for all y in O_x. Let $N_x = \bigcap_{i=1}^{m} N_{ix} \cap O_x$. Then

$$(v_i(\sigma_{i1} + \sigma_{i2}\tau + \cdots + \sigma_{in}\tau^{n-1}))(y) = 1_y$$

and $\sigma\tau(y) = 1_y$ for all i and for all y in N_x. The family $\{N_x\}_{x \in X}$ cover X and by the partition property there is a finite disjoint subcollection of open-closed subsets which cover X. By patching together the appropriate sections above each of the sets, we obtain $\bar{\tau}$ and $\bar{\sigma}$ in R with $\sigma_{i1} + \sigma_{i2}\bar{\tau} + \cdots + \sigma_{in}\bar{\tau}^{n-1}$ = unit for each i, and $\bar{\tau}\bar{\sigma} = 1$. That is, $\bar{\tau}$ is a unit and $[\sigma_{ij}][1,\bar{\tau},\cdots,\bar{\tau}^{n-1}]^t$ is a column of units.

(II.19) Corollary A von Neumann regular ring in which 2 and 3 are units is strongly full of type $\langle 1,3\rangle$.

(II.20) Corollary A zero-dimensional ring in which 2 and 3 are units is strongly full of type $\langle 1,3\rangle$.

(II.21) Proposition If R is strongly full of type $\langle m,n\rangle$, then R[[X]] is strongly full of type $\langle m,n\rangle$.

Proof The proof is nearly identical to the proof of (II.10) and will be omitted.

Let R be any commutative ring. If $f = \sum_{i=0}^{n} a_i X^i$ is in R[X], the content of f = c(f) = $(a_o, a_1, \cdots, a_n)$. f is primitive if c(f) = R. Let S denote the set of primitive polynomials in R[X]. Then ([32], pp. 17-18) S is a multiplicatively closed subset of R[X] containing no zero divisors. Let R(X) denote $S^{-1}R[X]$.

(II.22) Theorem Let R be a commutative ring, and let $m \geqslant 1$, $n \geqslant 2$, be integers. Then R(X) is strongly full of type $\langle m,n\rangle$.

Proof Let $A = [f_{ij}]$ be an m × n matrix over R(X) with unimodular rows. By "clearing denominators" of units (which will not affect calculations), we may assume all f_{ij} are in R[X]. There exist g_{ij} and h_{ij} in R[X] with

$$\sum_{j=1}^{n} \frac{g_{ij}}{h_{ij}} f_{ij} = 1$$

in R(X). Thus

$$\sum_j (\prod_{k\neq j} h_{ik}) g_{ij} f_{ij} = \prod_j h_{ij}.$$

Then the content $c(\prod_j h_{ij}) = \prod_j c(h_{ij}) = R$. So $\prod_j h_{ij}$ is a unit in R(X). Let $m_{ij} = \deg(f_{ij})$ for each i, j. Let s be any integer with $s > 2 \max_{i,j}\{m_{ij}\}$. Consider

$$g_i = f_{i1} + f_{i2}X^s + \cdots + f_{in}(X^s)^n.$$

The coefficients of g_i will be a union of the coefficients of $\{f_{ij}: j = 1,\cdots,n\}$. By the above, $c(g_i) = R$. Hence g_i is a unit for each i. X^s is also a unit in R(X), and the proof is complete.

(II.23) Corollary Every commutative ring is a subring of a strongly full ring of type ⟨m,n⟩ for any $m \geqslant 1$, $n \geqslant 2$.

Proof Observe $R \subset R(X)$ and apply (II.22).

This chapter is concluded with a condition on a commutative ring which seems to have no connection with the fullness conditions, but which is possessed by zero-dimensional rings in which 2 and 3 are units. The condition is useful in the normal subgroup theory of the orthogonal group.

(II.24) Definition A ring R is square representable if every element of R can be written as a sum of squares of units and negatives of squares of units, i.e., for any r in R, there exists a finite set of units

$u_1, u_2, \cdots, u_n$ such that $r = \sum_{i=1}^{n} (-1)^{k_i} u_i^2$ where $k_i \in \{0,1\}$.

Observe that in a field k with $2 \neq 0$, any element η, $\eta \neq 0, 2$, may be expressed as the sum of two squared units minus a squared unit: $\eta = (\eta/2)^2 + 1 - \left(\frac{\eta}{2} - 1\right)^2$. If $3 \neq 0$, $2 = 2^2 + \left(\frac{1}{2}\right)^2 - \left(\frac{3}{2}\right)^2$ has the same form. Further, $0 = 2^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 - \left(\frac{3}{2}\right)^2 - \left(\frac{3}{2}\right)^2$. Thus, when 2 and 3 are both units, every element of the field may be written in the form $u_1^2 + u_2^2 + u_3^2 - u_4^2 - u_5^2$ where the u_i are units (by adding and subtracting 1^2 if necessary). Thus, if R_λ is a field with characteristic different from 2 or 3, for all λ in an index set Λ, then $\prod_{\lambda \in \Lambda} R_\lambda$ is square representable.

(II.25) Proposition Let R be a stable ring with 2 a unit such that R/Rad(R) is square representable. Then R is square representable.

Proof Let π: R → R/Rad(R) be the canonical map and let u be an element of R. $\pi(u) = \sum_{i=1}^{k} (-1)^{n_i} \bar{v}_i^2$, where the $\bar{v}_i$ are units in R/Rad(R) and n_i is 0 or 1. Since the induced map $R^* \to (R/\mathrm{Rad}(R))^*$ is surjective, we may choose units v_i in R such that $\pi(v_i) = \bar{v}_i$. Then $u = \sum (-1)^{n_i} v_i^2 + r$ where r is in Rad(R). Now, r is in Rad(R) implies that $1 + r$ and $1 - r$ are units, so $r = \left(\frac{1 + r}{2}\right)^2 - \left(\frac{1 - r}{2}\right)^2$, a difference of squares of units. Thus u is written in the desired form.

(II.26) Corollary A semilocal ring in which 2 and 3 are units is square representable.

(II.27) Theorem A ring of cross sections of a sheaf of fields with characteristic $\neq$ 2 or 3, over a Boolean space is square representable.

Proof The proof follows the same outline as the proofs in (II.9) and (II.18). If η is an element of the ring R of cross sections, $\eta(x) = u_{1x}^2 + u_{2x}^2 + u_{3x}^2 - u_{4x}^2 - u_{5x}^2$, where u_{ix} are units in R_x. There are units

v_i, u_i in R such that $u_i(x) = u_{ix}$, $v_i(x) = u_{ix}^{-1}$ and

$$\eta(x) = (u_1^2 + u_2^2 + u_3^2 - u_4^2 - u_5^2)(x).$$

Then there is an open neighborhood N_x of x in X such that

$$\eta(y) = (u_1^2 + u_2^2 + u_3^2 - u_4^2 - u_5^2)(y)$$

and $u_i v_i(y) = 1_y$ for each y in N_x and for each i, $1 \leqslant i \leqslant 5$. The family $\{N_x\}_{x \in X}$ covers X. Patching together over a finite disjoint subcover, we obtain $\bar{u}_i$ units of R with $\eta = \bar{u}_1^2 + \bar{u}_2^2 + \bar{u}_3^2 - \bar{u}_4^2 - \bar{u}_5^2$.

(Note: in order to patch together, the same number of unit squares must be added and subtracted over each set in the subcover. This is why the hypothesis is less general than for the first two theorems involving a ring of cross-sections.)

(II.28) Corollary A von Neumann regular ring in which 2 and 3 are units is square representable.

(II.29) Corollary A zero-dimensional ring in which 2 and 3 are units is square representable.

CHAPTER III

INNER PRODUCT SPACES OVER $\langle 1,3\rangle$-FULL RINGS

The structure theory for the general linear group over a stable ring is given by Bass in [7]. We will be concerned with inner product spaces and their orthogonal groups over rings which are full of type $\langle 1,3\rangle$.

Throughout this chapter, V will be a free space of dimension n over a $\langle 1,3\rangle$-full ring R. Further, V posseses a symmetric inner product β: $V \times V \to R$, i.e., β is an R-bilinear form on V, $\beta(x,y) = \beta(y,x)$ and d_β: $V \to \mathrm{Hom}_R(V,R)$ by $d_\beta(x)(y) = \beta(x,y)$ is an R-isomorphism. We will use the basic terminology and facts on symmetric inner product spaces over commutative rings as given by Milnor in Chapter I of [31], by McDonald in Chapter III of [28], or by Baeza in Kapitel I in [4].

Let S be a commutative ring and M a finitely generated projective S-module. The module M is called stably free if there exist finitely generated free S-modules F_1 and F_2 with $M \oplus F_1 = F_2$. It can be shown ([15], p. 16), ([8], p. 2) or ([37], pp. 188-196) that "Every stably free projective is free" is equivalent to "For every subset $\{a_1,\cdots,a_n\}$ of S with $(a_1,\cdots,a_n) = S$, then there is an $n \times n$ matrix A having determinant a unit and first row $\langle a_1,\cdots,a_n\rangle$." It is a straightforward calculation to show this matrix condition is valid for stable rings. This gives the following useful lemma.

(III.1) Lemma A stably free projective module over a stable ring is free.

Notation: (u) denotes a 1-dimensional space spanned by a vector x having $\beta(x,x) = u$.

(III.2) Theorem Let R be a ring which is full of type $\langle 1,3\rangle$ and having 2 a unit. Then $V \simeq (u_1) \perp \cdots \perp (u_n)$ where $u_1,\cdots,u_n$ are units in R.

Proof (The matrix computation in this proof was part of the motivation for the definition of $\langle 1,3\rangle$-full.) The proof is by induction on the dimension of V. If n = 1 (n = dim(V)), the result is immediate. Let $\{e_1,e_2,\cdots,e_n\}$ be a basis for V and let $B = [\beta_{ij}]$ where $\beta_{ij} = \beta(e_i,e_j)$. Then

$$B = \begin{bmatrix} \beta_{11} & b \\ b^t & D \end{bmatrix}$$

where $b = [\beta_{12},\cdots,\beta_{1n}]$ and D is an $(n - 1) \times (n - 1)$ block. Since β is an inner product, the determinant of B, det(B), is a unit. Consequently, the elements of each column generate R and, in particular, using the second column, $(\beta_{12},\beta_{22},\cdots,\beta_{n2}) = R$. Since R is stable, there exist $\omega_2,\cdots,\omega_n$ with $\beta_{12} + \omega_2\beta_{22} + \cdots + \omega_n\beta_{n2} = v$ where v is a unit. Let $x = [\omega_2,\omega_3,\cdots,\omega_n]$. Then

$$\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}\begin{bmatrix} \beta_{11} & b \\ b^t & D \end{bmatrix}\begin{bmatrix} 1 & 0 \\ x^t & 1 \end{bmatrix} = \begin{bmatrix} a & b + xD \\ b^t + Dx^t & D \end{bmatrix}$$

where $a = \beta_{11} + bx^t + xb^t + xDx^t$. Then

$$b + xD = [\beta_{12},\cdots,\beta_{1n}] + [\omega_2,\cdots,\omega_n]D = [b_2,\cdots,b_n]$$

and, by the choice of x, b_2 is a unit.

Therefore, without loss of generality, we may assume $B = [\beta_{ij}]$ has the property that β_{12} (which equals β_{21}) is a unit. Since β_{12} is a unit, $R = (\beta_{11}, \beta_{12}, \beta_{22})$. Since 2 is a unit, $R = (\beta_{11}, 2\beta_{12}, \beta_{22})$. The ring R is ⟨1,3⟩-full, so there is a y in R with $\beta_{11} + 2\beta_{12}y + \beta_{22}y^2 = u$ where u is a unit. Then

$$\begin{bmatrix} 1 & y & \\ 0 & 1 & 0 \\ & 0 & I \end{bmatrix} B \begin{bmatrix} 1 & 0 & \\ y & 1 & 0 \\ & 0 & I \end{bmatrix} = \begin{bmatrix} u & * \\ * & * \end{bmatrix}.$$

Thus, after a suitable change of basis, we may assume the matrix $B = [\beta_{ij}]$ has $\beta_{11} = u$ a unit. If $\{f_1, \cdots, f_n\}$ is the basis of V having $\beta_{ij} = \beta(f_i, f_j)$ and $\beta_{11} = u$, then f_1 is non-isotropic, i.e., $\beta(f_1, f_1)$ is a unit, and by ((3.2), [31]), $V = Rf_1 \perp (Rf_1)^\perp \simeq (u) \perp (Rf_1)^\perp$. Since Rf_1 is free, we have $(Rf_1)^\perp$ is stably free. By (III.1) $(Rf_1)^\perp$ is free. Hence, $(Rf_1)^\perp$ with $\bar{\beta} = \beta\big|_{(Rf_1)^\perp \times (Rf_1)^\perp}$ is a free symmetric inner product space of dimension n - 1. The proof follows by induction.

A basis $\{e_1, \cdots, e_n\}$ of a free symmetric inner product space (V, β) giving rise to an orthogonal decomposition as given in (III.2), i.e., $\beta(e_i, e_i) = u_i$ and $\beta(e_i, e_j) = 0$ for $i \neq j$, is called an orthogonal basis for V.

Let (V, β) be a free symmetric inner product space. A unimodular vector x in V is isotropic if $\beta(x,x) = 0$. A direct summand W of V is totally isotropic if $\beta(w,w) = 0$ for all w in W. Further, V is split if V contains a totally isotropic summand W with $W = W^\perp$.

Suppose $\dim(V) = 2$ and V has a basis $\{e_1, e_2\}$ with $\beta(e_1, e_2) = 1$ and $\beta(e_i, e_i) = 0$ for i = 1, 2. Then V is split and is called a hyperbolic plane.

(III.3) Theorem Let R be a ⟨1,3⟩-full ring having 2 a unit. The following are equivalent:

(a) (V,β) is split.

(b) (V,β) is an orthogonal sum of hyperbolic planes.

Proof Since a hyperbolic plane is split and orthogonal sums of split spaces are split (see [31], Lemma (6.2)), it is clear that (b) implies (a).

Now assume (a), that (V,β) is split. Then $V = W \oplus Y$ where $W = W^{\perp}$. By (III.2), let $\{e_1,\cdots,e_n\}$ be an orthogonal basis for V. Let $e = e_1$ and $u = \beta(e,e)$. Then $e = w + y$ for w in W and y in Y. Clearly $y \neq 0$ since $\beta(e,e) = u$ a unit. Thus, $u = \beta(e,e) = 2\beta(w,y) + \beta(y,y)$. Define σ: $Y \rightarrow R$ by $\sigma(\ ) = \beta(2w + y,\ )$. Then $\sigma(y) = u$ and y is unimodular. Thus σ is surjective and y generates a free direct summand of Y, $Y = Ry \oplus \bar{Y}$.

Since V is split, Y is naturally isomorphic under $x \rightarrow \beta(\ ,x)$ with the dual space $W^* = \mathrm{Hom}_R(W,R)$ of W (see [31], p. 12). Thus $W^* = Rf \oplus \bar{W}$ where f is given by $f(\ ) = \beta(\ ,y)$. Since W is finitely generated and projective, we may identify W with its double dual $(W^*)^*$ via the pairing $\langle w^*,w\rangle = w^*(w)$ for w^* in W^* and w in W. Since f is unimodular in W^*, there is a w in W with $1 = \langle f,w\rangle = f(w) = \beta(w,y)$. Thus, we have an element w in W which is isotropic, i.e., $\beta(w,w) = 0$, and unimodular. Further, $H = Rw \oplus Ry$ is a hyperbolic plane. Then $V = H \perp \bar{V}$ by ([31], [28]). Again applying (III.1), $\bar{V}$ is a free inner product space. It is easy to see that $\bar{V}$ is also split. Hence, the proof follows by induction on the dimension of V.

A symmetric inner product space (V,β) is said to have hyperbolic rank $\geqslant t$, if there exists an orthogonal splitting $V = H_1 \perp \cdots \perp H_t \perp \bar{V}$ where the H_i for $1 \leqslant i \leqslant t$ are hyperbolic planes.

(III.4) Lemma Let (V,β) be a free symmetric inner-product space of dimension n over a $\langle 1,3\rangle$-full ring R. If x is isotropic in V then there is a y in V satisfying:

(a) $H = Rx \oplus Ry$ is a hyperbolic plane

(b) $\beta(x,y) = 1$

(c) $V = H \perp W$

Proof Since x is unimodular, $V = Rx \oplus W$. Let $x_2,\cdots,x_n$ be a basis for W. Then $\{x = x_1,x_2,\cdots,x_n\}$ is a basis for V. Let f_1, f_2, $\cdots$, f_n be a dual basis of $V^* = \mathrm{Hom}(V,R)$, where $f_i(x_j) = \delta_{ij}$. Since β is an inner product, $\beta(x_j, \ ): V \to V^*$ is an isomorphism for each j. Then there are $y = y_1$, y_2, $\cdots,y_n$ in V with $\beta(x_j,y_i) = \sigma_i(x_j)$. Then $Rx \oplus Ry$ is a hyperbolic plane.

(III.5) Corollary (Witt Decomposition). Let V be as in (III.4). V has a decomposition $V \simeq V_o \perp tH$ where V_o is anisotropic (has no isotropic vectors).

For the remainder of this chapter, R is a $\langle 1,3\rangle$-full ring in which 2 is a unit, and (V,β) is a free symmetric inner product space of dimension n over R.

Let $O(V)$ denote the orthogonal group of V, i.e., the set of all σ in the general linear group $GL(V)$ satisfying $\beta(\sigma x,\sigma y) = \beta(x,y)$ for all x and y in V. If σ is in $O(V)$, σ is called an isometry.

Our terminology and notation will basically follow Chapter III of [28]. We fix the following assumptions and notation for the remainder of this chapter: Assume the hyperbolic rank of V is $\geqslant 1$ and dim(V) $\geqslant 3$. Then $V = H \perp W$ where $H = Ru \oplus Rv$, $\beta(u,u) = \beta(v,v) = 0$, and $\beta(u,v) = 1$, i.e., H is a hyperbolic plane. Under this hypothesis, we can describe some elements of O(V). (See [19] or Chapter III of [28].)

(a) Define Δ in O(V) by $\Delta(v) = u$, $\Delta(u) = v$ and $\Delta(x) = x$ for all x in W.

(b) For ε a unit of R, define Φ_ε by $\Phi_\varepsilon(u) = \varepsilon u$, $\Phi_\varepsilon(v) = \varepsilon^{-1}v$ and $\Phi_\varepsilon(x) = x$ for all x in W.

(c) If x is in V with $\beta(x,u) = 0$, define $E_{u,x}$ by

$$E_{u,x}(z) = z - \beta(u,z)x + \beta(x,z)u - \tfrac{1}{2}\beta(x,x)\beta(u,z)u$$

and define $E_{v,x}$ (if $\beta(x,v) = 0$) in an analogous fashion. The maps $E_{u,x}$ and $E_{v,x}$ are Eichler-Siegal transvections.

(III.6) Theorem When V has hyperbolic rank $\geqslant 1$, the maps $E_{u,x}$, $E_{v,x}$, Δ and Φ_ε are in O(V). Further,

(a) $E_{u,x}E_{u,y} = E_{u,x+y}$, $(E_{u,x})^{-1} = E_{u,-x}$, and $E_{\alpha u,x} = E_{u,\alpha x}$ for α a unit.

(b) $\Delta^{-1}\Phi_\varepsilon\Delta = \Phi_{\varepsilon^{-1}}$, $\Phi_\varepsilon^{-1} = \Phi_{\varepsilon^{-1}}$.

(c) $\Phi_{\varepsilon^{-1}}\Delta\Phi_\varepsilon = \Delta$, $\Delta^2 = I$.

(d) If z is in V then $z = \alpha u + \delta v + y$ where y is in W, α and δ are in R. If x is in W, then

$$E_{u,x}(z) = [\alpha + \beta(x,y) - \tfrac{1}{2}\delta\beta(x,x)]u + \delta v + (y - \delta x).$$

(A similar formula is available for $E_{v,x}(z)$.)

(e) If θ is in O(V) and $\theta|_H$ = identity, then $\theta E_{u,x}\theta^{-1} = E_{u,\theta x}$. In general $\theta E_{u,x}\theta^{-1} = E_{\theta u,\theta x}$ for θ in O(V).

(f) If x is in W, then $\Phi_\varepsilon E_{u,x}\Phi_\varepsilon^{-1} = E_{u,\varepsilon x} = E_{\varepsilon u,x}$.

Proof See (III.15) and (III.16) of [28] or verify directly.

Since $V = H \perp W$ and H is a hyperbolic plane, then W is a free symmetric inner product space. By (III.2) we may select an orthogonal basis $\{e_1,\cdots,e_t\}$ ($t = n - 2$) of non-isotropic vectors in W, i.e., $\beta(e_i,e_i) = v_i$ a unit for $1 \leqslant i \leqslant t$. If $x = \alpha_1 e_1 + \cdots + \alpha_t e_t$ is in W and $z = \alpha u + \delta v + \delta_1 e_1 + \cdots + \delta_t e_t$ is in V, then

$$E_{u,x}(z) = [\alpha + \sum \alpha_i \delta_i v_i + \tfrac{1}{2}\delta(\sum \alpha_i^2 v_i)]u + \delta v + \sum(\delta_i - \delta\alpha_i)e_i$$

from (III.6)(d). Therefore, if z is unimodular and R is $\langle 1,3\rangle$-full, then, by (II.2) there exist $\alpha_1,\cdots,\alpha_t$ in R with $\alpha + \sum \alpha_i\delta_i v_i + \tfrac{1}{2}\delta\sum(\alpha_i^2 v_i)$ $= w$ a unit. (This is the second motivation for the term "full" of type $\langle 1,3\rangle$.) That is, after a transformation of z by a suitable transvection $E_{u,x}$ with $x = \alpha_1 e_1 + \cdots + \alpha_t e_t$, we may assume $E_{u,x}(z) = \alpha u + \delta v + \delta_1 e_1 + \cdots + \delta_t e_t$ where α is a unit. Then, if $y = \alpha^{-1}(\delta_1 e_1 + \cdots + \delta_t e_t)$, $E_{v,y}E_{u,x}(z) = h$ where h is in H. Further, $h = \alpha u + \bar{\delta} v$ where α is a unit.

(III.7) Theorem Let R be a ring, full of type $\langle 1,3\rangle$, having 2 a unit, and let (V,β) be a free symmetric inner product space of hyperbolic rank $\geqslant 1$. Then

(a) the orthogonal group $O(V)$ is transitive on unimodular vectors of the same norm.

(b) The orthogonal group $O(V)$ is transitive on the set of hyperbolic planes in V.

Proof Let y and z be unimodular of the same norm, i.e., $\beta(y,y) = \beta(z,z)$ and let $V = H \perp W$ where H is a hyperbolic plane. By the above discussion, there exist products E and F of transvections such that $E(y) = \alpha_1 u + \delta_1 v$, $F(z) = \alpha_2 u + \delta_2 v$, where α_1 and α_2 are units ($H = Ru \oplus Rv$). Then $\Phi_{\alpha_1^{-1}}E(y) = u + \alpha_1\delta_1 v$, $\Phi_{\alpha_2^{-1}}F(z) = u + \alpha_2\delta_2 v.$. Since $\beta(y,y) = \beta(z,z)$,

$\alpha_1\delta_1 = \alpha_2\delta_2$. Hence, $\Phi_{\alpha_1^{-1}}E(y) = \Phi_{\alpha_2^{-1}}F(z)$ and consequently,

$$y = E^{-1}\Phi_{\alpha_1}\Phi_{\alpha_2^{-1}}F(z).$$

This completes the proof of (a).

To show (b), we may assume that H_1 and H_2 are hyperbolic planes where $H_1 = H = Ru \oplus Rv$. Suppose $H_2 = R\bar{u} \oplus R\bar{v}$ where $\beta(\bar{u},\bar{v}) = 1$, $\beta(\bar{u},\bar{u}) = \beta(\bar{v},\bar{v}) = 0$. By part (a), we may transform u to $\bar{u}$. Thus, assume $u = \bar{u}$. Then $\bar{v} = \alpha u + \delta v + w$ where w is in W, $V = H \perp W$. Since $\delta = \beta(u,v) = \beta(\bar{u},\bar{v}) = 1$, we have $\bar{v} = \alpha u + v + w$. Then $E_{u,w}$ will carry $\bar{v}$ into H and simultaneously fix u. Hence H_2 is carried to H_1.

(III.8) Theorem (Cancellation). Let R be a ring, full of type $\langle 1,3 \rangle$, having 2 a unit. Let U, W, and Z be free symmetric inner product spaces over R. If $U \perp W \simeq U \perp Z$, then $W \simeq Z$.

Proof It suffices to prove the result when U = H where H is a hyperbolic plane. This follows since if $U = (U,\beta)$, then both sides of the above isometry may be augmented by replacing (U,β) by $(U,-\beta) \perp (U,\beta)$. But $(U,-\beta) \perp (U,\beta)$ is split, and by (III.3), it is a direct sum of hyperbolic planes. Then, by induction, we may assume U = H. Thus, let σ: $H \perp W \to H \perp Z$ be the given isometry. Let $\bar{H} = \sigma(H)$. By the preceding theorem there is a τ in $O(H \perp Z)$ with $\tau H = \bar{H}$. Since isometries carry orthogonal complements to orthogonal complements, the result follows.

Note that the above also shows that if W and Z are non-singular subspaces of a symmetric inner product space U, then any isometry σ: $W \to Z$ may be lifted to an isometry $\bar{\sigma}$: $U \to U$ with $\bar{\sigma}|_W = \sigma$.

Next we examine the generators of $O(V)$ when V has hyperbolic rank $\geqslant 1$.

Suppose σ is in $O(V)$ and $V = H \perp Re_1 \perp \cdots \perp Re_t$ where $\{e_1,\cdots,e_t\}$ is an orthogonal basis for $W = H^{\perp}$. Then $\beta(\sigma(e_s),\sigma(e_s)) = \beta(e_s,e_s)$. By the proof of (III.7) there is a product $\tau_1\cdots\tau_s$ of the isometries described in (III.6) with $\tau_1\cdots\tau_s\sigma(e_s) = e_s$. Then $\tau_1\cdots\tau_s\sigma\colon\ (Re_s)^{\perp} \to (Re_s)^{\perp}$. An induction argument would show that the isometries described in (III.6) generate $O(V)$ provided it is true for $V = H \perp Re$ where e is non-isotropic.

Thus, suppose $V = H \perp Re$ where $\beta(e,e) = w$ (a unit). Let σ be in $O(V)$. Then $\sigma(H) = \bar{H}$ where $\ddot{H}$ is a hyperbolic plane. By the proof of (III.7) there is a product $\tau_1\cdots\tau_s$ of isometries described in (III.6) with $\tau_1\cdots\tau_s\sigma$ = identity on H. Further, $\tau_1\cdots\tau_s\sigma\colon\ H^{\perp} \to H^{\perp}$. Hence, $\tau_1\cdots\tau_s\sigma(e) = \alpha e$. Using $\beta(e,e) = w$, one sees that $\alpha^2 = 1$.

To examine the equation $\alpha^2 = 1$, let P be a prime ideal of R. The localization $(\alpha)_P$ of α satisfies $(\alpha)_P^2 = 1$ in the local ring R_P. Since 2 is a unit, $(\alpha)_P = \pm 1$. Let $V = \{P \text{ in } \mathrm{Spec}(R) \mid (\alpha)_P = 1\}$ and let $W = \{P \text{ in } \mathrm{Spec}(R) \mid (\alpha)_P = -1\}$. Thus $V = \mathrm{Supp}(\alpha + 1)$ and $W = \mathrm{Supp}(\alpha - 1)$. Then $\mathrm{Spec}(R)$ is a disjoint union of V and W. This decomposition of $\mathrm{Spec}(R)$ determines a partition of unity $1 = e + f$ where e and f are orthogonal idempotents. Indeed, $e = (\alpha + 1)/2$, $f = (\alpha - 1)/2$. This gives natural decompositions $R = Re \oplus Rf$, $V = eV \oplus fV$ and, in particular, $O(V) = O(eV) \oplus O(fV)$. (For example, see [26] or [4].) After decomposition of $O(V)$, we may assume $\alpha = 1$ or $\alpha = -1$. We now treat each case.

If $\tau_1\cdots\tau_s\sigma(e) = e$, then $\tau_1\cdots\tau_s\sigma = I$ (identity) and $\sigma = \tau_s^{-1}\cdots\tau_1^{-1}$ is thus given as a product of the isometries described in (III.6).

Suppose $\tau_1 \cdots \tau_s \sigma(e) = -e$. This is more difficult and requires a brief digression.

If x is a non-isotropic vector in V, then the symmetry or hyperplane reflection σ_x determined by x is defined by $\sigma_x(z) = z - 2 \frac{\beta(x,z)}{\beta(x,x)} x$ for all z in V. The symmetry σ_x is an involution in O(V) and $\sigma_x = -I_{Rx} \perp I_{(Rx)^\perp}$. In the previous discussion, if $\tau_1 \cdots \tau_s \sigma(e) = -e$, then $\tau_1 \cdots \tau_s \sigma$ is precisely the symmetry σ_e. The next lemma shows that a symmetry σ_x where x is in $H^\perp$ may be written as a product of the isometries described in (III.6).

(III.9) Lemma Let $V = H \perp W$ and let x be non-isotropic in W. Then the symmetry σ_x is given by

$$\sigma_x = \Delta\Phi_{-\frac{1}{2}\beta(x,x)} E_{v,-x} E_{u,\frac{2x}{\beta(x,x)}} E_{v,-x}.$$

Proof It is straightforward but tedious to check that both sides of the above equation agree on u, v and arbitrary w in W.

For the remainder of this section, we assume that R is connected, i.e., has no nontrivial idempotents. (See Remark on page 29.)

(III.10) Theorem (Generators of O(V)). When the hyperbolic rank of V is $\geqslant 1$, the group O(V) is generated by the isometries $E_{u,x}$, $E_{v,x}$, Δ and Φ_ε for various choices of x and ε.

Let A be a proper ideal of R. The canonical ring morphism π: $R \to R/A$ induces a natural morphism of bilinear spaces π: $(V, \beta) \to (V/AV, \bar{\beta})$ where $\bar{\beta}$ is given by $\bar{\beta}(\pi x, \pi y) = \pi(\beta(x,y))$.

Similarly, we obtain a group morphism π: $O(V) \to O(V/AV)$ by $(\pi\sigma)(\pi x) = \pi(\sigma(x))$. Since V has hyperbolic rank $\geqslant 1$ with a hyperbolic plane $H = R u \oplus R v$, it is easy to see that V/AV has hyperbolic rank $\geqslant 1$ with a hyperbolic plane $\bar{H} = R\pi u \oplus R\pi v$. By (II.3), R/A is full of type $\langle 1,3\rangle$ with 2 a unit. Hence, each generator of $O(V/AV)$ is given by (III.10) and consequently (applying (II.5)(b) for Φ_ε) each generator in $O(V/AV)$ has a generator pre-image in $O(V)$. Thus, we have the next theorem.

(III.11) Theorem If A is a proper ideal of R, then the group morphism $\pi\colon\ O(V) \to O(V/AV)$ is surjective.

(III.12) Theorem The center of $O(V)$ is $\{\pm I\}$.

Proof The proof of the analogous result over a local ring given in ([19], Lemma 1) or ([28], Theorem (III.22)) carries over to the $\langle 1,3\rangle$-full ring without changes.

The subgroup of $O(V)$ generated by all $E_{u,x}$ and $E_{v,x}$ with x in W is denoted by $EO(V)$ and called the Eichler subgroup of $O(V)$. Since the generators of $O(V)$, by (III.10), are of the form Δ, Φ_ε, $E_{u,x}$ and $E_{v,x}$, and, since the $E_{u,x}$, $E_{v,x}$ behave properly under conjugation (see (III.6)) by these generators, we have that $EO(V)$ is a normal subgroup of $O(V)$.

Let $\Omega(V) = [O(V),O(V)]$ be the commutator subgroup of $O(V)$. We conclude by showing that if 3 is also a unit in R, then $\Omega(V) = EO(V)$.

(III.13) Theorem Let 3 also be a unit in R. Then

$$EO(V) = \Omega(V) = [\Omega(V),\Omega(V)].$$

Proof Prior to the proof we need a technical lemma. The lemma was proven over fields by Eichler [12] and later over local rings by James [19]. The lemma may be verified directly by checking the images of u and v and of x in W on both sides of the expression.

(III.14) Lemma If α and δ are in R and x is in W with $\eta = 1 - \frac{1}{2}\alpha\delta\beta(x,x)$ a unit, then

$$E_{v,\alpha x}E_{u,\delta x} = E_{u,\eta^{-1}\delta x}E_{v,\alpha\eta x}\Phi_{\eta^{-2}}.$$

We now begin a proof of (III.13). To show EO(V) = Ω(V), first observe $E_{u,x} = \Phi_3 E_{u,x/2}\Phi_{1/3}E_{u,-x/2} = [\Phi_3, E_{u,x/2}]$. Thus EO(V) is in Ω(V).

To show Ω(V) is in EO(V), recall from (III.10), if θ is in O(V), then θ may be written as $\theta = \Delta^a\Phi_\eta\chi$ where a is in {0,1}, η is a unit and χ is in EO(V). ((III.6) allows the factors to appear in the order described.) Then, for θ and ϕ in O(V),

$$\begin{aligned}[\theta,\phi] &= [\Delta^a\Phi_\eta\chi, \pm\Phi_\varepsilon\psi] \\ &= \Delta^a\Phi_\eta\chi\Phi_\varepsilon\psi\chi^{-1}\Phi_\eta^{-1}\Delta^a\psi^{-1}\Phi_\varepsilon^{-1} = \Delta^a\chi_1\psi_1\psi_2^{-1}\Delta^a\psi_2\Phi_{(\varepsilon^{-2a})}\end{aligned}$$

where $\chi_1 = \Phi_\eta\chi\Phi_\eta^{-1}$ is in EO(V), $\psi_1 = \Phi_{\eta\varepsilon}\psi\Phi_{\eta\varepsilon}^{-1}$ is in EO(V), $\chi_2 = \Phi_\varepsilon\chi_1\Phi_\varepsilon^{-1}$ and ψ_2 are in EO(V). Using (III.6) to remove Δ, we have

$$[\theta,\phi] = \Phi_{(\varepsilon^{-2a})}\psi_3$$

where ψ_3 is in EO(V). It remains to show Φ_{ε^2} is in EO(V) for ε a unit in R. Let ε be a unit and x be in W with $\beta(x,x)$ a unit. Set $\alpha = (1 - \varepsilon)\beta(x,x)^{-1}2$. Then $\varepsilon = 1 - \frac{1}{2}\alpha\beta(x,x)$. Applying (III.14), we have $\Phi_{\varepsilon^{-2}}$ (and hence Φ_{ε^2}) in EO(V). Thus Ω(V) = [O(V),O(V)] is in EO(V).

Clearly, [Ω(V),Ω(V)] = [EO(V),EO(V)] is in EO(V) = Ω(V). On the other hand, $E_{u,x} = [\Phi_{2^2}, E_{u,x/3}]$ is in [Ω(V),Ω(V)]. Thus EO(V) = [Ω(V),Ω(V)], completing the proof.

Remark The material following Lemma (III.9) may be extended to a ring which is full of type ⟨1,3⟩, has 2 a unit, and is not connected, provided Δ is redefined to reflect the existence of non-trivial idempotents.

CHAPTER IV

NORMAL SUBGROUPS OF O(V)

The central purpose of this chapter is to determine the normal subgroups of O(V). We assume that 2 is a unit of R, R is $\langle 1,3 \rangle$-full with no non-trivial idempotents, (V,β) is a free symmetric inner product space over R, $\dim(V) \geqslant 3$, and V has hyperbolic rank $\geqslant 1$. Thus V splits as $V = H \perp W$ where $H = Ru \oplus Rv$ is a hyperbolic plane with $\beta(u,v) = 1$ and $\beta(u,u) = \beta(v,v) = 0$.

Let $\Omega(V) = [O(V),O(V)]$ act on O(V) as a transformation group under conjugation and examine the orbit of a single element ρ. We show that among the elements of this orbit there is an isometry which is a product of two Eichler-Siegal transvections, a suitable ϕ_ε and an element of O(W).

First we establish some definitions and notation. Suppose A is a proper ideal of R. The ring morphism $\pi_A\colon R \to R/A$ induces a surjective R-morphism $\pi_A\colon (V,\beta) \to (V/AV,\beta_A)$ of symmetric inner product spaces where $\beta_A(\pi_A x,\pi_A y) = \pi_A\beta(x,y)$. In turn, this gives a surjective group morphism $\lambda_A\colon O(V) \to O(V/AV)$ (see (III.11)). The Special Orthogonal Group, SO(V) is defined by $SO(V) = \{\sigma \in O(V)\colon \det(\sigma) = 1\}$. Define $O(V,A) = \{\sigma \text{ in } O(V)\colon\ \lambda_A\sigma \text{ is in Center}(O(V/AV))\}$. Since $\dim(V) \geqslant 3$, (III.12) implies

$$O(V,A) = \{\sigma \text{ in } O(V)\colon\ \lambda_A\sigma = \pm I\}.$$

Let $SO(V,A) = SO(V) \cap O(V,A)$. The group O(V,A) is the congruence subgroup of $O(V)$ of level A and the group $SO(V,A)$ is the special congruence subgroup of $O(V)$ of level A.

If $A = R$ (hence $V/RV = 0$), let $O(V/RV) = I$ and $SO(V/RV) = I$. Further let

$$O(V,R) = O(V),$$

$$O(V,0) = \text{Center }(O(V)),$$

$$SO(V,R) = SO(V), \quad \text{and}$$

$$SO(V,0) = SO(V) \cap \text{Center}(O(V)).$$

Recall $\Omega(V) = [O(V),O(V)]$ denotes the commutator subgroup of $O(V)$. Define the mixed commutator subgroup of level A to be $\Omega(V,A) = [O(V),O(V,A)]$ for an ideal A, i.e., $\Omega(V,A)$ is the subgroup generated by all $g^{-1}h^{-1}gh$ for g in $O(V)$ and h in $O(V,A)$. Observe $\Omega(V,A) \leqslant O(V,A)$. Indeed, $\Omega(V,A) \leqslant SO(V,A)$. Let $EO(V)$ denote the subgroup of $O(V)$ generated by all the Eichler-Siegal transvections $E_{u,x}$ and $E_{v,y}$ where x and y are in W. For an ideal A of R, let $EO(V,A)$ denote the $EO(V)$-normal subgroup of $O(V,A)$ generated by all transvections $E_{u,x}$ and $E_{v,y}$ where x and y are in W and $\pi_A(x) = \pi_A(y) = 0$, i.e., the order $O(x)$ of x and the order $O(y)$ of y are in A. We call $EO(V)$ the Eichler subgroup of $O(V)$ and $EO(V,A)$ the Eichler subgroup of level A. Observe $EO(V,A) \leqslant O(V,A)$ and $EO(V,A)$ is the subgroup generated by all $\theta E_{u,x}\theta^{-1}$ and $\theta E_{v,y}\theta^{-1}$ for θ in $EO(V)$ and $O(x) \subseteq A$, $O(y) \subseteq A$.

(IV.1) Theorem Let A be an ideal of R and ρ be in $O(V,A)$. Then for suitable ψ in $\Omega(V)$,

$$\psi\rho\psi^{-1} = \sigma_1\sigma_2\Phi_\varepsilon\theta \qquad \text{where}$$

(a) σ_1 and σ_2 are Eichler-Siegal transvections of order contained in A;

(b) $\varepsilon \equiv \pm 1 \bmod A$;

(c) $\theta|_H = $ identity. Hence θ is in $O(W,A)$.

(Note that σ_1, σ_2, Φ_ε or θ may be trivial, e.g., ρ may be I. This will not affect the subsequent proofs.)

Proof Suppose $\rho(v) = \alpha u + \delta v + z$, where α and δ are in R, z is in W, and ρ is in O(V,A). Since $\lambda_A\rho = \pm I$, $\delta \equiv \pm 1 \bmod A$, $\alpha \equiv 0 \bmod A$ and $\pi_A z = 0$, i.e., $O(z) \subset A$. First we show that ρ may be modified by conjugation so that δ is a unit. Let $\psi = E_{v,-s}$ where s is in W. Clearly ψ is in $\Omega(V)$. Set $\bar{\rho} = \psi\rho\psi^{-1}$. Then $\bar{\rho}(v) = \psi\rho\psi^{-1}(v) = \psi\rho(v)$ $= \alpha u + [\delta - \beta(s,z) - \frac{1}{2}\alpha\beta(s,s)]v + (z + \alpha s)$. Let $\{e_1,e_2,\cdots,e_k\}$ be an orthogonal basis for W with $\beta(e_i,e_i) = v_i$ a unit. Then $z = \sum d_ie_i$ for d_i in R. Since $\rho(v)$ is unimodular, $(\alpha,\delta,d_1,\cdots,d_k) = R$. Since 2 is a unit and each v_i is a unit,

$$R = (\delta,-d_1v_1,-d_2v_2,\cdots,-d_kv_k,-\tfrac{1}{2}\alpha v_1,\cdots,-\tfrac{1}{2}\alpha v_k).$$

Applying (II.2), there exist $w_1,w_2,\cdots,w_k$ in R such that

$$\delta - \textstyle\sum_{i=1}^k d_iv_iw_i - \tfrac{1}{2}\alpha \textstyle\sum_{i=1}^k w_i^2v_i = \mu,$$

a unit. Let $s = \sum_{i=1}^k w_ie_i$, which is in W. Observe that $\beta(s,z) = \sum w_id_iv_i$, $\beta(s,s) = \sum w_i^2v_i$ so $\delta - \beta(s,z) - \frac{1}{2}\alpha\beta(s,s) = \mu$ and $\bar{\rho}(v) = \alpha u + \mu v + (z + \alpha z)$ has coefficient of v a unit. $\delta \equiv \mu \bmod A$ since $O(z) \subset A$ and α is in A. Thus, we may write $\psi\rho\psi(v) = \bar{\rho}(v)$ $= \alpha u + \delta v + z$ where α and δ are in R, δ is a unit, $\delta \equiv \pm 1 \bmod A$, α is in A, z is in W and $O(z) \subset A$.

The transvection $E_{u,\delta^{-1}z}$ is in $\Omega(V,A) = EO(V,A)$, and

$$E_{u,\delta^{-1}z}(\bar{\rho}(v)) = [\alpha + \tfrac{1}{2}\delta^{-1}\beta(z,z)]u + \delta v.$$

Then

$$E_{u,\delta^{-1}z}(\bar{\rho}(v)) = [\delta\alpha + \tfrac{1}{2}\beta(z,z)]u + v.$$

Set $\rho_1 = \Phi_\delta E_{u,\delta^{-1}z}\bar{\rho}$. Since $\beta(v,v) = 0$, then $\beta(\rho_1(v),\rho_1(v)) = 0$, and consequently, $\delta\alpha + \frac{1}{2}\beta(z,z) = 0$. Thus $\rho_1(v) = v$.

Next consider the action of ρ_1 on u. As above, in general, $\rho_1(u) = \gamma u + \mu v + w$ for γ, μ in R and w in W. Since ρ_1 is in O(V,A), $O(w) \subseteq A$. Since $1 = \beta(u,v) = \beta(\rho_1(u),\rho_1(v))$, we have $\gamma = 1$. Then $E_{v,w}\rho_1(u) = u + \bar{\mu}v$, and using $\beta(u,u) = 0$, it is clear that $\bar{\mu} = 0$. Hence, $E_{v,w}\Phi_\delta E_{u,\delta^{-1}z}\bar{\rho} = \theta$ where $\theta(u) = u$ and $\theta(v) = v$, i.e., θ fixes H. Further, $O(w) \subset A$ implies $E_{v,w}$ is in $\Omega(V,A)$. This is because $E_{v,w}(z) = z + \beta(w,z)v - \beta(v,z)w - \frac{1}{2}\beta(w,w)\beta(v,z)v$ and all the terms except z have coefficients in A, so $\pi_A E_{v,w}(z) = \pi_A(z)$. Then

$$\bar{\rho} = E_{u,-\delta^{-1}z}\Phi_{\delta^{-1}}E_{v,-w}\theta = E_{u,-\delta^{-1}z}E_{v,-\delta w}\Phi_{\delta^{-1}}\theta.$$

For the remainder of this chapter we fix the following setting:

Let G denote an $\Omega(V)$-normal subgroup of O(V), i.e., G is a subgroup of O(V) and $\sigma\rho\sigma^{-1}$ is in G for all σ in O(V) and ρ in G. For ρ in G, let C_ρ denote the orbit of ρ under conjugation by elements of $\Omega(V)$. Certainly, C_ρ is in G. Further, by (IV.1), we may assume there is a ψ in $\Omega(V)$ with $\psi\rho\psi^{-1} = E_{u,x}E_{v,y}\Phi_\varepsilon\theta$ where $\theta|_H$ is the identity and x and y are in W.

(IV.2) <u>Lemma</u> (For the above setting). Assume 3 and 5 are also units in R. Then there are units ε and η such that $E_{u,\varepsilon x}$ and $E_{v,\eta y}$ belong to G.

<u>Proof</u> Observe that $\Phi_4 = [\Phi_2,\Delta]$ is in $\Omega(V)$. Thus the commutator

$$\begin{aligned}[\psi\rho\psi^{-1},\Phi_4] &= \psi\rho\psi^{-1}\Phi_4\psi\rho^{-1}\psi^{-1}\Phi_4^{-1} = E_{u,x}E_{v,y}\Phi_\varepsilon\theta\Phi_4\theta^{-1}\Phi_\varepsilon E_{v,-y}E_{u,-x}\Phi_4^{-1}\\ &= E_{u,x}E_{v,y}\Phi_4E_{v,-y}E_{u,-x}\Phi_4^{-1} = E_{u,x}E_{v,y}\Phi_4E_{v,-y}\Phi_4^{-1}\Phi_4E_{u,-x}\Phi_4^{-1}\\ &= E_{u,x}E_{v,y}E_{v,-y/4}E_{u,-4x} = E_{u,x}(E_{v,3y/4}E_{u,-3x})E_{u,x}^{-1}\end{aligned}$$

is in G. Conjugating by $E_{u,-x}$ shows that $E_{u,3y/4}E_{u,-3x}$ is in G. It now suffices to show that if $E_{u,x}E_{v,y}$ lies in G, then there are units ε and η such that $E_{u,\varepsilon x}$ and $E_{v,\eta y}$ lie in G.

Observe since $E_{u,x}E_{v,y}$ is in G then

$$E_{v,y}E_{u,x} = E_{u,x}^{-1}(E_{u,x}E_{v,y})E_{u,x}$$

is in G. Thus

$$E_{u,2x}E_{v,2y} = E_{v,y}^{-1}(E_{v,y}E_{u,x})(E_{u,x}E_{v,y})E_{v,y}$$

is in G. Repeating the argument of the previous paragraph shows that $E_{u,4x}E_{v,4y}$ is in G. Then $E_{u,16x}E_{v,y} = \Phi_4 E_{u,4x}E_{v,4y}\Phi_4^{-1}$ is in G since, as noted above, Φ_4 is in $\Omega(V)$. Then

$$E_{u,15x}E_{v,y}E_{u,x} = E_{u,x}^{-1}(E_{u,16x}E_{v,y})E_{u,x}$$

is in G and since $E_{v,y}E_{u,x}$ is in G, we conclude that $E_{u,15x}$ is in G. Hence, there is a unit $\varepsilon = 15$ such that $E_{u,15x}$ is in G. An analogous argument shows there is a unit η such that $\sigma_{v,\eta y}$ is in G. This completes the proof.

Observe that if one is interested only in the normal subgroups of O(V) rather than the $\Omega(V)$-normal subgroups, then in the above proof the conjugation by Φ_4, which lies in $\Omega(V)$, may be replaced by conjugation by Φ_2, which is in O(V). Then, with minor modifications, the argument will carry through under the hypothesis only that 2 and 3 are units, omitting the assumption that 5 is a unit.

Having obtained $E_{u,x}$ in G, we next show that suitable conjugation gives $\Omega(V,O(x)) \leqslant G$. That is, the orbit of $E_{u,x}$ when $\Omega(V)$ acts on O(V) via conjugation is $\Omega(V,O(x))$.

(IV.3) <u>Theorem</u> Let R be a ring which is strongly $\langle 1,3\rangle$-full and square representable, having 2 a unit. Let G be an $\Omega(V)$-normal subgroup of

O(V), dim(V) = 3 or $\geqslant 5$, and hyperbolic rank of V $\geqslant 1$. If $E_{u,x}$ is in G, then $\Omega(V,O(x)) \leqslant G$.

Proof The proof will follow from a series of steps.

(a) If $E_{u,x}$ is in G, then $E_{u,\eta x}$ is in G for all η in R. Observe, if δ is a unit, then ϕ_{δ^2} is in $\Omega(V)$ since $\phi_{\delta^2} = [\phi_\delta,\Delta]$. Then, if $E_{u,x}$ is in G, we have $E_{u,\delta^2x} = \phi_{\delta^2}E_{u,x}\phi_{\delta^2}^{-1}$ is in G. Suppose, using square representability, $\eta = \sum_{i=1}^{t} v_i$ where $v_i = \pm u_i^2$ and u_i is a unit for each i. Then $E_{u,\eta x} = E_{u,v_1x}E_{u,v_2x}\cdots E_{u,v_tx}$ is in G. This argument shows that $\Omega(V,O(x)) \leqslant G$ in the case dim(V) = 3. For the remainder of the proof, we assume dim(V) $\geqslant 5$ and, consequently, $V = H \perp W$ where dim(W) = m $\geqslant 3$.

(b) Next we manufacture some elements in $\Omega(V)$. It was noted in (III.9) that the symmetry σ_z for z nonisotropic in W could be written as

$$\sigma_z = \Delta\phi_{-\frac{1}{2}\beta(z,z)}E_{v,-z}E_{u,-2z/\beta(z,z)}E_{v,-z}$$

in terms of the Eichler-Siegal transvections, Δ, and ϕ_ε. Recall that $\Delta^2 = I$ and $\Delta\phi_\varepsilon\Delta = \phi_{\varepsilon^{-1}}$. Hence, letting $\varepsilon = -\frac{1}{2}\beta(z,z)$,

$$\phi_\varepsilon^{-1}\Delta\sigma_z = E_{v,-z}E_{u,\varepsilon^{-1}z}E_{v,-z}$$

is in $\Omega(V)$. Consequently, for y and z nonisotropic in W and letting $\alpha = -\frac{1}{2}\beta(y,y)$, the isometry

$$\phi_\varepsilon^{-1}\Delta\sigma_z\phi_\alpha^{-1}\Delta\sigma_y = \phi_\varepsilon^{-1}\phi_\alpha\Delta^2\sigma_z\sigma_y = \phi_{\varepsilon^{-1}}\phi_\alpha\sigma_z\sigma_y$$

is in $\Omega(V)$. It is easy to check that if λ is a unit of R, $\sigma_z = \sigma_{\lambda z}$. Thus, in $\phi_{\varepsilon^{-1}}\phi_\alpha\sigma_z\sigma_y$, z may be replaced by $\beta(z,z)^{-1}z$ and y by $\frac{1}{2}y$ without changing the factor $\sigma_z\sigma_y$. However, $\phi_{\varepsilon^{-1}}\phi_\alpha = \phi_{\varepsilon^{-1}\alpha}$ becomes $\phi_{\beta(z,z)\beta(y,y)/4}$ under these replacements. Therefore, $\phi_{\beta(z,z)\beta(y,y)/4}\sigma_z\sigma_y$ is in $\Omega(V)$.

(c) Suppose further that y and z are nonisotropic in W and satisfy $\beta(y,z) = 1$. A direct computation gives

$$(\sigma_z\sigma_y - \sigma_y\sigma_z)(x) = [4/\beta(z,z)\beta(y,y)][\beta(y,x)z - \beta(z,x)y].$$

Hence, if $\varepsilon = \beta(z,z)\beta(y,y)/4$, then

$$\varepsilon(\sigma_z\sigma_y - \sigma_y\sigma_z)(x) = \beta(y,x)z - \beta(z,x)y.$$

(d) Next we combine (b) and (c) and apply them to the transvection $E_{u,x}$ in G. Since G is $\Omega(V)$-normal and $\Phi_\varepsilon\sigma_z\sigma_y$ is in $\Omega(V)$ where z, y, and ε are as given in (c), we have

$$(\Phi_\varepsilon\sigma_z\sigma_y)E_{u,x}(\Phi_\varepsilon\sigma_z\sigma_y)^{-1} = E_{u,\varepsilon\sigma_z\sigma_y x}$$

is in G. Likewise, $E_{u,\varepsilon\sigma_y\sigma_z x}$ is in G. Thus,

$$E_{u,\varepsilon\sigma_z\sigma_y x}E^{-1}_{u,\varepsilon\sigma_y\sigma_z x} = E_{u,\varepsilon\sigma_z\sigma_y x}E_{u,-\varepsilon\sigma_y\sigma_z x}$$

$$= E_{u,\varepsilon\sigma_z\sigma_y x - \varepsilon\sigma_y\sigma_z x} = E_{u,\beta(y,x)z - \beta(z,x)y}$$

is in G. We now complete the proof by carefully choosing x, y, and z.

(e) Suppose $E_{u,x}$ is in G. Let W have an orthogonal basis $\{x_1,x_2,\cdots,x_m\}$ where $m = n - 2 \geqslant 3$. Then $x = \alpha_1x_1 + \cdots + \alpha_mx_m$ for α_i in R and $O(x) = (\alpha_1,\cdots,\alpha_m)$. We want to show $\Omega(V,O(x)) \subseteq G$. Since $\Omega(V,O(x)) = EO(V,O(x))$, we need to show $E_{u,\bar{x}}$ is in G where $O(\bar{x})$ is in $(\alpha_1,\cdots,\alpha_m)$. (A similar argument employing $E_{v,x}$ will place $E_{v,\bar{x}}$ in G.) If $\bar{x} = \delta_1x_1 + \cdots + \delta_mx_m$, then δ_i is in $O(x)$ and consequently, $\delta_i = \sum_j\mu_{ij}\alpha_j$. Hence, $\bar{x} = \sum_i \sum_j \mu_{ij}\alpha_jx_i$. Thus, if we are to show $E_{u,\bar{x}}$ is in G, we need first to show E_{u,α_jx_i} is in G for each i and j. Then, by (a), $E_{u,\mu_{ij}\alpha_jx_i}$ will be in G for all μ_{ij} in R. In turn,

$$E_{u,\bar{x}} = E_{u,\Sigma\mu_{ij}\alpha_jx_i} = \prod E_{u,\mu_{ij}\alpha_jx_i}$$

is in G. We use part (d) above, i.e., if y and z are nonisotropic in W with $\beta(y,z) = 1$, then

(*) $$E_{u,\beta(y,x)z - \beta(z,x)y}$$

is in G whenever $E_{u,x}$ is in G.

Let $\varepsilon_i = \beta(x_i,x_i)$ for $1 \leqslant i \leqslant n$. Let $y_i = \varepsilon_i^{-1}x_i$. Then $\beta(x_i,y_i) = 1$ for $1 \leqslant i \leqslant m$.

For $i \neq j$, since $(\varepsilon_i,\varepsilon_j) = R$ and R is strongly ⟨1,3⟩-full, there is a unit η so that with $z = x_i + \eta x_j$ and $y = y_i$, $\beta(z,z) = \varepsilon_i + \eta^2\varepsilon_j$ is a unit. Thus y and z are nonisotropic and $\beta(y,z) = 1$. By substituting in (*), $E_{u,\beta(y,x)z - \beta(z,x)y} = E_{u,\eta(\alpha_i x_j - \alpha_j\varepsilon_j y_i)}$. Thus, by part (a), $E_{u,\bar{\eta}(\alpha_i x_j - \alpha_j\varepsilon_j y_i)}$ is in G for all $\bar{\eta}$ in R.

Let $1 \leqslant i,j,k \leqslant m$ be distinct. (Recall $m \geqslant 3$). In (*) set

$$x = \alpha_i x_j - \alpha_j\varepsilon_j y_i,$$
$$z = x_k,$$
$$y = y_k + \delta y_j,$$

where δ is a unit such that $\beta(y,y) = \varepsilon_k^{-1} + \delta^2\varepsilon_j^{-1}$ is a unit, applying the fact that R is strongly full of type ⟨1,3⟩. Then $\beta(z,y) = 1$ and $E_{u,\beta(y,x)z - \beta(z,x)y} = E_{u,\delta\alpha_i x_k}$ is in G, where $i \neq k$. Since δ is a unit, by part (b), $E_{u,\alpha_i x_k}$ is in G for all i and k with $i \neq k$.

It remains to show $E_{u,\alpha_i x_i}$ is in G for $1 \leqslant i \leqslant m$. In (*) set

$$x = \alpha_i x_k,$$
$$z = x_k + \gamma x_i,$$
$$y = \varepsilon_k^{-1}x_k,$$

where γ is a unit such that $\beta(z,z)$ is a unit and $i \neq k$. Then $E_{u,\beta(y,x)z - \beta(z,x)y} = E_{u,\gamma\alpha_i x_i}$ and by (b), $E_{u,\alpha_i x_i}$ is in G. This completes the proof of the theorem. An analogous statement and proof will apply for $E_{v,x}$ in G.

If one is interested only in the case that G is a normal subgroup of O(V), square representability is nct necessary to prove the preceding theorem, as is shown next.

(IV.4) Theorem Let R be a ring which is strongly full of type $\langle 1,3\rangle$ and in which 2 is a unit. Assume dim(V) = 3 or $\geqslant 5$ and that V has hyperbolic rank $\geqslant 1$. If G is a normal subgroup of O(V) containing $E_{u,x}$, then $\Omega(V,O(x)) \leqslant G$.

Proof For any η in R, there is a δ in R such that both $\eta - \delta$ and $\eta + \delta$ are units: $(\eta^2,-1) = R$ implies there is a unit δ in R such that $\eta^2 - 1\cdot\delta^2$ is a unit. Since $\eta^2 - \delta^2 = (\eta - \delta)(\eta + \delta)$, both $\eta - \delta$ and $\eta + \delta$ are units.

If $E_{u,x}$ is in G, then $E_{u,\eta x}$ is in G for all η in R: Let δ be an element of R such that $\eta - \delta$ and $\eta + \delta$ are units. Then $\Phi_{\eta-\delta}E_{u,x}\Phi^{-1}_{\eta-\delta} = E_{u,\eta x - \delta x}$ is in G and $\Phi_{\eta+\delta}E_{u,x}\Phi^{-1}_{\eta+\delta} = E_{u,\eta x + \delta x}$ is in G, by normality of G. Thus $E_{u,\eta x - \delta x}E_{u,\eta x + \delta x} = E_{u,2\eta x}$ is in G, and $\Phi_{\frac{1}{2}}E_{u,2\eta x}\Phi^{-1}_{\frac{1}{2}} = E_{u,\eta x}$ is in G.

This shows that $\Omega(V,O(x)) \leqslant G$ in the case dim(V) = 3. For dim(V) $\geqslant 5$, the proof is exactly the same as parts (b) through (e) in the proof of (IV.3).

Now we can prove the main theorem of this chapter.

(IV.5) Theorem Let R be a ring which is strongly full of type $\langle 1,3\rangle$ and square representable and in which 2, 3, and 5 are units. Let dim(V) = 3 or dim(V) $\geqslant 5$ and assume V has hyperbolic rank $\geqslant 1$. Suppose G is a subgroup of O(V) normalized by $\Omega(V)$ and let A be an ideal which is maximal with respect to $\Omega(V,A) \leqslant G$. Then $\Omega(V,A) \leqslant G \leqslant O(V,A)$.

Proof Observe $\Omega(V,0) = I$ is always in G. Thus there exists an ideal B with $\Omega(V,B) \leqslant G$.

If $\{B_\lambda\}$, $\lambda \in \Lambda$, is a family of ideals satisfying $\Omega(V,B_\lambda) \leqslant G$, then since $EO(V,B_\lambda) = \Omega(V,B_\lambda)$, it is easy to see that $\Omega(V,\sum_\lambda B_\lambda) \leqslant G$. Thus the A in the statement of the theorem is unique and contains every ideal B with $\Omega(V,B) \leqslant G$.

Let ϕ be in G. There is a ψ in $\Omega(V)$ with $\psi\phi\psi^{-1} = E_{u,x}E_{v,y}\Phi_\varepsilon\theta$, where $E_{u,x}$ and $E_{v,y}$ are in G. Thus $\Phi_\varepsilon\theta$ is in G. For arbitrary z in W, we have, since $\theta|_H = I$, $[E_{u,-z},\Phi_\varepsilon\theta] = E_{u,\varepsilon\theta(z)-z}$ in G. Then $\Omega(V,O(\varepsilon\theta(z) - z)) \leqslant G$ and consequently, by the above remark, $O(\varepsilon\theta(z) - z) \subset A$. Therefore, $\varepsilon\theta(z) \equiv z \bmod A$. Select z in W with z nonisotropic, i.e., $\beta(z,z)$ is a unit. Then $\varepsilon^2\beta(\theta(z),\theta(z)) = \beta(\varepsilon\theta(z),\varepsilon\theta(z)) \equiv \beta(z,z) \bmod A$. Since $\beta(z,z)$ is a unit, $\varepsilon^2 \equiv 1 \bmod A$ and thus $\theta(z) \equiv \varepsilon z \bmod A$ for all z in W. If we apply the above to ϕ, $\phi(x) \equiv \varepsilon x \bmod A$ for all x in V. Let $\bar\phi = \lambda_A\phi$. Then $\bar\phi(x) = \varepsilon x$ for all x in V/AV. Let ψ be any element of O(V/AV). For any x in V/AV, $\psi\bar\phi(x) = \psi(\varepsilon x) = \varepsilon\psi(x) = \bar\phi\psi(x)$. Thus $\psi\bar\phi = \bar\phi\psi$, and $\bar\phi = \lambda_A\phi$ is in Center(O(V/AV)). This shows that ϕ is in O(V,A), and completes the proof.

Recall that if we ask G to be normal rather than $\Omega(V)$-normal, the assumptions that 5 is a unit and R is square representable may be omitted.

This chapter is concluded with several useful observations.

Remark Let G be a subgroup of O(V). The order of G, denoted O(G), is the smallest ideal A satisfying $\lambda_A G \leqslant \text{Center}(O(V/AV))$. Thus, since $\dim(V) \geqslant 3$, O(G) is the smallest ideal A with $\lambda_A\sigma = \pm I$ for all σ in G.

Suppose G is $\Omega(V)$-normal and $O(G) = A$. Under the hypothesis of the main theorem in this section, there is an ideal B with $\Omega(V,B) \leqslant G \leqslant O(V,B)$. Thus, since $G \leqslant O(V,B)$, we have A contained in B.

On the other hand, $\Omega(V,B) = EO(V,B)$ and clearly the generators of $EO(V,B)$ indicate $O(EO(V,B)) = B$. Hence $O(\Omega(V,B)) = B$ and since $\Omega(V,B) \leqslant G$, B is contained in A. Hence $A = B$. Thus, if G is an $\Omega(V)$-normal subgroup of $O(V)$ and $O(G) = A$, then

$$\Omega(V,A) \leqslant G \leqslant O(V,A).$$

Remark Suppose G is any subgroup of $O(V)$ satisfying $\Omega(V,A) \leqslant G \leqslant O(V,A)$ for an ideal A of R. Let σ be in $O(V)$ and τ be in G. Then $\sigma\tau\sigma^{-1}\tau^{-1}$ is in $\Omega(V,A)$ since τ is in $O(V,A)$. Hence $\sigma\tau\sigma^{-1}\tau^{-1} = \rho$ for some ρ in G since $\Omega(V,A)$ is in G. That is, $\sigma\tau\sigma^{-1} = \rho\tau$ is in G and G is normal in $O(V)$. Therefore, if G is any subgroup of $O(V)$ satisfying $\Omega(V,A) \leqslant G \leqslant O(V,A)$ for an ideal A, then G is normal (hence $\Omega(V)$-normal) in $O(V)$.

CHAPTER V

THE WITT RING

In this chapter, the Witt ring, W(R), is defined for a ring R which is full of type $\langle 1,3\rangle$ and has 2 a unit. Generators and relations for W(R) are given, the prime ideal theory is described, and some facts about nilpotent and torsion elements are shown. For a ring which is full of type $\langle 3,3\rangle$, the generators of the torsion part of W(R) are identified using the theory of round forms, particularly Pfister forms. The theory of Witt rings over semi-local rings is given in Baeza [4].

Let R be a ring which is full of type $\langle 1,3\rangle$ and has 2 a unit. Denote by Bil(R) the category of free symmetric inner product spaces over R. On Bil(R) we have the following operations:

For (V_1,β_1) and (V_2,β_2) in Bil(R),

(1) $(V_1,\beta_1) \perp (V_2,\beta_2) = (V_1 \oplus V_2,\beta)$ where β is defined by

$$\beta(x_1 + x_2,\ y_1 + y_2) = \beta_1(x_1,y_1) + \beta_2(x_2,y_2)$$

(2) $(V_1,\beta_1) \otimes (V_2,\beta_2) = (V_1 \otimes_R V_2,\ \beta_1 \otimes \beta_2)$ where $\beta_1 \otimes \beta_2$ is defined by

$$\beta_1 \otimes \beta_2(x_1 \otimes x_2,\ y_1 \otimes y_2) = \beta_1(x_1,y_1)\beta_2(x_2,y_2)$$

where x_i, y_i are in V_i.

Now in the category Bil(R) we construct the Grothendieck ring and obtain the Witt-Grothendieck ring $\hat{W}(R) = K_0(\text{Bil}(R))$ of free symmetric inner product spaces over R. The identity element of $\hat{W}(R)$ is represented by the one-dimensional space (1). An element x of $\hat{W}(R)$ has the form $x = [V_1] - [V_2]$ where $[V_i]$ is the isomorphism class of $V_i = (V_i,\beta_i)$. By definition, $[V_1] - [V_2] = [W_1] - [W_2]$ when there is a U in Bil(R) with $V_1 \perp W_2 \perp U \simeq W_1 \perp V_2 \perp U$. By cancellation (III.8), $V_1 \perp W_2 \simeq W_1 \perp V_2$.

In $\hat{W}(R)$ define $H(R) = \{[V_1] - [V_2]$: V_1 and V_2 are split spaces in Bil(R)$\}$. By (III.3), all split spaces are sums of hyperbolic planes, so that $H(R) = ZH$ where H is a hyperbolic plane.

(V.1) Proposition H(R) is an ideal of $\hat{W}(R)$.

Proof It is sufficient to show that for H a hyperbolic plane and (V,β) in Bil(R), $V \otimes H$ is in H(R). Since $H \simeq (1,-1)$, $V \otimes H \simeq (V \otimes 1) \perp (V \otimes -1) \simeq V \perp (-V)$, which is split. Thus $V \otimes H$ is in H(R).

(V.2) Definition $W(R) = \hat{W}(R)/H(R)$. W(R) is the Witt Ring of free symmetric inner product spaces over R.

In W(R), denote the class of a space (V,β) by $[V,\beta]$ or simply [V]. $[V,\beta]$ is called the Witt class of the space (V,β). Since $(V,\beta) \perp (V,-\beta)$ is split, $-[V,\beta] = [V,-\beta]$ in W(R). Thus every element of W(R) is the Witt class of some space, not just the difference of two Witt classes.

(V.3) Definition We call two spaces V and W over R equivalent or Witt-equivalent, and write $V \sim W$ if $[V] = [W]$ in W(R).

Clearly W(R) is the quotient of the semiring Bil(R) by this equivalence relation: $W(R) = \text{Bil}(R)/\sim$. We have the following description of Witt equivalence.

(V.4) Proposition Two spaces V and W over R are equivalent if and only if $V \perp nH \simeq W \perp mH$ for m, n nonnegative integers. (nH denotes the orthogonal sum of n hyperbolic planes.)

Proof If $[V] = [W]$, then in $\hat{W}(R)$, $[V] - [W] = [P] - [Q]$ with P, Q in $H(R)$. By definition of $\hat{W}(R)$, there is a space (U,β) in Bil(R) such that

$$V \perp Q \perp U \simeq W \perp P \perp U.$$

Add $-U$ to both sides. $Q \perp U \perp -U$ and $P \perp U \perp -U$ are split spaces, thus sums of hyperbolic planes.

Recalling the Witt decomposition (see III.5), every space V has a decomposition $V \simeq V_o \perp tH$ where V_o is anisotropic. By cancellation, the isomorphism class of V_o and the number $t \geqslant 0$ are uniquely determined by V. Observe that in W(R), $[V] = [V_o]$. V_o is called the kernel space of V.

(V.5) Corollary Two spaces V and W in Bil(R) are equivalent if and only if $V_o \simeq W_o$.

W( ) is a functor from the category of full rings of type $\langle 1,3 \rangle$ and ring morphisms to the category of rings and ring morphisms, as follows. Let α: $R \to S$ be a homomorphism of $\langle 1,3 \rangle$-full rings with 2 a unit, and let (V,β) be in Bil(R). S is an R-module via α and consequently $V \otimes_R S$ is a free S-module. On $V \otimes_R S$, define the bilinear form $\beta_S(x \otimes \lambda, y \otimes \mu) = \alpha(\beta(x,y))\lambda\mu$ for x, y in V and λ, μ in S. It is easy to check that $(V \otimes_R S, \beta_S)$ is in Bil(S). This construction is called scalar extension via α: $R \to S$. With it, one obtains an additive and multiplicative functor α^*: $\text{Bil}(R) \to \text{Bil}(S)$ which induces the Witt-Grothendieck ring homomorphism α^*: $\hat{W}(R) \to \hat{W}(S)$. Now suppose H is a hyperbolic plane in Bil(R), say $H = \langle u,v \rangle$, $\beta(u,u) = \beta(v,v) = 0$ and $\beta(u,v) = 1$. Then $H \otimes_R S$ has basis $\{u \otimes 1, v \otimes 1\}$ and $\beta_S(u \otimes 1, u \otimes 1)$ $= \alpha(\beta(u,u)) \cdot 1 \cdot 1 = 0$, $\beta_S(v \otimes 1, v \otimes 1) = \alpha(\beta(v,v)) \cdot 1 \cdot 1 = 0$,

$\beta_S(u \otimes 1, v \otimes 1) = \alpha(\beta(u,v))\cdot 1\cdot 1 = 1$. Thus $H \otimes_R S$ is a hyperbolic plane in Bil(S) and $\alpha^*H(R) \subset H(S)$. Then α^* induces a ring homomorphism α^*: $W(R) \to W(S)$.

Next we define two homomorphisms which are useful for examining the structure of W(R).

For spaces, we have the obvious homomorphism dim: Bil(R) → {non-negative integers}. This yields a homomorphism dim: $\hat{W}(R) \to Z$. Since dim(V) is even for any V in H(R), we obtain a ring homomorphism ν: $W(R) \to Z/2Z$ defined by $\nu([V]) = \dim(V) \bmod 2$. We usually write $\nu(V)$ instead of $\nu([V])$.

Let Q(R) denote the group $R^*/(R^*)^2$ of square classes of R. If $V = [a_{ij}]$ and $V' = [a'_{ij}]$ are isomorphic bilinear spaces over R, then $[a'_{ij}] = B^t[a_{ij}]B$ for some B in $GL_n(R)$. Taking determinants, $\det[a'_{ij}] = b^2 \det[a_{ij}]$ with $b = \det B$ a unit.

(V.6) <u>Definition</u> We call the square class $\det[a_{ij}](R^*)^2$ the <u>determinant</u> of the space V, denoted det(V), and we have shown that det(V) is a well-defined invariant of V.

For two spaces V and W over R, we have $\det(V \perp W) = \det(V)\det(W)$. Thus our invariant yields a determinant map det: $\hat{W}(R) \to Q(R)$ defined by $\det([V] - [W]) = \det(V)\det(W)$. (Notice that $\det([V] + [W] - [W]) = \det(V)\det(W)^2 = \det(V)$). Unfortunately, $\det(H) = \det([1] \perp [-1]) = -1(R^*)^2$. Thus, det does not factor through W(R). To repair this, let $(Z/2Z) \circ Q(R)$ denote the abelian group consisting of the pairs (ν,d) in $(Z/2Z) \times Q(R)$ with "twisted" multiplication $(\nu_1,d_1)(\nu_2,d_2) = (\nu_1 + \nu_2, (-1)^{\nu_1\nu_2}d_1d_2)$. Consider the map $z \to (n \bmod 2, (-1)^{n(n-1)/2}\det z)$ from $\hat{W}(R)$ to $(Z/2Z) \circ Q(R)$, where $n = \dim z$. This map is a group homomorphism and vanishes on H. Thus it induces a map $(\nu,d)\colon W(R) \to (Z/2Z) \circ Q(R)$ by $(\nu,d)(z) = (\nu(z), d(z))$. The second component of this map, $d\colon W(R) \to Q(R)$ is defined by $d([V]) = (-1)^{n(n-1)/2}\det(V)$ and is called the signed determinant. This square class is denoted by $d(V)$. For spaces V, W over R, $d(V \perp W) = (-1)^{\nu(V)\nu(W)} d(V)\, d(W)$.

$Q(R)$ can be regarded as the group of isomorphism classes (a) of dimension 1 over R with the tensor product as multiplication. We have a natural map $(a) \to [(a)]$ from $Q(R)$ to $W(R)$. Since $d([(a)]) = a(R^*)^2$, this map is injective. Henceforth we regard $Q(R)$ as a subset of $W(R)$, i.e., we identify a square class $a(R^*)^2$ with the Witt class $[(a)]$. Now $Q(R)$ is a subgroup of the group of units $W(R)^*$ of the ring $W(R)$.

For convenience, let $G = Q(R) = R^*/(R^*)^2$.

(V.7) Proposition W(R) is additively generated by G.

Proof Let V be in Bil(R). V has an orthogonal basis, so $V = (a_1) \perp (a_2) \perp \cdots \perp (a_n) = (a_1,a_2,\cdots,a_n)$ where a_i is a unit, $n = \dim(V)$. In $W(R)$ we have the equation $V = [(a_1)] + [(a_2)] + \cdots + [(a_n)]$.

According to this proposition we have a surjective homomorphism from the integral group ring $Z[G]$ to $W(R)$, $\Phi\colon Z[G] \to W(R)$ induced by the inclusion map from G to $W(R)$. If we consider a square class $a(R^*)^2$ as an element of $Z[G]$ we denote this square class by $\langle a \rangle$. The homomorphism Φ maps $\langle a \rangle$ to $[(a)]$. Let K denote the kernel of Φ.

(V.8) Proposition The ideal K is additively generated by the element $\langle 1 \rangle + \langle -1 \rangle$ and all elements

$$z = \sum_{i=1}^{n} \langle a_i \rangle - \sum_{i=1}^{n} \langle b_i \rangle,$$

for n any positive integer and where $\perp_{i=1}^{n} (a_i) \simeq \perp_{i=1}^{n} (b_i)$.

Proof Clearly all of these elements lie in K. Now let z be a given element of K. We have $z = \langle a_1\rangle + \cdots + \langle a_r\rangle - \langle b_1\rangle - \cdots - \langle b_s\rangle$ where a_i, b_j are units. Replacing z by $-z$ if necessary, we may assume $r \geqslant s$. The spaces $V = (a_1,\cdots,a_r)$ and $W = (b_1,\cdots,b_s)$ are Witt-equivalent. In particular, since $[V] - [W] = 0$ in W(R), the difference in $\hat{W}(R)$ is a sum of hyperbolic planes, so $r - s$ is an even number, say 2t. Then in $\hat{W}(R)$, V and $W \perp t(1,-1)$ have the same image. Thus $V \simeq W \perp t(1,-1)$. For $s < i \leqslant r$, let $b_i = \pm 1$ so that $W \perp t(1,-1) = (b_1,b_2,\cdots,b_r)$. Then we have $z = t(\langle 1\rangle + \langle -1\rangle) + \sum_{i=1}^n \langle a_i\rangle - \sum_{i=1}^n \langle b_i\rangle$.

(V.9) Theorem W(R) is additively generated by $\{(a)\colon a \in R^*\}$ with the following relations:

(i) $(ab^2) = (a)$ for all b in R^*.

(ii) $(a_1) + (a_2) + \cdots + (a_n) = (b_1) + \cdots + (b_n)$ if and only if

$$(a_1) \perp \cdots \perp (a_n) \simeq (b_1) \perp \cdots \perp (b_n).$$

(iii) $(a) + (-a) = 0$

(iv) $(a) + (b) = (a + b) + (ab(a + b))$ if $a + b \in R^*$.

(v) $(a)(b) = (ab)$

Proof Using $W(R) \cong Z[R^*/(R^*)^2]/K$, parts (i), (ii), (iii) and (v) clearly hold in W(R). To see that (iv) holds, suppose $(V,\beta) = (a) \perp (b)$ has basis elements x, y with $\beta(x,y) = 0$, $\beta(x,x) = a$, $\beta(y,y) = b$. Then $\beta(x + y, x + y) = a + b$ is a unit implies that there exists z in V such that $\{x + y, z\}$ is an orthogonal basis for V, i.e., $V = (a + b) \perp (c)$ where $\beta(z,z) = c$ is a unit. Now comparing determinants, $ab \equiv (a + b)c$ and since $(a + b) \equiv (a + b)^{-1} \bmod (R^*)^2$, $c \equiv ab(a + b) \bmod (R^*)^2$. Thus $(a) \perp (b) \simeq (a + b) \perp (ab(a + b))$. Notice that (iv) is a result of (i) and (ii).

Now let S be a ring generated by $\{(a): a \in R^*\}$ with relations (i) through (v). Since these relations hold in W(R), there is a canonical ring homomorphism h: $S \to W(R)$ which maps (a) in S to the class of the bilinear space (a) in W(R). h is clearly surjective. Suppose $h(\sum_{i=1}^{n} (a_i)) = 0$ in W(R). Then $(a_1) \perp \cdots \perp (a_n)$ is a sum of hyperbolic planes. That is, n is even, and $(a_1) \perp \cdots \perp (a_n) \approx \frac{1}{2}nH$, so $(a_1) \perp \cdots \perp (a_n) = \frac{1}{2}n((1) + (-1)) = 0$. Thus, h is injective, hence an isomorphism.

Since W(R) is isomorphic in a natural way to the quotient Z[Q(R)]/K, the prime ideals of W(R) correspond uniquely with those prime ideals of Z[Q(R)] which contain K. Thus, to determine the prime ideals of W(R), we determine the prime ideals of Z[Q(R)] and then look at which of them contain K.

The prime ideals of Z[G], for G any group of exponent 2 (i.e., $g^2 = 1$ for all g in G), are determined by Knebusch in [25], pp. 166-169.

Denote by I(R) the kernel of ν: $W(R) \to Z/2Z$. From [25], Proposition 1 (iii), p. 167, we obtain:

(V.10) Proposition I(R) is the unique prime ideal of W(R) which contains $2\cdot 1_{W(R)}$.

(Observe that the generators of K are even-dimensional and thus are contained in I(R)).

(V.11) Definition A signature σ of R is a ring homomorphism from W(R) to Z.

The kernel of a signature σ is denoted by P_σ; thus, $W(R)/P_\sigma \cong Z$. Part (i) of Proposition 1, in [25] gives the following.

(V.12) Proposition For every prime ideal P of W(R) which does not contain $p\cdot 1_{W(R)}$ for any rational prime p, there exists a unique signature σ such that $P = P_\sigma$.

Recall that a character of a group G is a homomorphism x: G → {±1}. x extends uniquely to a ring homomorphism x: Z[G] → Z. To analyze the prime ideals P of W(R) which contain $p\cdot 1_{W(R)}$ for p an odd prime, we need the following information about the ideal K.

(V.13) Lemma For every character x of $G = R^*/(R^*)^2$ either $x(K) = 0$ or $x(K) = 2^n Z$ for some $n \geqslant 1$.

Proof We know the additive generators of K, by (V.8). On (1) + (-1), every character x has value 0 or 2, since x(1) = 1. We claim that on an element $z = \sum_{i=1}^n \langle a_i\rangle - \sum_{i=1}^n \langle b_i\rangle$, x has a value 0 or 4n, n an integer. To prove the claim, let s be the number of square classes $\langle a_i\rangle$ with $x(\langle a_i\rangle) = -1$ and let t be the number of classes $\langle b_i\rangle$ with $x(\langle b_i\rangle) = -1$. Then $x(z) = -s + (n - s) + t - (n - t) = 2(t - s)$. Now for z a generator of K, the spaces $(a_1,\cdots,a_n)$ and $(b_1,\cdots,b_n)$ are isomorphic, so they have the same determinant, $\prod_{i=1}^n a_i = \prod_{i=1}^n b_i$. Applying x we obtain $(-1)^s = (-1)^t$. Thus t - s is even. This implies $x(z) \equiv 0 \mod 4$.

From this lemma it is clear that if $x(K) \subset pZ$ for an odd prime p, then $x(K) = 0$. Thus we obtain from part (ii) of Proposition 1 in [25], the following.

(V.14) Proposition Let p be an odd prime. Then for every prime ideal M of W(R) with $p\cdot 1_{W(R)}$ in M there exists a unique signature σ of R such that M coincides with the set $M_{\sigma,p} = pZ + P_\sigma$ consisting of all z in W(R) with $\sigma(z) \equiv 0 \mod p$.

Thus the P_σ, the $M_{\sigma,p}$, and $I(R)$ are all the prime ideals of $W(R)$. The ring R is called <u>real</u> (or <u>formally real</u>) if R has at least one signature. Otherwise R is called <u>non-real</u>. This description of the prime ideals of $W(R)$ implies the following.

(V.15) <u>Corollary</u> Assume R is real. Then the P_σ are the minimal prime ideals of $W(R)$. The ideals $M_{\sigma,p}$ and $I(R)$ are the maximal ideals of $W(R)$. Every $M_{\sigma,p}$ contains a unique minimal prime ideal, which is P_σ. The ideal $I(R)$ contains all minimal prime ideals.

(V.16) <u>Proposition</u> The following are equivalent:

(a) R is non-real.

(b) $I(R)$ is the unique prime ideal of $W(R)$.

(c) $2^n W(R) = 0$ for some positive integer n.

<u>Proof</u> The equivalence of (a) and (b) is evident from our analysis of the prime ideals of $W(R)$. (c) implies (a) is trivial since $W(R)$ does not admit homomorphisms to Z if $W(R)$ consists entirely of torsion elements. It remains to prove (b) implies (c). By (b) and elementary commutative algebra, $I(R)$ is the nilradical of $W(R)$. In particular $2\cdot 1_{W(R)}$ is nilpotent, hence $2^n\cdot 1_{W(R)} = 0$ for some n. Then $2^n W(R) = 0$.

Next we consider the nilpotent and torsion elements of $W(R)$ for R a $\langle 1,3\rangle$-full ring with 2 a unit.

If R is non-real we know that all elements of $W(R)$ are torsion, annihilated by a fixed power of 2. Moreover, $I(R)$ is the set of all nilpotent elements.

From now on, we assume that R is real. Since the P_σ are precisely all minimal prime ideals of $W(R)$ we have the following characterization.

(V.17) *Proposition* An element z of W(R) is nilpotent if and only if $\sigma(z) = 0$ for every signature σ of R.

Now we consider the torsion elements of W(R).

(V.18) *Theorem* An element z of W(R) is a torsion element if and only if z is nilpotent.

Proof Assume $nz = 0$ for some $n \geqslant 1$. Then certainly $\sigma(z) = 0$ for all signatures σ of R, hence z is nilpotent. The proof of the converse follows exactly the proof given by Knebusch in [25], and will be omitted.

(V.19) *Corollary* All zero-divisors of W(R) have even dimension.

Proof P_σ is contained in I(R) for every signature σ of R.

(V.20) *Proposition* For every torsion element z of W(R) there exists a 2-power 2^r with $2^r z = 0$.

Proof The proof given by Kenbusch ([25]) carries over without change.

Next we explore some useful properties of signatures.

Let σ be a signature of R, that is, a ring homomorphism from W(R) to Z. σ yields a homomorphism $R^* \xrightarrow{\pi} Q(R) = R^*/(R^*)^2 \xrightarrow{\sigma|_{Q(R)}} \{\pm 1\}$ where π is the canonical map. σ is completely determined by the composite homomorphism from R* to {±1}, since W(R) is generated by Q(R). Henceforth we identify a signature σ and the corresponding map from R* to {±1}, and write $\sigma(a)$ instead of $\sigma([(a)])$.

(V.21) *Proposition* If a map σ: R* → {±1} is a signature then the following properties hold:

(i) $\sigma(ab) = \sigma(a)\sigma(b)$ for a, b in R*,

(ii) $\sigma(-1) = -1$,

(iii) If $a_1, a_2, \cdots, a_r$ are units with $\sigma(a_i) = 1$, $1 \leqslant i \leqslant r$, then for any unit $b = \lambda_1{}^2 a_1 + \cdots + \lambda_r{}^2 a_r$ for λ_i in R, $\sigma(b) = 1$.

Proof (i) and (ii) are evident from the fact that σ is a ring homomorphism. To prove (iii), consider the bilinear space $(a_1,a_2,\cdots,a_r)$. This space contains a vector x with $\beta(x,x) = b$. Thus $(a_1,\cdots,a_r) = (b) \perp (b)^\perp$. Let $G = (b)^\perp$, the orthogonal complement of Rx. The space $G \perp (1)$ has an orthogonal basis. Thus $(1,a_1,\cdots,a_r) \simeq (b,b_1,\cdots,b_r)$ for b_i in R*. Computing the values of σ on the classes of these two spaces, we obtain $r + 1 = \sigma(b) + \sigma(b_1) + \cdots + \sigma(b_r)$. Since each summand on the right side is either 1 or -1, they must be 1. In particular, $\sigma(b) = 1$.

(V.22) Theorem Let R be a $\langle 1,3 \rangle$-full ring in which 2 is a unit. Let $a_1,\cdots,a_r$ be units of R. Then for any unit b of R the following statements are equivalent:

(a) For every signature σ of R with $\sigma(a_i) = 1$ for $1 \leqslant i \leqslant r$, also $\sigma(b) = 1$.

(b) The unit b can be expressed in the form

$$b = \sum_{i_k = 0 \text{ or } 1} d_{i_1,\cdots,i_r} a_1^{i_1} \cdots a_r^{i_r}$$

with coefficients $d_{i_1,\cdots,i_r}$ which are sums of squares of elements in R.

Proof (b) implies (a) is evident from (V.21). To prove (a) implies (b), consider the "Pfister forms" $F = (1,a_1) \otimes (1,a_2) \otimes \cdots \otimes (1,a_r)$ and $E = (1,-b) \otimes F = F \perp (-b) \otimes F$. Assumption (a) implies $\sigma(E) = 0$ for all signatures σ of R. Thus the class of E in W(R) is nilpotent (V.17) hence torsion (V.18), and there exists some natural number m (actually, a power of 2) such that $mE \sim 0$. From this, $mF \sim m(b) \otimes F$. Since mF and $m(b) \otimes F$ have the same dimension, it follows that $mF \cong m(b) \otimes F$. Since F represents 1 (i.e., for some x in F, $\beta(x,x) = 1$), the space $(b) \otimes F$ represents b, so mF represents b. This gives the desired expression for b with sums of m squares as coefficients.

(V.23) Corollary The units of R which have the value +1 under all signatures are precisely the units which are sums of squares.

Proof This is the special case $r = 1$, $a_1 = 1$ of (V.22).

(V.24) Corollary Let R be a full ring of type $\langle 1,3 \rangle$ with 2 a unit. Then R is non-real if and only if -1 is a sum of squares.

Proof If -1 is a sum of squares, then from (V.21)(iii) it is clear that R has no signatures. Now suppose R is non-real. In (V.21), take $r = 1$, $a_1 = 1$, $b = -1$. We see that $b = -1$ is a sum of squares.

Let $W(R)_t$ denote the torsion part of $W(R)$.

(V.25) Proposition If $W(R)_t = 0$, then any unit a of R which is a sum of squares is itself a square, but -1 is not a square.

Proof If a is a sum of squares, by (V.23), $\sigma(a) = 1$ for all signatures σ of R. Hence $\sigma([(1,-a)]) = 0$ for each σ, so $[(1,-a)]$ is in $W(R)_t$, by (V.17). Thus $[(1,-a)] = 0$, or $[a] \sim [1]$. This implies $a \equiv 1 \bmod (R^*)^2$, i.e., a is a square. Now $W(R)_t = 0$ implies $W(R)_t \neq W(R)$ so R is real and the set of signatures on R is non-empty. Thus -1 is not a square, by (V.21)(ii) and (V.23).

The converse of (V.25) will be proven for rings which are full of type $\langle 3,3 \rangle$, farther in this chapter.

We give one further description of $W(R)_t$.

(V.26) Theorem Let $M = \{a \text{ in } R^*: a \text{ is a sum of squares}\}$. If $W(R)_t \neq W(R)$, then

$$W(R)_t = \cup \operatorname{Ann}[(1,a_1) \otimes \cdots \otimes (1,a_r)]$$

where a_i is in M for each i and r runs through integers $\geqslant 0$.

Proof Let A denote the right-hand side. If x is in A, then $x[(1,a_1)][(1,a_2)]\cdots[(1,a_r)] = 0$ for some a_i in M. Since $\sigma(a_i) = 1$ for any a_i in M (V.23), we have $2^r\sigma(x) = 0$, so $\sigma(x) = 0$, for all signatures σ of R. Thus x is a torsion element. On the other hand, if x is torsion, there is an integer n with $2^n x = 0$. Therefore, $x[(1,1)]^n = 0$, and x is in A.

A powerful stimulus for the study of Witt rings was Pfister's theory of multiplicative forms, which was simplified by the concept of a round form, introduced by Witt and later generalized by Knebusch [22]. For a nice summary of the historical development, see Hsia [18]. We next study round forms over a full ring of type $\langle 3,3\rangle$.

At first, R will be a full ring of type $\langle 1,3\rangle$ with 2 a unit. Let (V,β) be in Bil(R). $D(V)^*$ or $D(\beta)^*$ denotes the set of units of R represented by β; that is,

$$D(V)^* = \{\beta(x,x) \text{ in } R^* \mid x \text{ is in } V\}$$

A unit λ of R is called a similarity norm of (V,β) if $(V,\beta) \simeq (\lambda) \otimes (V,\beta)$. $N(\beta)$ denotes the group of similarity norms of (V,β). For example, λ is in $N(\beta)$ means that there is an R-linear isomorphism $\sigma: V \to V$ with $\beta(\sigma(x),\sigma(x)) = \lambda\beta(x,x)$ for each x in V. σ is called a similarity with norm λ.

If 1 is in $D(\beta)$, it follows that $N(\beta) \subset D(\beta)^*$, since if $\sigma: E \to E$ is a similarity with norm λ and $\beta(x,x) = 1$, then $\beta(\sigma(x),\sigma(x)) = \lambda\beta(x,x) = \lambda\cdot 1$ so λ is in $D(\beta)$.

(V.27) Definition A bilinear space (V,β) is called round if $N(\beta) = D(\beta)^*$.

Remark If $D(\beta)^* \subset N(\beta)$, then (V,β) is round. To show this, we need only show 1 is in $D(\beta)$. Suppose $\beta(x,x)$ is in $D(\beta)^*$. Since $\beta(x,x)$ is in $N(\beta)$, there is a similarity σ of (V,β) with norm $\beta(x,x)$. So $\beta(\sigma(z),\sigma(z)) = \beta(x,x)\beta(z,z)$ for every z in V. In particular, for $z = x$, $\beta(\beta(x,x)^{-1}\sigma(x), \beta(x,x)^{-1}\sigma(x)) = \beta(x,x)^{-2}\beta(x,x)\beta(x,x) = 1$, so 1 is in $D(\beta)$.

An example of a round form is given in the following lemma.

(V.28) Lemma Let b be a unit of R. Then the bilinear space $(1,b)$ is round.

Proof Let $(1,b)$ have basis $\{x,y\}$ where $\beta(x,x) = 1$, $\beta(y,y) = b$, $\beta(x,y) = 0$. Let $z = \alpha x + \gamma y$ be in $(1,b)$ with $\beta(z,z)$ a unit. Then the matrix

$$T = \begin{bmatrix} \alpha & \gamma \\ -b\gamma & \alpha \end{bmatrix}$$

is a similarity of $(1,b)$ with norm $\beta(z,z) = \alpha^2 + \gamma^2 b$.

Several easy observations about round spaces can be made. If V is a round form, V must represent 1, since $1 \otimes V \simeq V$. Also, if r and s are both represented by V, so is their product, since $rs \otimes V \simeq r \otimes (s \otimes V) \simeq r \otimes V \simeq V$. If r is represented by V, so is $r^{-1} = r^{-2}r$. Therefore, the set of units represented by a round form is a multiplicative group. Since in our setting every space has an orthogonal basis, it is easy to see that a round form represents its own determinant.

Since round forms always represent 1, any one-dimensional round form is isomorphic to (1). A two-dimensional form is round if and only if it has the form $(1,a)$ where a is a unit.

(V.29) Proposition Let (V,β) be a round form in Bil(R) of odd dimension. If c is in $D(\beta)^*$, then c is a square.

Proof Since c is in $D(\beta)^* = N(\beta)$, $c \otimes V \simeq V$ and $\det(c \otimes V) = \det(V)$. Thus $c^{\dim(V)} \det(V) = \det(V)$. Thus $c^{\dim(V)} \equiv 1 \bmod (R^*)^2$. Since dim(V) is odd, this gives $c \equiv 1 \bmod (R^*)^2$, and c is a square.

Thus, if V is round of odd dimension, V has a diagonalization $(1,1,\cdots,1) = n\cdot(1)$, and every element of the ring R which is represented by V is not only a sum of squares but a square itself.

(V.30) Lemma If V is in Bil(R) and $V \perp H$ is round, then V is round and $D(V)^* = R^*$.

Proof Let x be in V with $\beta(x,x)$ a unit. Then $\beta(x,x)$ is in $D(V \perp H)^*$ so $\beta(x,x) \otimes (V \perp H) \simeq V \perp H$. But $\beta(x,x) \otimes (V \perp H) = (\beta(x,x) \otimes V) \perp (\beta(x,x) \otimes H)$. Now since 2 is a unit, $H = (1,-1)$ represents any r in R: $r = (\frac{1}{2}(1 + r))^2\cdot 1 + (\frac{1}{2}(1 - r))^2(-1)$. Also, by (V.28), H is round. So $\beta(x,x) \otimes (V \perp H) = (\beta(x,x) \otimes V) \perp H \simeq V \perp H$. By cancellation, $\beta(x,x) \otimes V \simeq V$.

To show $D(V)^* = R^*$, observe that since $D(H)^* = R^*$, $D(V \perp H)^* = R^*$. Then for any unit r, $r \otimes (V \perp H) \simeq (r \otimes V) \perp (r \otimes H) \simeq (r \otimes V) \perp H$. $V \perp H$ is round implies $r \otimes (V \perp H) \simeq V \perp H$. Thus $V \perp H \simeq (r \otimes V) \perp H$ and by cancellation, $V \simeq r \otimes V$. Thus $R^* = D(V)^*$.

The next theorem, (V.33), shows how to build a new round form from other round forms, when R is full of type $\langle 3,3 \rangle$. The proof of the theorem uses the following lemma.

(V.32) Lemma Let a be a unit in R and let V be in Bil(R). Suppose η is in R such that $1 + a\eta^2$ is a unit. Let $\{x,y\}$ be the orthogonal basis for the diagonal space $(1,a)$. The map $(1,a) \otimes V \to (1,a) \otimes V$ defined by $\theta \otimes \mathrm{id}_V$ where $\theta(x) = x + \eta y$, $\theta(y) = a\eta x - y$ is a similarity of $(1,a) \otimes E$ with norm $1 + a\eta^2$.

Proof The claim may be verified directly by computation. Observe that the matrix of θ with respect to the basis $\{x,y\}$ is

$$\begin{bmatrix} 1 & a\eta \\ \eta & -1 \end{bmatrix}$$

which has determinant $-(1 + a\eta^2)$.

(V.33) Theorem Let R be a ring which is full of type $\langle 3,3 \rangle$ and has 2 a unit. Let (V,β) be a round space in Bil(R). Then for every a in R*, $(1,a) \otimes V$ is round.

Proof Let $W = (1,a) \otimes V = V \perp (a) \otimes V$. Choose t in (a) with $\beta(t,t) = a$; that is, $Rt = (a)$. For ease of notation, we write n(x) for the norm of x, the inner product of x with itself. For an arbitrary element $x + t \otimes y$ of W (x,y in V),

$$n(x + t \otimes y) = n(x) + an(y).$$

If $n(x) + an(y)$ is a unit, we must show $(n(x) + an(y)) \otimes W \simeq W$. We consider two cases.

Case I. Suppose n(x) and n(y) are both units. Then because V is round, $n(x) \otimes V \simeq V$ and $n(y) \otimes V \simeq V$. Therefore, $(1,a) \otimes V \simeq (1,an(x)n(y)) \otimes V$. So $(n(x) + an(y)) \otimes W \simeq (n(x) + an(y)) \otimes (1,an(x)n(y)) \otimes V$. On the other hand, for two units λ, μ with $\lambda + \mu$ a unit,

(*) $$(\lambda) \perp (\mu) \simeq (\lambda + \mu) \otimes (1,\lambda\mu).$$

Applying (*) to $\lambda = n(x)$ and $\mu = an(y)$, it follows that

$$\begin{aligned}(n(x) + an(y)) \otimes W &\simeq [(n(x)) \perp (an(y))] \otimes V \\ &\simeq (n(x) \otimes V) \perp (an(y) \otimes V) \\ &\simeq V \perp (a) \otimes V \simeq W.\end{aligned}$$

Case II. Suppose $n(x)$ and $n(y)$ are not both units. Consider the following matrix over R:

$$A = \begin{bmatrix} 1 & 0 & a \\ n(x) & -2a\beta(x,y) & a^2n(y) \\ n(y) & 2\beta(x,y) & n(x) \end{bmatrix}$$

Since $n(x) + an(y)$ is a unit and a is a unit, A has unimodular rows. Since R is full of type $\langle 3,3\rangle$, there exists an η in R with

$$A[1,\eta,\eta^2]^t = [u_1,u_2,u_3]^t$$

where u_1, u_2, u_3 are units. Now let $x' = x - a\eta y$ and $y' = y + \eta x$. Then $n(x') = n(x) - 2a\eta\beta(x,y) + a^2\eta^2n(y) = u_2$; $n(y') = n(y) + 2\eta\beta(x,y) + \eta^2n(x) = u_3$; and $n(x') + an(y') = (1 + a\eta^2)(n(x) + an(y)) = u_1(n(x) + an(y))$ is a unit. By the lemma (V.32), $(1 + a\eta^2) \otimes W \simeq W$. Applying case I gives $(n(x') + an(y')) \otimes W \simeq W$. This gives

$$W \simeq (1 + a\eta^2)(n(x) + an(y)) \otimes W \simeq (n(x) + an(y)) \otimes W,$$

which is what we wanted to show.

(V.34) <u>Definition</u> A bilinear space of the form $(1,a_1) \otimes (1,a_2) \otimes \cdots \otimes (1,a_n)$, where each a_i is a unit, is called a <u>bilinear Pfister-space</u>, or a <u>bilinear Pfister-form</u>.

(V.35) <u>Corollary</u> If R is full of type $\langle 3,3\rangle$ having 2 a unit, then every bilinear Pfister form ϕ over R is round.

<u>Proof</u> Use induction on n where $\phi = (1,a_1) \otimes \cdots \otimes (1,a_n)$. $(1,a_i)$ is round by (V.28).

(V.36) <u>Corollary</u> Let $n \geq 1$ be a positive integer. Let R be a $\langle 3,3\rangle$-full ring having 2 a unit, and let S represent the set of units of R which are sums of 2^n squares. Then S is a subgroup of R*.

Proof The 2^n-dimensional form $\phi = (1,1) \otimes (1,1) \otimes \cdots \otimes (1,1)$ (n factors) is round, by (V.34). Observe that $S = D(\phi)^*$, which, as we have already seen, is a group.

The next theorem identifies the generators of the annihilator ideal of a round form and leads to the promised converse of (V.25).

(V.37) Theorem Let R be a ring which is full of type $\langle 3,3 \rangle$ having 2 a unit. If V is a round space over R, $V \not\sim 0$, then the annihilator ideal Ann(V) in W(R) is generated by the spaces $(1,-\lambda)$ with λ a unit represented by V.

Proof We may assume V is anisotropic, since the kernel space V_o is round and represents the same units as V (see (V.30)). Let I be the ideal of W(R) generated by $\{(1,-\lambda): \lambda$ is a unit represented by $V\}$. Since $(1,-\lambda) \otimes V = V \perp (-\lambda) \otimes V \simeq V \perp -V \sim 0$, we have $I \subseteq \mathrm{Ann}(V)$.

We will use the following observation: Let b be a unit of R and let c be a unit of the form $c = n(x) + b\eta^2 n(y)$ with $n(x)$ and $n(y)$ units and η an element of R, x and y elements of V. c is represented by the round space $(1,b) \otimes V$, so that $(c) \otimes (1,b) \otimes V \simeq (1,b) \otimes V$ and thus $(1,-c) \otimes (1,b) \otimes V \sim 0$. Now consider the space $F = (n(x), bn(y), -c, -bc)$. The subspace $(n(x), bn(y))$ represents the unit $c = n(x) + b\eta^2 n(y)$, so F can be written as $(c,t,-c,-bc)$ where t is a unit. Comparing determinants of the two diagonalizations of F, $n(x)n(y)b \equiv ct \mod (R^*)^2$, so $t \equiv bcn(x)n(y) \mod (R^*)^2$. Then

$$F = (c, bcn(x)n(y), -c, -bc) \sim (bcn(x)n(y), -bc)$$
$$= (-bc) \otimes (1, -n(x)n(y))$$

which is in I. Thus $F \equiv 0 \mod I$. On the other hand,

$$(1,-c) \otimes (1,b) - F = (1,-c,b,-bc,-n(x),-bn(y),c,bc)$$
$$\sim (1,b,-n(x),-bn(y)) = (1,-n(x)) \perp b \otimes (1,-n(y)),$$

which is also in I. Thus, $(1,-c) \otimes (1,b) \equiv F \equiv 0 \bmod I$. Thus $(1,b) \equiv (c) \otimes (1,b) \bmod I$.

Congruences of this type will be used in the remainder of the proof.

Assume $\mathrm{Ann}(V) \not\subset I$. Let $F = (b_1,\cdots,b_n)$ be a space of minimal dimension n with F not in I and $F \otimes V \sim 0$. The space $(b_2,\cdots,b_n) \otimes V$ must have kernel space isomorphic to $(-b_1) \otimes V$. Since V represents 1, $(-b_1) \otimes V$ represents $-b_1$, and there is an equation

$$b_1 + b_2 n(x_2) + \cdots + b_n n(x_n) = 0$$

with x_i in V. We will alter F modulo I to a space $F' = (b_1',\cdots,b_n')$ so that $b_1' + b_2' + \cdots + b_n' = 0$.

First, we find a unit c of the form $1 + \eta^2 b_2/b_1$ such that $c(b_1 + b_2 n(x_2)) = b_1 n(x_1') + b_2 n(x_2')$ with x_1' and x_2' in V and $n(x_1')$ and $n(x_2')$ both units. Let x_1 be in V with $n(x_1) = 1$. Let A be the matrix

$$\begin{bmatrix} 1 & 0 & b_2/b_1 \\ n(x_1) & -2(b_2/b_1)\beta(x_1,x_2) & (b_2/b_1)^2 n(x_2) \\ n(x_2) & 2\beta(x_1,x_2) & n(x_1) \end{bmatrix}$$

A has unimodular rows. Then since R is full of type $\langle 3,3\rangle$, there is an η in R such that $A[1,\eta,\eta^2]^t = [u_1,u_2,u_3]^t$ where u_1, u_2, u_3 are units. Let $x_1' = x_1 - (b_2/b_1)\eta x_2$ and $x_2' = x_2 + \eta x_1$. Then $n(x_1') = u_2$, $n(x_2') = u_3$, and $n(x_1') + (b_2/b_1)n(x_2') = (1 + \eta^2 b_2/b_1)(n(x_1) + (b_2/b_1)n(x_2))$. Multiplying both sides of this equation by b_1 gives

$$\begin{aligned} b_1 n(x_1') + b_2 n(x_2') &= (1 + \eta^2 b_2/b_1)(b_1 n(x_1) + b_2 n(x_2)) \\ &= (1 + \eta^2 b_2/b_1)(b_1 + b_2 n(x_2). \end{aligned}$$

Let $c = 1 + \eta^2 b_2/b_1$.

Claim: $(b_1,b_2,\cdots,b_n) \equiv (c^{-1}b_1,c^{-1}b_2,b_3,\cdots,b_n)$ mod I.

Proof of claim: As in the earlier observation, $(1,-c^{-1}) \otimes (1,b_2/b_1)$ is in I, so $b_1 \otimes (1,-c^{-1}) \otimes (1,b_2/b_1) = (1,-c^{-1}) \otimes (b_1,b_2)$ is in I, and thus $(b_1,b_2) \equiv (c^{-1}b_1,c^{-1}b_2)$ mod I. Now let $b_1' = c^{-1}b_1 n(x_1')$ and $b_2' = c_2^{-1}b_2 n(x_2')$. Since x_1' and x_2' are in V and have unit norms, $(c^{-1}b_1,c^{-1}b_2,b_3,\cdots,b_n) \equiv (b_1',b_2',b_3,\cdots,b_n)$ mod I. Further, $b_1 n(x_1) + b_2 n(x_2) = c^{-1}b_1 n(x_1') + c^{-1}b_2 n(x_2')$ so that $b_1' + b_2' + b_3 + \cdots + b_n = 0$.

This process is continued (next using b_1' and $b_3 n(x_3)$) until $F \equiv (b_1',b_2',\cdots,b_n')$ mod I with $b_1' + \cdots + b_n' = 0$. Let $e_1,e_2,\cdots,e_n$ be the orthogonal basis of $F' = (b_1',b_2',\cdots,b_n')$ with $n(e_i') = b_i'$. The vector $e_1 + e_2 + \cdots + e_n$ is isotropic. Then $F' = H \perp G$ where H is a hyperbolic plane and $\dim(G) = n - 2$. $F \not\equiv 0$ mod I and H is in I, so $G \not\equiv 0$ mod I. But $0 \sim F \otimes V \sim H \otimes V \perp G \otimes V \sim G \otimes V$. This contradicts the minimality of $\dim(F)$. (Notice that $\dim F > 2$, since if $n = 2$, this argument shows $F = H$ which is in I, contrary to the choice of F.)

(V.38) Corollary If R is a full ring of type $\langle 3,3\rangle$ with 2 a unit, $W(R)_t$ is generated by elements of the form $[(1,-a)]$ where a is a unit and a sum of squares.

Proof By (V.26) and (V.37), $W(R)_t$ is generated by elements of the form $(1,-a)$ where a is a unit represented by a Pfister-space $(1,a_1) \otimes \cdots \otimes (1,a_n)$ where each a_i is a unit and a sum of squares. Elements represented by such a space are again sums of squares, hence the corollary.

(V.39) Corollary W(R) is torsion free if and only if every unit which is a sum of squares is itself a square, with the exception that -1 is not a square.

Proof If every element which is a sum of squares is already a square, then $W(R)_t$ is generated by $(1,-a^2) \sim (1,-1) \sim 0$ so $W(R)_t = 0$. The converse is (V.25).

REFERENCES

[1] Baeza, R. "Eine Bemerkung über Pfisterform," *Archiv. der. Math.* 25 (1974), 254-259.

[2] Baeza, R. "Über die Torsion der Wittgruppe Wq(A) eines semi-lokalen Ringes," *Math. Ann.* 207 (1974), 121-131.

[3] Baeza, R. "Über die Stufe eines semi-lokalen Ringes," *Math. Ann.* 215 (1975), 13-21.

[4] Baeza, R. *Quadratische Formen über semilokalen Ringen*. Habilitationsschrift, Saarbrucken, 1975.

[5] Baeza, R. "Common splitting rings of quaternion algebras over semi-local rings," *Conf. on Quadratic Forms* - 1976, Ed., G. Orzech, Queen's University, Kingston.

[6] Baeza, R. and M. Knebusch. "Annullatoren von Pfisterformen über semi-lokalen Ringen," *Math. Z.* 140 (1975), 41-62.

[7] Bass, H. "K-theory and stable algebra," *Publ. I.H.E.S.* No. 22 (1964), 5-60.

[8] Cassel, D. W. "Rings over Which Projective Modules are Free," Ph.D. Thesis, Syracuse University, 1967.

[9] Chang, C.-N. "Orthogonal groups over semilocal domains," *J. of Algebra* 37 (1975), 137-164.

[10] Coleman, D. B. and Joel Cunningham. "Comparing Witt rings," *J. of Algebra* 28 (1974), 296-303.

[11] Connell, Ian G. "Some ring theoretic Schröder-Berstein theorems," Trans. Amer. Math. Soc. 132 (1968), 335-351.

[12] Eichler, M. Quadratishe Formen und Orthogonale Gruppen. Springer-Verlag, 1952.

[13] Estes, D. and J. Ohm. "Stable range in commutative rings," J. of Algebra 7 (1967), 343-362.

[14] Fujisaki, G. "A note on Witt rings over local rings," J. Fac. Sci. Univ. Tokyo 19 (1972), 403-414.

[15] Gabel, M. "Stably Free Projectives over Commutative Rings," Ph.D. Thesis, Brandeis University, 1972.

[16] Goodearl, K. R. and R. B. Warfield, Jr. "Algebras over zero dimensional rings," preprint.

[17] Hornix, E. "Stiefel-Whitney invariants of quadratic forms over local rings," J. of Algebra 26 (1973), 258-279.

[18] Hsia, J. S. "On the Witt Ring and Some Arithmetical Invariants of Quadratic Forms," J. of Number Theory 5 (1973), 339-355.

[19] James, D. G. "On the structure of orthogonal groups over local rings," Amer. J. Math. 95 (1973), 255-265.

[20] Klingenberg, W. "Orthogonal Gruppen über lokalen Ringen," Amer. J. Math. 83 (1961), 281-320.

[21] Knebusch, M. "Isometrien über semilokalen Ringen," Math. Z. 108 (1969), 255-268.

[22] Knebusch, M. "Runde Formen über semilokalen Ringen," Math. Ann. 193 (1971), 21-34.

[23] Knebusch, M. "Bemerkungen zur Theorie der quadratischen Formen uber semi-lokalen Ringen," Schriften des math. Inst. der Univ. des Saarlandes, Saarbrüken, 1971.

[24] Knebusch, M. "Generalization of a theorem of Artin-Pfister to arbitrary semi-local rings," preprint.

[25] Knebusch, M. "Symmetric bilinear forms over algebraic varieties," Conf. on Quadratic Forms - 1976, Ed. G. Orzech, Queen's University, Kingston, 103-283.

[26] Knebusch, M., A Rosenberg and R. Ware. "Structure of Witt rings and quotients of Abelian group rings," J. Math. 94 (1972), 119-155.

[27] Knebusch, M., A. Rosenberg and R. Ware. "Signatures on semilocal rings," J. of Algebra 26 (1973), 208-250.

[28] McDonald, B. R. Geometric Algebra over Local Rings. Monographs on Pure and Applied Math., Dekker, 1976.

[29] McDonald, B. R. and Hershberger, B. "The Orthogonal Group over a Full Ring," (to appear), J. of Algebra.

[30] Mandelberg, K. I. "On the classification of quadratic forms over semilocal rings," J. of Algebra 33 (1975), 463-471.

[31] Milnor, J. and D. Husemoller. Symmetric Bilinear Forms. Ergebnisse d. Math., Vol. 73, Springer, Berlin-Heidelberg-New York, 1973.

[32] Nagata, M. Local Rings. Vol. 13, Tracts in Pure and Applied Math., Wiley-Interscience, 1962.

[33] Pierce, R. S. "Modules over commutative regular rings," Mem. Amer. Math. Soc. #70, 1967.

[34] Reiter, H. "Witt's theorem for noncommutative semilocal rings," J. of Algebra 35 (1975), 483-499.

[35] Rosenberg, A. and R. Ware. "Equivalent topological properties of the space of signatures of a semilocal ring," preprint.

[36] Roy, Amit. "Cancellation of quadratic forms over commutative rings," J. of Algebra 10 (1968), 286-298.

[37] Simis, Aron. "When are projective modules free?" Queen's Papers in Pure and Applied Math., Vol. 21, Queen's University, 1969.