COMMUNICATIONS IN ALGEBRA

Volume 16, Number 6, 1988

CONTENTS

MARCEL DEKKER, INC. New York and Basel

Contributions to this journal are published free of charge

COMMUNICATIONS IN ALGEBRA, 16(6), 1275-1313 (1988)

WITT RINGS OF HIGHER DEGREE FORMS

D.K. Harrison *)

Dept. of Mathematics
University of Oregon
Eugene, Oregon, USA

Bodo Pareigis

Mathematisches Institut
Universität München
Munich, Germany

In this paper we study the theory of higher degree forms. It can be expressed in two ways. One way is to consider vector spaces V together with an r-linear symmetric map from the r-fold product of V to the base field R. We call these spaces simply symmetric spaces. Witt rings of such symmetric spaces will be introduced in section 1. The equivalence relation used for this construction coinsides with the equivalence relation for the usual Witt ring in case R is the field of real numbers and r = 2. The second way is to study homogeneous polynomials of degree r in n variables. Some of our results which we obtain by studying symmetric spaces, can be translated to such homogeneous polynomials and are presented below for readers who are more interested in that point of view. Some other results have translations so complicated to express that we prefered not to give the explicit formulas.

*) Supported by a Humboldt-Award of the Alexander von Humboldt-Stiftung

In the first section we construct a Witt ring $W_r(R,H)$ of symmetric spaces by imposing an equivalence relation on all nondegenerate symmetric spaces defined by H-spaces. They are a certain analog of hyperbolic spaces, but here H stands for a rather arbitrary finite abelian group. The subring of $W_r(R,H)$ consisting of diagonalizable spaces will be explicitly computed. Since these Witt rings depend on the degree r of the mulitlinear forms, we then reduce the degree by a homomorphism from the Witt ring of r-forms to the Witt ring of s-forms where s divides r. An especially nice class of symmetric spaces is constructed from separable field extensions of R by the trace map. These forms will be called separable forms and can be characterized by properties of their centers. A subclass of these is given by Galois extensions of a special type. They are studied in the last section.

We now describe some of our results in terms of homogeneous polynomials, leaving to the reader to verify the appropriate translation. For simplicity we restrict our attention to the field of real numbers. For $r > 1$, we are interested in

$$f \in \mathbb{R}[X_1,\ldots,X_n]$$

homogeneous of degree r (a form of degree r in n variables). We write

$$f = f(X_1,\ldots,X_n),\ \deg(f) = r.$$

If $f = f(X_1,\ldots,X_n)$, $g = g(X_1,\ldots,X_m)$ and $\deg(f) = \deg(g) = r$, we write $f \cong g$ if $n = m$ and

$$f(\sum \alpha_{1j}X_j,\ldots,\sum \alpha_{nj}X_j) = g(X_1,\ldots,X_n)$$

for some $[\alpha_{ij}] \in GL_n(\mathbb{R})$. We write

$$f \oplus g = f(X_1,\ldots,X_n) + g(X_{n+1},\ldots,X_{n+m}).$$

We write

$$f_i = \partial f/\partial X_i, f_{ij} = \partial^2 f/(\partial X_i \partial X_j), \text{ etc.}$$

We call $(\beta_1,\ldots,\beta_n) \in \mathbb{R}^n$ a $(t+1)$-fold zero of f if

$$f_{i_1\ldots i_t}(\beta_1,\ldots,\beta_n) = 0$$

for all $i_1,\ldots,i_t \in \{1,\ldots,n\}$, i.e. the n-tuple $(\beta_1,\ldots,\beta_n)$ is a common zero of all higher partial derivatives of f of order t. We call f nondegenerate if its only r-fold zero is $(0,\ldots,0)$. This happens if and only if none of the variables can be removed from f; i.e., if there is no form $h = h(X_1,\ldots,X_n)$ with $0 < n$,

$$f \cong h, h(X_1,\ldots,X_{n-1},0) = h(X_1,\ldots,X_{n-1},X_n).$$

We can always write

$$f \cong g \oplus h$$

with g nondegenerate and h trivial (i.e., with

$$h = h(X_1,\ldots,X_q) = 0, n \leq q).$$

We call f an H-form (the reader may take H-form for "hyperbolic" or for H a finite subgroup of $U(\mathbb{R})/U(\mathbb{R})^r$ (see 1)) if

$$-f \cong f.$$

If f is an H-form, $0 < n, \gamma \in \mathbb{R}$, then one can always solve

$$\gamma = f(X_1,\ldots,X_n).$$

We write

$$\mathrm{Cent}(f) = \{M \in \mathrm{Mat}_n(R) \mid M^t \cdot [f_{ij}] = [f_{ij}] \cdot M\}.$$

If f is nondegenerate and $r \neq 2$, this is a commutative $\mathbb{R}$-algebra. We write

$$\mathrm{Aut}(f) = \{[\alpha_{ij}] \in GL_n(\mathbb{R}) \mid f(\sum \alpha_{1j}X_j,\ldots,\sum \alpha_{nj}X_j) = f\}.$$

This is a group.

We write $f \sim g$ if there exist H-forms h, t (of degree r) with

$$f \oplus h \cong g \oplus t.$$

In our first section we put a natural commutative ring structure on the set

$$W_r(\mathbb{R},H)$$

of all $\sim$-classes of forms of degree r (one gets the same thing if one takes all $\sim$-classes of all nondegenerate forms). We are interested in the ring structure of $W_r(\mathbb{R},H)$. In our second section we define a natural ring homomorphism

$$\Omega : W_r(\mathbb{R},H) \longrightarrow W_s(\mathbb{R},H)$$

for s a divisor of r with $s > 1$. We have Sylvester's theorem

$$W_2(\mathbb{R},H) \cong \mathbb{Z}$$

and for r odd,

$$W_r(\mathbb{R},H) = 0.$$

In our third section we restrict attention to $r \neq 2$ and f being separable, by which we mean:

i) f is nondegenerate,
ii) $M \in \mathrm{Cent}(f)$, $M^2 = 0$ implies $M = 0$, and
iii) $n \leq \dim_{\mathbb{R}} \mathrm{Cent}(f)$.

We write

$$k_r = \sum\nolimits_{0 \leq j \leq r/2} (-1)^j \binom{r}{2j} X_1^{2j} X_2^{r-2j},$$

and

$$s_r = X_1^r, \quad t_r = -X_1^r.$$

Then any direct sum of copies of h_r, s_r, t_r is separable, and the converse holds (up to isomorphism). In our last section we show f is isomorphic to a direct sum of copies of h_r if and only if

$$f = f_{(1)} \oplus \ldots \oplus f_{(q)}$$

where $f_{(1)}, \ldots, f_{(q)}$ are indecomposable (for $r \neq 2$ every form is isomorphic to a direct sum of indecomposable forms in a unique way) and for $i = 1, \ldots, q$:

1) $f_{(i)}$ has no 2-fold zero besides $(0,\ldots,0)$,

2) $rn_i \leq |\mathrm{Aut}(f_{(i)})|$,

3) $n_i \leq \dim_{\mathbb{R}} \mathrm{Cent}(f_{(i)})$,

where $f_{(i)} = f_{(i)}(X_1,\ldots,X_{n_i})$. This remains true if the inequalities in 2) and 3) are replaced by equalities. Also 2) may be replaced by "$1 < n_i$".

We have chosen to give this introduction for the reals. We could equally well have chosen a Galois field $GF(p^m)$ where $r < p$. The paper itself is for a field whose characteristic does not divide $r!$.

1. The Witt ring $W_r(R,H)$ of higher degree forms

Let R be a field. Let $r > 1$ be a natural number. We always assume that the characteristic of R does not divide $r!$. A multilinear form $\Theta : V \times\ldots\times V \longrightarrow R$ of degree r ($\Theta : V^r \longrightarrow R$) on a finite dimensional vector space V is *symmetric*, if for every permutation $\sigma \in S_r$ and all $v_1,\ldots,v_r \in V$

$$\Theta(v_1,\ldots,v_r) = \Theta(v_{\sigma(1)},\ldots,v_{\sigma(r)}).$$

We call (V,Θ) a *symmetric space of degree* r. Let (V,Θ) and (W,Ψ) be two symmetric spaces of degree r and $f : V \longrightarrow W$ be a linear map. f is a homomorphism of symmetric spaces if

$$\Theta(v_1,\ldots,v_r) = \Psi(f(v_1),\ldots,f(v_r))$$

for all $v_i \in V$. Let $P_r'(R)$ denote the set of isomorphism classes of symmetric spaces. A symmetric space (V,Θ) with $\Theta = 0$ is called *trivial*.

A symmetric space (V,Θ) is *nondegenerate* if

$$\Theta(v,v_2,\ldots,v_n) = 0 \text{ for all } v_2,\ldots,v_r \in V$$

implies $v = 0$. Let $P_r(R)$ denote the set of isomorphism classes of nondegenerate symmetric spaces of degree r over R.

Let (V,Θ) and (W,Ψ) be in $P'_r(R)$. Then

$$V \perp W := (V \otimes W, \Theta \otimes \Psi)$$

(called *orthogonal sum*) and $V \otimes W := (V \otimes W, \Theta \otimes \Psi)$ are in $P'_r(R)$ with

$$(\Theta \otimes \Psi)(v_1+w_1,\ldots,v_r+w_r) = \Theta(v_1,\ldots,v_r) + \Psi(w_1,\ldots,w_r)$$

$$(\Theta \otimes \Psi)(v_1\otimes w_1,\ldots,v_r\otimes w_r) = \Theta(v_1,\ldots,v_r) \cdot \Psi(w_1,\ldots,w_r).$$

It is easily checked that $\Theta \otimes \Psi$ exists. The operations $\perp$ and $\otimes$ define a structure of a semiring on $P'_r(R)$ (see [1] Prop. 2.1).

The operations $\perp$ and $\otimes$ can be restricted to $P_r(R)$ ([1] p. 131) so that $P_r(R)$ becomes a sub semiring of $P'_r(R)$. For $P_r(R)$ we have the following two theorems.

Theorem (Witt cancellation theroem): If $r = 2$ and $t_1 \in P_2(R)$ for $i = 1,2,3$, then $t_1 \perp t_2 = t_1 \perp t_3$ implies $t_2 = t_3$. [2]

Theorem: If $r > 2$ and $t_i \in P_r(R)$ for $i = 1,2,3$, then $t_1 \perp t_2 = t_1 \perp t_3$ implies $t_2 = t_3$. [1, Prop. 2.4]

Let (R,Θ) be in $P_r(R)$. Then

$$\Theta(\alpha_1,\ldots,\alpha_r) = \alpha_1\ldots\alpha_r\Theta(1,\ldots,1) = \alpha \cdot \alpha_1\ldots\alpha_r$$

for some $\alpha \in U(R)$, the group of units of R. If $\beta : (R,\Theta) \longrightarrow (R,\Psi)$ is an isomorphism (i.e. $\beta \in U(R)$) then $\alpha = \Theta(1,\ldots,1) = \Psi(\beta,\ldots,\beta) = \alpha'\beta^r$. So the isomorphism classes of one-dimensional spaces in $P_r(R)$ can be identified with the elements $\bar{\alpha} \in G_r(R) = U(R)/U(R)^r$. The image of $\bar{\alpha}$ under this map will be denoted by $<\alpha>$.

Thus the following multiplication

$$\alpha\cdot(V,\Theta) := (V,\alpha\Theta)$$

for $\alpha \in U(R)$, $[(V,\Theta)] \in P'_r(R)$ coincides with the operation of $G_r(R)$ by tensor products on $P'_r(R)$ resp. $P_r(R)$

$$\alpha\cdot[(V,\Theta)] = [<\alpha>\otimes(V,\Theta)] = [(V,\alpha\Theta)] = [\alpha\cdot(V,\Theta)].$$

The image of $G_r(R)$ in $P_r(R)$ generates an additive sub monoid

$$P_r^D(R) := \{\langle\alpha_1\rangle \perp \ldots \perp \langle\alpha_n\rangle \mid \bar{\alpha}_i \in G_r(R)\}.$$

The spaces $\langle\alpha_1\rangle \perp \ldots \perp \langle\alpha_n\rangle$ in $P_r^D(R)$ are called *diagonalizable*. Since $\langle\alpha\rangle \otimes \langle\beta\rangle = \langle\alpha\beta\rangle$ we get that $P_r^D(R)$ is a sub semiring of $P_r(R)$. If we identify $G_r(R)$ with its image in $P_r(R)$ then we have the following situation

$$G_r(R) \subseteq P_r^D(R) \subseteq P_r(R) \subseteq P_r'(R)$$

where G is a multiplicative group and the P's are semirings.

Since G_r is an abelian torsion group, it is the union of finite subgroups. For a fixed $r > 1$ we consider *objects* (R,H_r) where R is a field and $H = H_r$ is a finite subgroup of $G_r(R)$. Let (S,K_r) be another object. A *morphism* $\sigma : (R,H_r) \longrightarrow (S,K_r)$ is a ring homomorphism $\sigma : R \longrightarrow S$ such that the induced map $\bar{\sigma} = G_r(\sigma)$ maps the group H_r surjectively onto K_r, i.e.

$$\{\sigma(\alpha)U(S)^r \mid \alpha U(R) \in H_r\} = K_r.$$

Given an object (R,H_r). A nondegenerate symmetric space (V,Θ) is called an H-*space* if $\langle\alpha\rangle \otimes (V,\Theta) \cong (V,\Theta)$ for all $\bar{\alpha} \in H_r$. The class t of (V,Θ) in $P_r(R)$ is then also called an H-*class*, which means that the H_r-orbit of t consists of a single element t. An element y in $P_r(R)$ is called H-*reduced* if $y = t \perp z$ with an H-class t implies $t = 0$.

Theorem 1.1: For each $u \in P_r(R)$ there is an H-reduced class u_H and an H-class $t_H(u)$ in $P_r(R)$ such that $u = u_H \perp t_H(u)$.

Proof: This follows from an induction on the dimension of u. Let $u = z \perp t$ with an H-class t. If $t \neq 0$ then $z = z_H \perp t_H(z)$ and $u = z_H \perp t_H(z) \perp t$, where z_H is H-

reduced and $t_H(z) \perp t$ is an H-class. If $t = 0$ is the only possibility then $u = z$ is H-reduced by definition.

Theorem 1.2: Let $r > 2$. The decomposition $u = u_H \perp t_H(u)$ into an H-reduced class u_H and an H-class $t_H(u)$ for $u \in P_r(R)$ is unique.

Proof: Let y,z be H-reduced and s,t be H-classes with $y \perp s = z \perp t$. If $s = 0$ then $y = z \perp t$ and y H-reduced implies $t = 0$. Now let $s \neq 0$. Write $s = s_1 \perp \ldots \perp s_m$ with $s_1,\ldots,s_m$ indecomposable [1, Prop. 2.3]. For $\bar{\alpha} \in H, <\alpha> \circledast s = s$, so

$$<\alpha> \circledast s_1 \in \{s_1,\ldots,s_m\}.$$

We call $<\alpha> \circledast s_1$ an H-*conjugate* of s_1 and write $H \cdot s_1$ for the sum of the distinct H-conjugates of s_1. Then $H \cdot s_1$ is an H-class. Write

$$s = H \cdot s_1 \perp w.$$

One checks that w is an H-class. Write

$$z = z_1 \perp \ldots \perp z_n, \quad t = t_1 \perp \ldots \perp t_p$$

with $z_1,\ldots,z_n,t_1,\ldots,t_p$ indecomposable. Each H-conjugate of s_1 is in $\{z_1,\ldots,z_n,t_1,\ldots,t_p\}$ and they are not all in $\{z_1,\ldots,z_n\}$ (for otherwise $z = H \cdot s_1 \perp u$ which contradicts that z is H-reduced). Hence at least one H-congugate of s_1 is in $\{t_1,\ldots,t_p\}$. Thus they all are in $\{t_1,\ldots,t_p\}$ (using t is an H-class and [1, Prop. 2.3]). Hence

$$t = H \cdot s_1 \perp v.$$

Multiplying by $\bar{\alpha} \in H$, one checks that v is an H-class. We have $y \perp w = z \perp v$. Also, $\dim(w) < \dim(s)$. By induction theorem 1.2 is proved.

We introduce an equivalence relation on $P_r(R)$. Let y_1,y_2 be in $P_r(R)$. $y_1 \sim y_2$ will mean there are H-classes t_1,t_2

such that $y_1 \perp t_1 = y_2 \perp t_2$. Let $[y]$ denote the equivalence class of y. We write

$$W_r(R,H) = \{[y] \mid y \in P_r(R)\}.$$

The canonical map from $P_r(R)$ to $W_r(R,H)$ will be denoted by

$$r_H : P_r(R) \longrightarrow W_r(R,H).$$

Observe that theorems 1.1 and 1.2 imply

Corollary 1.3: For every $r > 1$ each equivalence class $[y]$ contains at least one H-reduced representative $[y] = [y_H]$.

Corollary 1.4: If $r > 2$ then the H-reduced representative in each equivalence class is uniquely determined, so $W_r(R,H)$ can be viewed as a subset of $P_r(R)$.

Lemma 1.5: The equivalence relation $\sim$ is compatible with $\perp$ and $\otimes$, hence there is an induced addition and multiplication on $W_r(R,H)$ given by

$$[x] + [y] = [x \perp y], \quad [x] \cdot [y] = [x \otimes y].$$

Proof: Let $x \perp t = x' \perp t'$ with H-classes t and t'. Then $x \perp y \perp t = x' \perp y \perp t'$ and $x \otimes y \perp t \otimes y = (x \perp t) \otimes y = (x' \perp t') \otimes y = x' \otimes y \perp t' \otimes y$ where $t \otimes y$ and $t' \otimes y$ are again H-classes.

Theorem 1.6: $W_r(R,H)$ is a commutative ring and

$$r_H : P_r(R) \longrightarrow W_r(R,H)$$

is a surjective map which preserves addition and multiplication.

Proof: Since $W_r(R,H)$ inherits the structure of $P_r(R)$ we only have to prove the existence of additive inverses. So let $[x]$ be given. Let u be the orthogonal sum of the non-isomorphic $\langle\alpha\rangle \otimes x$, $\overline{\alpha} \in H$, which are not iso-

morphic to $x = \langle 1\rangle \otimes x$. Then $x \perp u$ is an H-class, so $[x] + [u] = 0$.

Theorem 1.7: Let $W(R)$ be the Witt ring of quadratic forms. Then the canonical ring homomorphism $W(R) \longrightarrow W_2(R,H)$ is surjective and has the annihilator

$$\mathrm{Ann}_{W(R)}\{\langle 1\rangle - \langle h\rangle \mid h \in H\}$$

as kernel.

Proof: The elements of $W(R)$ are equivalence classes of nondegenerate classes modulo hyperbolic classes, i.e. t_1 is equivalent to t_2 if and only if there are hyperbolic classes z_1 and z_2 such that $t_1 \perp z_1 = t_2 \perp z_2$. It is easy to see that hyperbolic classes are always H-classes. This defines the canonical epimorphism. Now let $[t]$ be in the annhilator. Then $\langle 1\rangle[t] = \langle h\rangle[t]$ for all h in H, where the equality is taken in $W(R)$. But since $\langle h\rangle[t]$ is anisotropic whenever t is anisotropic this shows that t is an H-class, hence zero under the canonical map. Conversely let $[t]$ be in the kernel of the map. Then $t \perp s = r$, where r,s are H-spaces and t is anisotropic. So $t \perp s = r = \langle h\rangle r = \langle h\rangle t \perp \langle h\rangle s = \langle h\rangle t \perp s$ and by the cancellation theorem $t = \langle h\rangle t$. Thus t is in the annihilator.

Lemma 1.8: Let $\Gamma : P_r(R) \longrightarrow P_s(S)$ be a map preserving (orthogonal) sums. Let $H \subseteq G_r(R)$ and $K \subseteq G_s(S)$ be finite subgroups, such that $\Gamma(t)$ is a K-class for every H-class t. Then there exists an additive map

$$\tilde{\Gamma} : W_r(R,H) \longrightarrow W_s(S,K)$$

such that

$$\begin{array}{ccc} P_r(R) & \xrightarrow{\Gamma} & P_s(S) \\ \downarrow{\scriptstyle r_H} & & \downarrow{\scriptstyle r_K} \\ W_r(R,H) & \xrightarrow{\tilde{\Gamma}} & W_s(S,K) \end{array}$$

commutes.

Proof: Let $x \sim x'$ in $P_r(R)$. Then there are H-classes t,t' such that $x \perp t = x' \perp t'$; hence $\Gamma(x) \perp \Gamma(t) = \Gamma(x') \perp \Gamma(t')$ with K-classes $\Gamma(t), \Gamma(t')$ and $\Gamma(x) \sim \Gamma(x')$ in $P_s(S)$.

Theorem 1.9: For J a finite subgroup of $G_r(R)$ with $H \subseteq J$, the map

$$r_H : W_r(R,J) \longrightarrow W_r(R,H)$$

is a surjective ring homomorphism.

Proof: By definition a J-class is also an H-class. Thus the following diagram commutes

$$\begin{array}{ccc} P_r(R) & \xrightarrow{\text{id}} & P_r(R) \\ \downarrow{\scriptstyle r_J} & & \downarrow{\scriptstyle r_H} \\ W_r(R,J) & \longrightarrow & W_r(R,H). \end{array}$$

Using this it is easy to see the remaining part of the theorem.

Now let $\sigma : (R,H) \longrightarrow (S,K)$ be a morphism of objects.

Theorem 1.10: The map

$$W_r(\sigma) : W_r(R,H) \longrightarrow W_r(S,K),\ [(V,\Theta)] \longrightarrow [S \otimes_R (V,\Theta)]$$

is a ring homomorphism. In fact, W_r is a functor to the category of commutative rings.

Proof: σ induces a homomorphism $P_r(\sigma) : P_r(R) \longrightarrow P_r(S)$ [1, p. 128]. Let $t \in P_r(R)$ be an H-class and $\overline{\alpha} \in K$. Then there is a $\overline{\beta} \in H$ such that $\overline{\sigma(\beta)} = \overline{\alpha}$ and $\langle\alpha\rangle \otimes P_r(\sigma)(t) = P_r(\sigma)(\langle\beta\rangle) \otimes P_r(\sigma)(t) = P_r(\sigma)(\langle\beta\rangle \otimes t) = P_r(\sigma)(t)$. Consequently $y \sim y'$ in $P_r(R)$ with respect to H implies $\sigma(y) \sim \sigma(y')$ in $P_r(S)$ with respect to K. So the diagram

$$\begin{array}{ccc} P_r(R) & \xrightarrow{P_r(\sigma)} & P_r(S) \\ \downarrow & & \downarrow \\ W_r(R,H) & \xrightarrow{W_r(\sigma)} & W_r(S,K) \end{array}$$

commutes. Then it is easy to see that $W_r(\sigma)$ is a ring homomorphism.

Let $\sigma : R \longrightarrow S$ be a finite extension of fields. Let

$$0 \neq f \in \mathrm{Hom}_R(S,R).$$

We assume H and K such that $\sigma : (R,H) \longrightarrow (S,K)$ is a morphism of objects. Using lemma 2.7 of [1], we define

$$f_\sigma : W_r(S,K) \longrightarrow W_r(R,H), \quad [(V,\Theta)] \longmapsto r_H(V, f\cdot\Theta).$$

Theorem 1.11: For $a \in W_r(S,K)$, $b \in W_r(R,H)$

$$f_\sigma(W_r(\sigma)(b)\cdot a) = b\cdot f_\sigma(a).$$

Also, f_σ preserves addition.

Proof: Let $a = [(W,\Psi)]$ and $b = [(V,\Theta)]$. Then the R-linearity of f implies

$$f(\sigma\Theta(v_1,\ldots,v_r)\cdot\Psi(w_1,\ldots,w_r)) = \Theta(v_1,\ldots,v_r)\cdot f(\Psi(w_1,\ldots,w_r))$$

hence $f_\sigma(P_r(\sigma)(b)\cdot a) = b\cdot f_\sigma(u)$. So f_σ satisfies the given equation on the level of P_r. Now we show that $f_\sigma(t)$ is an H-class for every K-class t in $P_r(S)$. Let $\overline{\alpha} \in H$ and $t = (W,\Psi)$. Then $\langle\alpha\rangle \circledast (W, f\cdot\Theta) = (W, \alpha f\Psi) = (W, f\sigma(\alpha)\Psi) = f_\sigma(\langle\sigma(\alpha)\rangle \circledast (W,\Psi)) = f_\sigma(W,\Psi) = (W, f\cdot\Psi)$. One easily checks that f_σ is compatible with the equivalence relation, so it defines a map from $W_r(S,K)$ to $W_r(R,H)$ satisfying the given relations.

For $\beta \in U(R)$, $y \in P_r(R)$ we say $\beta = y$ *has a solution*, if $\langle\beta\rangle \leq y$, i.e. $\langle\beta\rangle$ is a symmetric subspace of y. $\beta = y$ has a solution for $y = (V,\Theta)$ if and only if there is a non-zero $v \in V$ such that $\beta = \Theta(v,\ldots,v)$. The subspace isomorphic to $\langle\beta\rangle$ is the one-dimensional space generated by v.

Theorem 1.12: Let $\overline{\gamma} \in G_r(R)$, $y \in P_r(R)$. Suppose y is an H-class and $\gamma = y$ has a solution. Then $\beta = y$ has a solution for all $\overline{\beta} \in \overline{\gamma}H$.

Proof: $\langle\gamma\rangle \leq y$ and $\langle\beta\gamma^{-1}\rangle \otimes y = y$ imply $\langle\beta\rangle = \langle\beta\gamma^{-1}\rangle \otimes \langle\gamma\rangle \leq y$, since $\overline{\beta\gamma}^{-1} \in H$.

We define now $W_r^D(R,H)$ as the image of $P_r^D(R)$ under the map $-_H : P_r(R) \longrightarrow W_r(R,H)$. Then $-_H^D : P_H^D(R) \longrightarrow W_r^D(R,H)$ is a surjective homomorphism of semirings and $W_r^D(R,H)$ is a subring of $W_r(R,H)$. This is a consequence of the fact that the additive inverse of a class $\langle\beta\rangle$ in $W_r(R,H)$ is diagonalizable.

Theorem 1.13: Let $r > 2$. Then $W_r^D(R,H) \cong \mathbb{Z}[G]/(h_1+\ldots+h_n)$.

Proof: Without loss we take H nontrivial. We first define a map from $W_r^D(R,H)$ to $\mathbb{Z}[G]/(h_1+\ldots+h_n)$. Let $\langle\alpha\rangle \in W_r^D(R,H)$. We map it to $\overline{\alpha} \in \mathbb{Z}[G]/(h_1+\ldots+h_n)$. Since $\langle\alpha\rangle$ comes from an element in $G \subseteq P_r^D(R)$, we only have to check for the map to be well-defined that this definition is compatible with the equivalence relation induced by H. By corollary 1.4 $\langle\alpha\rangle$ is the only H-reduced class in its equivalence class. The elements of this form generate $W_r^D(R,H)$ as an abelian group. The relations are defined by the H-classes, since the neutral element in $W_r^D(R,H)$ has only 0 as an H-reduced representative, so it consists of H-classes only. But by [1, Prop. 2.3] and an easy induction argument, the H-classes are orthogonal sums of classes of the form $H\cdot\langle b\rangle$, which are mapped to multiples of $\sum h_i\overline{b}$. Conversely define a map from $\mathbb{Z}[G]/(h_1+\ldots+h_n)$ to $W_r^D(R,H)$ by sending the elements $\overline{\alpha} \in G$ to the equivalence class of $\langle\alpha\rangle$. Then $h_1+\ldots+h_n$ is sent to an H-class with equivalence class 0, hence this map is a well-defined ring homomorphism. Obviously, the two maps defined above are inverses of each other.

Corollary 1.14: Let p be prime and let $H \subseteq G$ be a cyclic subgroup of order p. Then $W_p^D(R,H) \cong \mathbb{Z}[\xi_p][G/H]$.

Proof: Let H be generated by σ. Since $G = U(R)/U(R)^p$, G is a vectorspace over $\mathbb{Z}/p\mathbb{Z}$ and H splits off as a direct summand: $G = H \oplus G/H$. Then the map

$$\mathbb{Z}[G]/(h_1+\ldots+h_p) \longrightarrow \mathbb{Z}[\xi_p][G/H]$$

is defined by $\sigma \longmapsto \xi_p$ and $v \longmapsto v$ for $v \in G/H$, and is an isomorphism.

2. The ring homomorphism $\Omega : W_r(R,H) \longrightarrow W_s(R,H)$

In this paragraph we first study the radicals of symmetric spaces and their relationship to non-degeneracy. Then we construct maps which reduce the degree of symmetric spaces and investigate their behavior with respect to sums and products.

Let (V,Θ) be a symmetric space of degree r over R. Let $s < r$. Then Θ induces a homomorphism $\Theta_s : S^s(V) \longrightarrow S^{r-s}(V)^*$ of R-modules by

$$\Theta_s(v_1 \otimes \ldots \otimes v_s)(v_{s+1} \otimes \ldots \otimes v_r) = \Theta(v_1,\ldots,v_r).$$

We define the *s-radical* s-rad(V,Θ) of (V,Θ) to be the kernel of Θ_s. By reasons of dimension the s-radical of V will be non-zero if $2s > r$.

Using the concept of a derivative of the multilinear form in direction $v \in V$ $(\partial/\partial v(\Theta)(v_2,\ldots,v_r) = \Theta(v,v_2,\ldots,v_r))$ of [1] the (1-)radical of (V,Θ) is the set of $v \in V$ for which the derivatives vanish. We write rad(V,Θ) for 1-rad(V,Θ). Similarly the s-radical of (V,Θ) is the subspace of $S^s(V)$ for whose elements the higher derivatives vanish.

Lemma 2.1: Let $s + t = r$. Then s-rad$(V,\Theta) = 0$ iff there is an element $\sum a_{i1} \otimes \ldots \otimes a_{it} \otimes a_{it+1} \otimes \ldots \otimes a_{ir} \in S^t(V) \otimes S^s(V)$ such that for all $v_{t+1},\ldots,v_r$ we have

$$(*)\quad \sum (a_{i1},\dots,a_{it},v_{t+1},\dots,v_r)\, a_{it+1}\otimes\dots\otimes a_{ir} = v_{t+1}\otimes\dots\otimes v_r.$$

Proof: Let $\sum v_{it+1}\otimes\dots\otimes v_{ir}$ be an element of s-rad(V,θ)

By applying (*) to it we see that this element is zero, hence s-rad$(V,\theta) = 0$. To prove the converse observe that θ_s is injective by the definition of the s-radical. Now let A and B be arbitrary finite R-modules. Then the following diagram commutes

$$\begin{array}{ccc} \mathrm{Hom}_R(A,B^*) & \longrightarrow & \mathrm{Hom}_R(B,A^*) \\ \searrow\!\!\nearrow & & \searrow\!\!\nearrow \\ & \mathrm{Hom}_R(A\otimes B,R). & \end{array}$$

Hence $\theta_t = \theta_s^* : S^t(V) \longrightarrow (S^s(V))^*$ is surjective. Let $e_1,\dots,e_n$ be a basis of V. Then $e_{i_{t+1}}\otimes\dots\otimes e_{i_r}$ with $1 < i_{t+1} <\dots< i_r < n$ is a basis of $S^s(V)$. Let $f(i_{t+1},\dots,i_r)$ be a dual basis to this. Then

$$\sum f(i_{t+1},\dots,i_r)(v_{t+1}\otimes\dots\otimes v_r)e_{i_{t+1}}\otimes e_{i_r} = v_{t+1}\otimes\dots\otimes v_r.$$

But the elements of the dual basis f(...) are in the image of θ_t, hence can be represented in the form

$$\sum \theta(a_1,\dots,a_t,-,\dots,-),$$

which gives the required formula.

Lemma 2.2: For a symmetric space (V,θ) the following are equivalent:

a) (V,θ) is nondegenerate.

b) If $(V,\theta) = A_1 \perp A_2$ with A_2 trivial, then $A_2 = 0$.

c) rad$(V,\theta) = 0$.

d) There is an element $\sum a_{i1}\otimes\dots\otimes a_{ir-1} \otimes a_{ir} \in S^{r-1}(V)\otimes V$ with

$$\sum \Theta(a_{i1},\dots,a_{ir-1},v)a_{ir} = v$$

for all $v \in V$.

Proof: c) $\iff$ d) by lemma 2.1 (see [1] Lemma 1.1). Let $v \in V$, $v \neq 0$ such that $\partial/\partial v(\Theta) = 0$, then $Rv \neq 0$ has a trivial multilinear form and any direct complement V' of Rv in V is an orthogonal complement. This shows b) $\Rightarrow$ c). c) $\Rightarrow$ a) holds by definition. If v is an element of a trivial orthogonal summand of (V,Θ) and $v \neq 0$, then (V,Θ) is degenerate, hence a) $\Rightarrow$ b).

If V is a symmetric space then the multilinear form Θ can be restricted to a form $\overline{\Theta}$ on $V/\mathrm{rad}(V)$. It is easily checked that $\mathrm{rad}(V/\mathrm{rad}(V)) = 0$ and that $V \cong \mathrm{rad}(V) \perp V/\mathrm{rad}(V)$ as symmetric spaces. This defines a map $\Delta : P'_r(R) \longrightarrow P_r(R)$, which is a homomorphism of semirings.

Let (V,Θ) be a symmetric space of degree r and let $st = r$, $s > 1$. Then $S^t(V)$ is a symmetric space of degree s with the bilinear form

$$\Theta^*(v_1 \otimes \dots \otimes v_t,\dots,v_{r-1+1} \otimes \dots \otimes v_r) = \Theta(v_1,\dots,v_r).$$

This defines a map $\Phi'_s : P'_r(R) \longrightarrow P'_s(R)$ on the set of isomorphism classes of symmetric spaces. In general this map will not preserve orthogonal sums or tensor products of symmetric spaces. However

Lemma 2.3: If $st = r$, $s > 1$ then $t\text{-rad}(V,\Theta) = \mathrm{rad}(\Phi'_s(V,\Theta))$.

Proof: $\mathrm{rad}(\Phi'_s(V,\Theta)) = \mathrm{Ker}(S^t(V) \xrightarrow{\Theta^*_1} (S^{s-1}(S^t(V)))^*)$. Since $S^{s-1}(S^t(V))$ has a natural surjective map onto $S^{(s-1)t}(V) = S^{r-t}(V)$, the dual of this map is injective, hence $\mathrm{Ker}(\Theta^*_1) = \mathrm{Ker}(\Theta_t) = t\text{-rad}(V,\Theta)$ and the proof is done.

Lemma 2.4: Let $(V,\Theta) = (A_1,\Psi_1) \perp (A_2,\Psi_2)$. Then

$$s\text{-rad}(V) = s\text{-rad}(A_1) \oplus s\text{-rad}(A_2) \oplus \bigoplus_{i=1}^{s-1} S^i(A_1)\otimes S^{s-i}(A_2).$$

Proof: We use the formula

$$(*)\quad S^s(A_1 \oplus A_2) = S^s(A_1) \oplus S^s(A_2) \oplus \bigoplus_{i=1}^{s-1} S^i(A_1)\otimes S^{s-1}(A_2).$$

Since $A_1 \perp A_2$ we get

$$\oplus\, S^i(A_1)\otimes S^{s-i}(A_2) \subseteq s\text{-rad}(V).$$

Furthermore $s\text{-rad}(A_i) \subseteq s\text{-rad}(V)$. If $x \in s\text{-rad}(V)$ then x can be decomposed according to (*). Let x_i be the component in $S^s(A_i)$. Since it must have the s-radical property with respect to elements of $A_i \subseteq V$ it is in $s\text{-rad}(A_i)$.

Corollary 2.5: Let $st = r$, $s > 1$, and $V = A_1 \perp A_2$. Then

$$\text{rad}(\Phi'_s(V)) = \text{rad}(\Phi'_s(A_1)) \oplus \text{rad}(\Phi'_s(A_2)) \oplus \bigoplus_{i=1}^{s-1} S^i(A_1)\otimes S^{s-i}(A_2).$$

Proof: Use $s\text{-rad}(V) = \text{rad}(\Phi'_s(V))$.

Lemma 2.6: Let $st = r$, $s > 1$. Then the following diagram commutes

$$\begin{array}{ccc} G_r(R) & \longrightarrow & P'_r(R) \\ \Big\downarrow \text{can} & & \Big\downarrow \Phi'_s \\ G_s(R) & \longrightarrow & P'_s(R). \end{array}$$

In particular this induces an epimorphism $H_r \longrightarrow H_s$ of the finite subgroups of $G_r(R)$ resp. $G_s(R)$.

Proof: $\Phi'_s(\langle\alpha\rangle) = (S^s(R),\Theta_\alpha{}^*)$ and $\Theta_\alpha{}^*(1\otimes\ldots\otimes 1,\ldots) = \alpha, S^s(R) \cong R$ so $\Phi'_s(\langle\alpha\rangle) = \langle\alpha\rangle$.

Corollary 2.7: Φ'_s is a G-map, i.e. for each $\alpha \in U(R)$ and $x \in P_r(R)$ we have $\alpha\cdot\Phi'_s(x) = \Phi'_s(\alpha\cdot x)$.

Proof: $\langle\alpha\rangle \otimes \Phi'_s(V,\Theta) = (S^s(V),\alpha\cdot\Theta^*) = (S^s(V),(\alpha\cdot\Theta)^*) = \Phi'_s(V,\alpha\cdot\Theta) = \Phi'_s(\langle\alpha\rangle \otimes V,\Theta)$.

Lemma 2.8: Let (V,Θ) (W,Ψ) be symmetric spaces. Let $f : V \longrightarrow W$ be a surjective homomorphism of symmetric spaces. Then $\Delta(f)$, the restriction of f to the nondegenerate parts of V and W is an isomorphism.

Proof: Observe that $\mathrm{Ker}(f) \subseteq \mathrm{rad}(V,\Theta)$ by the definition of the radical and a homomorphism of symmetric spaces. Since $V = \mathrm{Ker}(f) \perp V'$ for some space V', f restricted to V' is an isomorphism, so $\Delta(f)$ is also an isomorphism.

We define a map $\Phi_s : P_r(R) \longrightarrow P_s(S)$ by

$$\Phi_s : P_r(R) \longrightarrow P_r'(R) \xrightarrow{\Phi_s'} P_s'(R) \xrightarrow{\Delta} P_s(R).$$

Lemma 2.9: $\Phi_s : P_r(R) \longrightarrow P_s(R)$ preserves (orthogonal) sums and products with elements of $G_r(R)$.

Proof: Let $x = y \perp z$ in $P_r(R)$. Then by corollary 2.5 $\Delta(\Phi_s'(x)) = \Delta(\Phi_s'(y) \perp \Phi_s'(z))$. Furthermore all three maps used for the definition of Φ preserve multiplication with elements $\alpha \in U(R)$ so does Φ.

Corollary 2.10: Φ_s preserves H-classes.

Proof: Observe that H-classes in $P_r(R)$ are defined with respect to $H = H_r \subseteq G_r(R)$, H-classes in $P_s(R)$ with respect to $H_s \subseteq G_s(R)$, the image of H_r under the canonical epimorphism. Then the previous lemma shows that $H \cdot x \subseteq x$ implies $H \cdot \Phi_s(x) \subset \Phi_s(x)$.

Lemma 2.11: Φ induces an additive homomorphism

$$\Omega : W_r(R,H) \longrightarrow W_s(R,H).$$

Proof: This is an immediate consequence of lemma 1.8.

This map allows us to reduce the structure of $W_r(R,H)$ to that of $W_p(R,H)$ for primes p dividing r. Now we in-

vestigate the behavior of the maps Φ'_s, Φ_s and Ω with respect to (tensor) products. It is easy to see that Φ'_s does not preserve products in general. We have, however, the following

Theorem 2.12: $\Phi_s : P_r(R) \longrightarrow P_s(R)$ is a homomorphism of semirings.

Proof: We have to show that Φ_s is compatible with the multiplication. The canonical map can : $S^s(V \odot W) \longrightarrow S^s(V) \odot S^s(W)$ is surjective and a homomorphism of symmetric spaces:

$$\begin{aligned}(\Theta \otimes \Psi)^*((a_1 \otimes b_1)\odot..\odot(a_s \otimes b_s),...) \\ = (\Theta \otimes \Psi)(a_1 \otimes b_1,...,a_r \otimes b_r) \\ = \Theta(a_1,...,a_r)\cdot\Psi(b_1,...,b_r) \\ = \Theta^*(a_1\odot...\odot a_s,...)\cdot\Psi^*(b_1\odot...\odot b_s,...).\end{aligned}$$

Now we can apply lemma 2.8 to get $\Phi_s(V \otimes W) \cong \Phi_s(V) \otimes \Phi_s(W)$.

Theorem 2.13: $\Omega : W_r(R,H) \longrightarrow W_s(R,H)$ is a ring homomorphism.

Proof: The following diagram is commutative

$$\begin{array}{ccc} P_r(R) & \xrightarrow{\Phi_s} & P_s(R) \\ \downarrow{\scriptstyle r_H} & & \downarrow{\scriptstyle r_H} \\ W_r(R,H) & \xrightarrow{\Omega} & W_s(R,H) \end{array}$$

and the maps r_H and Φ_s are compatible with tensor products by theorem 1.6 and lemma 1.8. Furthermore r_H is surjective. Then one easily sees that Ω must preserve tensor products.

Corollary 2.14: The ring homomorphism Ω induces an epimorphism $\Omega^D : W^D_r(R,H) \longrightarrow W^D_s(R,H)$.

Proof: follows immediately from the fact that $W^D_r(R,H)$ is generated by elements of the form $\langle\alpha\rangle$ and that $\Phi_s(\langle\alpha\rangle) = \langle\alpha\rangle$ (lemma 2.6).

3. The Witt ring $Z_r(R,H)$ of separable forms

In this paragraph we will assume throughout that R is a field and $r > 2$. Following [1, p. 133] we define the *center* of a symmetric space (V,Θ) of degree r to consist of all elements $f \in \mathrm{Hom}_R(V,V)$ such that

$$\Theta(f(v_1),v_2,\ldots,v_r) = \Theta(v_1,f(v_2),\ldots,v_r).$$

The center will be denoted by $\mathrm{Cent}(V,\Theta)$ or simply $\mathrm{Cent}(V)$. By [1, Prop. 4.1] the center of a nondegenerate space is a commutative algebra and $\mathrm{Cent}(V)$ has no nontrivial idempotents if and only if (V,Θ) is indecomposable.

We define a *separable space* to be a symmetric space (V,Θ) of degree r such that

i) (V,Θ) is nondegenerate,
ii) $\mathrm{Cent}(V,\Theta)$ is a separable R-algebra,
iii) $\dim_R(V,\Theta) \leq \dim_R(\mathrm{Cent}(V,\Theta))$.

Lemma 3.1: Let (V_i,Θ_i), $i = 1,2$ be nondegenerate symmetric spaces. Then

$$\mathrm{Cent}(V_1 \perp V_2) \cong \mathrm{Cent}(V_1) \times \mathrm{Cent}(V_2).$$

Proof: Clearly we have $\mathrm{Cent}(V_1) \times \mathrm{Cent}(V_2) \subseteq \mathrm{Cent}(V_1 \perp V_2)$. Conversely let $f \in \mathrm{Cent}(V_1 \perp V_2)$ and $v_1 \in V_1$. Then f decomposes into a matrix of homomorphisms $f_{ij} \in \mathrm{Hom}_R(V_i,V_j)$. For all $v_{2i} \in V_2$ we get

$$\Theta_2(f_{12}(v_1),v_{22},v_{23},\ldots) = \Theta(f_{12}(v_1),v_{22},v_{23},\ldots)$$
$$= \Theta(f(v_1),v_{22},v_{23},\ldots) = \Theta(v_1,f(v_{22}),v_{23},\ldots) = 0.$$

Since (V_2,Θ_2) is nondegenerate, we get $f_{12}(v_1) = 0$, hence $f_{12} = 0$. So $f = f_{11} + f_{22} \in \mathrm{Cent}(V_1) \times \mathrm{Cent}(V_2)$.

Lemma 3.2: Let (V,Θ) be separable. Then $\dim_R(V,\Theta) = \dim_R(\mathrm{Cent}(V,\Theta))$.

Proof: By lemma 3.1 a decomposition of V into indecomposable spaces induces a decompostion of Cent(V) into a product of the centers of the indecomposable components. So it suffices to prove the lemma for V indecomposable. But then Cent(V) is connected and a separable commutative finite-dimensional R-algebra, hence a separable field extension K which acts on $V \neq 0$ by a linear action. This shows that $\dim_R(K) \leq \dim_K \cdot \dim_R(K) = \dim_R(V)$.

Lemma 3.3: The space $\langle\alpha\rangle$ is separable for all $\overline{\alpha} \in G_r(R)$.

Proof: We know that $\langle\alpha\rangle$ is nondegenerate. The center of $\langle\alpha\rangle$ is $\mathrm{Hom}_R(\langle\alpha\rangle,\langle\alpha\rangle) = R$ hence separable with the correct dimension.

Lemma 3.4: (V_i,θ_i), $i = 1,2$ are separable spaces if and only if $V_1 \perp V_2$ is separable.

Proof: The orthogonal sum of separable spaces is separable by lemma 3.1 and the fact that products of separable commutative algebras are separable. Conversely decompose V_1 and V_2 into indecomposable spaces. That defines a decomposition of

$$V = V_1 \perp V_2 = V_{11} \perp \ldots \perp V_{11} \perp V_{21} \perp \ldots \perp V_{2m}$$

with $\mathrm{Cent}(V_{ij})$ separable fields and $\dim_R(\mathrm{Cent}(V_{ij})) = \dim_R(V_{ij})$. Hence V_1 and V_2 must be separable.

Lemma 3.5: Let (V_i,θ_i), $i = 1,2$ be separable. Then $V_1 \otimes V_2$ is separable.

Proof: By [1, Prop. 4.2] we have $\mathrm{Cent}(V_1 \otimes V_2) \cong \mathrm{Cent}(V_1) \otimes \mathrm{Cent}(V_2)$ separable and $\dim_R(\mathrm{Cent}(V_1 \otimes V_2)) = \dim_R(\mathrm{Cent}(V_1))\cdot\dim_R(\mathrm{Cent}(V_2)) = \dim_R(V_1)\cdot\dim_R(V_2) = \dim_R(V_1 \otimes V_2)$.

Combining lemmas 3.3, 3.4, 3.5 we get the following

Theorem 3.6: The isomorphism classes of separable spaces form a sub-semiring $P_r^{sep}(R)$ containing $P_r^D(R)$.

Lemma 3.7: Let H be a finite subgroup of $G_r(R)$ and let u be a separable class in $P_r(R)$. Then the (unique) decomposition $u = u_H \perp t_H(u)$ has separable factors.

Proof: Use theorem 1.2 for the decomposition and lemma 3.4.

Theorem 3.8: Let H be a finite subgroup of $G_r(R)$. Then the set $Z_r(R,H)$ of H-equivalence classes in $W_r(R,H)$ whose unique H-reduced representative is separable, is a subring of $W_r(R,H)$.

Proof: If $H = \{\overline{1}\}$ then $W_r(R,H) = Z_r(R,H) = 0$. Let $H \neq 0$. Then $\langle 1 \rangle$ is in $Z_r(R,H)$ by lemma 3.3. The sum resp. product of two H-reduced separable equivalence classes has an H-reduced separable representative by lemma 3.4 resp. 3.5 and lemma 3.7. Finally the additive inverse of an element u in $Z_r(R,H)$ is the sum in $Z_r(R,H)$ of elements of the form $\langle \alpha \rangle \cdot u$ for certain $\overline{\alpha} \in H$, which are all separable.

Corollary 3.9: $W_r^D(R,H)$ is a subring of $Z_r(R,H)$.

Observe that not all elements of a "separable" equivalence class in $Z_r(R,H)$ are separable spaces. However, the uniquely defined H-reduced representative is separable. So we are in fact developing a theory of equivalence classes modulo the equivalence relation defined by H-spaces. It is clear that the equivalence relation can be restricted to P_r^{sep}: two separable H-classes u^1 and u_2 are equivalent if and only if there are separable H-classes t_1 and t_2 such that $u_1 \perp t_1 = u_2 \perp t_2$. This defines again $Z_r(R,H)$ and yields a commutative diagram

$$\begin{array}{ccccc} P_r^D(R) & \longrightarrow & P_r^{sep}(R) & \longrightarrow & P_r(R) \\ \downarrow{\scriptstyle r_H^D} & & \downarrow{\scriptstyle r_H'} & & \downarrow{\scriptstyle r_H} \\ W_r^D(R,H) & \longrightarrow & Z_r(R,H) & \longrightarrow & W_r(R,H) \end{array}$$

where all horizontal maps are injective and all vertical maps are surjective.

The next theorem will give an important characterization of indecomosable separable H-reduced spaces. First we need two lemmas.

Lemma 3.10: Let K:R be a separable finite field extension and $b \in \mathcal{U}(K)$ and let $tr : K \longrightarrow R$ denote the trace map. Then (K,Ψ) with

$$\Psi(a_1,\ldots,a_r) := b\cdot tr(a_1\cdot\ldots\cdot a_r) = tr(a_1\cdot\ldots a_r\cdot b)$$

is an indecomposable separable space with center K.

Proof: Since the trace of a separable field extension generates $Hom_R(K,R)$ as a K-space and $b \neq 0$, the space (K,Ψ) is nondegenerate. Let $f \in Cent(K,\Psi)$. Let $a \in K$. Then we claim $f(a) = f(1)\cdot a$. To prove this let $x \in K$ and consider

$$tr((f(a)-f(1)\cdot a)\cdot bx) = tr(f(a)bx)-tr(f(1)abx)$$

$$= \Psi(f(a),x,1,\ldots,1) - \Psi(f(1),x,a,\ldots,1)$$

$$= \Psi(a,x,f(1),\ldots,1) - \Psi(f(1),x,a,\ldots,1) = 0,$$

hence $f(a) - f(1)\cdot a = 0$. This shows that f is given by multiplication with an element $f(1) \in K$. Conversely any element $a \in K$ defines by multiplication an element of the center of (K,Ψ). Hence $K \cong Cent(K,\Psi)$ is separable with the correct dimension. We will denote this separable space by $(K,\langle b\rangle_r)$.

Lemma 3.11: Let (V,Θ) be an indecomposable separable space with center K. Then there is an element $b \in K$ and an isomorphism $(V,\Theta) \cong (K,\langle b\rangle_r)$.

Proof: Observe that $K = \mathrm{Cent}(V)$ is a finite separable field extension of R. Let $v \in V$, $v \neq 0$. Then there is a map $g : K \longrightarrow V$, $g(a) = a(v)$. This map is an R-linear isomorphism. g induces the structure of a symmetric separable space on K by

$$\Psi(a_1,\ldots,a_r) := \Theta(g(a_1),\ldots,g(a_r)).$$

Furthermore there exists an $h \in \mathrm{Hom}_R(K,R)$ such that $\Psi(a_1,\ldots,a_r) = h(a_1\cdot\ldots\cdot a_r)$, since

$$\Psi(a_1,\ldots,a_r) = \Theta(a_1(v),\ldots,a_r(v)) = \Theta(a_1\cdot\ldots\cdot a_r(v),v,\ldots v).$$

Since K is a separable field extension there is an element $b \in K$ such that $h = b\cdot\mathrm{tr}$, hence $\Psi(a_1,\ldots,a_r) = b\cdot\mathrm{tr}(a_1\cdot\ldots\cdot a_r)$.

Theorem 3.12: Every indecomposable separable space (V,Θ) is isomorphic to a space of the form $(K,\langle b\rangle_r)$ for some separable field extension K of R and $b \in U(K)$ and every space $(K,\langle b\rangle_r)$ is indecomposable. Two separable spaces $(K,\langle b\rangle_r)$ and $(L,\langle b'\rangle_r)$ with finite separable field extensions K and L are isomorphic if and only if K is isomorphic to L and there is a field isomorphism τ over R and an element $c \in K$, $c \neq 0$ such that

$$b = \tau(b')c^r.$$

Proof: The first part of the theorem was proved in lemma 3.10 and lemma 3.11. Let $(K,\langle b\rangle_r)$ and $(L,\langle b'\rangle_r)$ be isomorphic. Then their centers K and L are isomorphic as rings. Now let $g : K \longrightarrow L$ be an isomorphism between $(K,\langle b\rangle_r)$ and $(L,\langle b'\rangle_r)$. Then we have $\mathrm{tr}(b'g(a_1)\ldots g(a_r)) = \mathrm{tr}(ba_1\ldots a_r) = b\cdot\mathrm{tr}(a_1a_2\cdot 1\cdot\ldots\cdot a_r) = b'\cdot\mathrm{tr}(g(a_1a_2)\cdot g(1)\cdot\ldots\cdot g(a_r)) = \mathrm{tr}(b'g(a_1a_2)g(1)\ldots g(a_r))$. This holds for all choices of $a_i \in K$, so we get $g(a_1a_2)g(1) = g(a_1)g(a_2)$. Define $\sigma(a) = g(a)\cdot g(1)^{-1}$. Then we get $\sigma(a_1)\sigma(a_2) = \sigma(a_1a_2)$ and $\sigma(1) = 1$, hence σ is a field isomorphism over R. Let $\tau = \sigma^{-1}$ and $c = \tau(g(1))$. Then $\mathrm{tr}(b\cdot a_1\ldots a_r) = \mathrm{tr}(b'\cdot g(a_1)\ldots g(a_r)) = \mathrm{tr}(b'\cdot g(1)^r\cdot\sigma(a_1\ldots a_r))$

$= tr(\sigma(\tau(b') \cdot c^r \cdot a_1 \ldots a_r)) = tr(\tau(b') \cdot c^r \cdot a_1 \ldots a_r)$ by a property of the trace, hence $b = \tau(b') \cdot c^r$.

Conversely consider $g : K \longrightarrow K$, $g(a) = \sigma(a \cdot c)$ with $\sigma = \tau^{-1}$. This is an R-linear isomorphism such that $b' \cdot tr(g(a_1) \ldots g(a_r)) = tr(b' \cdot \sigma(a_1) \cdot \sigma(c) \cdot \ldots \cdot \sigma(a_r) \cdot \sigma(c)) = tr(\sigma(\tau(b')c^r \cdot a_1 \cdot \ldots \cdot a_r)) = tr(\tau(b')c^r \cdot a_1 \ldots a_r) = b \cdot tr(a_1 \ldots a_r)$, so g is an isomorphism of symmetric spaces.

Corollary 3.13: Let K be a finite separable field extension of R. Then there is an additive map

$$P_r^D(K) \longrightarrow P_r^{sep}(R), \quad <b> \longmapsto (K, <b>_r).$$

The sum of the images of these maps for all finite separable field extensions K of R is all of $P_r^{sep}(R)$.

Proof: The map is defined by using elements of K. To show it is well-defined observe that b and $b \cdot c^r$ with $c \in U(K)$ define the same class $<b>$. But by previous theorem $(K, <b>_r)$ and $(K, <bc^r>_r)$ are also isomorphic.

Corollary 3.14: Let K be a finite separable field extension of R and let $H \subseteq G_r(R)$ be a finite subgroup. Let H' be the image of H under the map $G_r(R) \longrightarrow G_r(K)$. Then there is an additive map $W_r^D(K,H') \longrightarrow Z_r(R,H)$, induced by $<b> \longmapsto (K, <b>_r)$.

Proof: Apply theorem 1.11 with f = tr and compute the image.

We will now investigate the behavior of $Z_r(R,H)$ under the homomorphism Ω. More generally we can induce several homomorphisms on $Z_r(R,H)$. They all are special cases of the following

Lemma 3.15: Let $\Gamma : P_r(R) \longrightarrow P_s(S)$ be a map preserving (orthogonal) sums. Let $H \subseteq G_r(R)$ and $L \subseteq G_s(S)$ be finite

subgroups, such that $\Gamma(t)$ is a L-class for every H-class t. Assume that $\Gamma(t)$ is separable whenever t is separable. Then there exists an additive map $\tilde{\Gamma} : Z_r(R,H) \longrightarrow Z_s(S,L)$ such that

$$\begin{array}{ccc} P_r^{sep}(R) & \xrightarrow{\Gamma} & P_s^{sep}(S) \\ \downarrow{\scriptstyle r'_H} & & \downarrow{\scriptstyle r'_K} \\ Z_r(R,H) & \xrightarrow{\tilde{\Gamma}} & Z_s(S,L) \end{array}$$

and

$$\begin{array}{ccc} Z_r(R,H) & \xrightarrow{\tilde{\Gamma}} & Z_s(S,L) \\ \downarrow & & \downarrow \\ W_r(R,H) & \xrightarrow{\tilde{\Gamma}} & W_s(S,L) \end{array}$$

commute.

Proof: By lemma 1.8 Γ induces a homorphism $\tilde{\Gamma}$ on $W_r(R,H)$. If $u \in P_r(R)$ is separable, then $\Gamma(u)$ decomposes into an orthogonal sum of separable classes $\Gamma(u)_L \perp t_L(\Gamma(u))$ by lemma 3.7, so $\tilde{\Gamma}$ restricts to $Z_r(R,H) \longrightarrow Z_s(S,L)$ making the given diagrams commutative.

Corollary 3.16: For J a finite subgroup of $G_r(R)$ with $H \subseteq J$, the map

$$r'_H : Z_r(R,J) \longrightarrow Z_r(R,H)$$

is a surjective ring homomorphism.

Proof: We use the commutative diagram

$$\begin{array}{ccc} P_r(R) & \xrightarrow{id} & P_r(R) \\ \downarrow{\scriptstyle r_J} & & \downarrow{\scriptstyle r_H} \\ W_r(R,J) & \longrightarrow & W_r(R,H) \end{array}$$

of the proof ot theorem 1.9 and observe that it can be restricted to separable spaces.

Corollary 3.17: Let $\sigma : (R,H) \longrightarrow (S,K)$ be a morphism of objects. Then the map

$$W_r(\sigma) : W_r(R,H) \longrightarrow W_r(S,K), \quad [(V,\Theta)] \longrightarrow [S \otimes_R (V,\Theta)]$$

of theorem 1.10 restricts to a ring homomorphism

$$Z_r(\sigma) : Z_r(R,H) \longrightarrow Z_r(S,K).$$

In fact, Z_r is a functor to the category of commutative rings.

Proof: To use the arguments in the proof of theorem 1.10 we check that $S \otimes_R (V,\Theta)$ is separable whenever (V,Θ) is separable. By lemma 3.4 this has only to be checked for an indecomposable space (V,Θ). This is an easy consequence of [1, Prop.4.3.].

Theorem 3.18: Let $st = r$, $s > 2$. Let K be a finite separable field extension of R and $b \in K$, $b \neq 0$. Then

$$\Phi_s(K,\langle b\rangle_r) \cong (K,\langle b\rangle_s).$$

Furthermore the ring homomorphism Ω restricts to $Z_r(R,H)$ such that the following diagram commutes

$$\begin{array}{ccc} Z_r(R,H) & \longrightarrow & Z_s(R,H) \\ \downarrow & & \downarrow \\ W_r(R,H) & \xrightarrow{\Omega} & W_s(R,H). \end{array}$$

Proof: Let $\Phi'_s(K,\langle b\rangle_r) = (S^t(K),\rho)$. Define $f : S^t(K) \longrightarrow K$ by

$$f(a_1 \otimes \ldots \otimes a_t) = a_1 \cdot \ldots \cdot a_t.$$

Then

$$\rho(a_1 \otimes \ldots \otimes a_t, \ldots) = \mathrm{tr}(b \cdot a_1 \ldots a_r)$$

$$= b \cdot \mathrm{tr}(f(a_1 \otimes \ldots \otimes a_t) \cdot \ldots \cdot f(a_{r-t+1} \otimes \ldots \otimes a_r)),$$

so f is a surjective homomorphism of symmetric spaces. By lemma 2.8 we get $\Delta\ (S^t(K),\rho) \cong (K,\langle b\rangle_s)$. This shows that Φ_s preserves indecomposable, hence arbitrary separable spaces and can be defined by the formula in the theorem.

Thus Φ_s can be restricted to $P_r^{sep}(R)$ and induces by lemma 3.13 a homomorphism on $Z_r(R,H)$.

Corollary 3.19: $\Omega : Z_r(R,H) \longrightarrow Z_s(R,H)$ is surjective.

Proof: The isomorphism classes of the form $(K,\langle b\rangle_s)$ with a finite separable field extension K of R form an additive generating set of $Z_s(R,H)$ and are all in the image of $Z_r(R,H)$.

We briefly discuss the connection with the Witt ring $W_2(R,H)$ of quadratic spaces. By the diagonalization theorem one knows that $W_2^D(R,H) = W_2(R,H)$. We have already seen for even numbers r that $\Omega : W_r^D(R,H) \longrightarrow W_2^D(R,H)$ is surjective (corollary 2.14). Hence Ω maps $Z_r(R,H)$ surjectively onto $W_2(R,H)$. So it makes sense to define $Z_2(R,H) := W_2(R,H)$ and we get $\Omega(Z_r(R,H)) = Z_2(R,H)$ for even numbers r.

Finally we want to calculate a specific example.

Theorem 3.20: For all even $r > 1$ we have $Z_r(\mathbb{R},C_2) \cong \mathbb{Z}$.

Proof: Since $G_r(\mathbb{R}) = C_2$, the only 1-dimensional indecomposable separable spaces are $\langle 1\rangle$ and $\langle -1\rangle$. Furthermore $(\mathbb{C},\langle 1\rangle_r)$ is the only 2-dimensional indecomposable separable space. In fact the center of such a space must be $\mathbb{C}$. But then it is an H-space, since $H \subseteq G_r(\mathbb{C}) = \{\overline{1}\}$. So the only H-reduced separable spaces are the 1-dimensional spaces given above. They are additive inverses of each other and freely generate $Z_r(\mathbb{R},C_2)$.

4. Bimaximal forms

Let (V,Θ) be a symmetric space of degree $r > 2$. An element $v \in V$ is called an $(r-s+1)$-*zero* if

$$\Theta(v,\ldots,v,v_{s+1},\ldots,v_r) = 0$$

for all $v_{s+1},\ldots,v_r \in V$. This is equivalent to saying that the s-fold symmetric product of v with itself is in the s-radical of V:

$$v \otimes \ldots \otimes v \in \text{s-rad}(V).$$

In particular an element v is in rad(V) if and only if v is an r-zero.

We call (V,θ) s-*nondegenerate* if it has only trivial (r-s+1)-zeros, i.e. if $v\otimes\ldots\otimes v = v^s \in$ s-rad(V) implies $v = 0$. Observe that an s-nondegenerate space is also t-nondegenrate for all $t \leq s$, that a 1-nondegenerate space is just a nondegenerate space.

Lemma 4.1: If $s > 1$ and (V,θ) is an s-nondegenerate indecomposable space then the center Cent(V) is a field.

Proof: Since $r > 2$ and V is indecomposable Cent(V) is a commutative local algebra [1]. Let t be in the maximal ideal of Cent(V) and assume that $t^2 = 0$. Then we have for all $u,x_{s+1},\ldots,x_r \in V$

$$\theta(t(u),t(u),\ldots,t(u),x_{s+1},\ldots,x_r) =$$
$$\theta(t^2(u),u,t(u),\ldots,t(u),s_{s+1},\ldots,x_r) = 0$$

since $t^2(u) = 0$. But (V,θ) is s-nondegenerate, so $t(u) = 0$ for all u and thus $t = 0$. But this suffices to show that Cent(V) is a field.

Lemma 4.2: Let $V = V_1 \perp V_2$ be an orthogonal sum of symmetric spaces. V is s-nondegenerate if and only if V_1 and V_2 are s-nondegenerate.

Proof: Given v_i, $v_{ij} \in V_i$ for $i = 1,2$ and $j = 1,\ldots,r-s$. Then we have

$$\theta(v_1+v_2,\ldots,v_1+v_2,v_{11}+v_{21},\ldots,v_{1(r-s)}+v_{2(r-s)}) =$$
$$\theta_1(v_1,\ldots,v_1,v_{11},\ldots,v_{1(r-s)}) + \theta_2(v_2,\ldots,v_2,v_{21},\ldots,v_{2(r-s)} = 0$$

for all choices of v_{ij} if and only if

$$\Theta_i(v_i,\dots,v_i,v_{i1},\dots,v_{i(r-s)}) = 0$$

for $i = 1,2$ and all choices of v_{ij}. So the first equation implies $v_1 + v_2 = 0$ if and only if the second equation implies $v_1 = 0$, $v_2 = 0$.

We call a space (V,Θ) *maximal* if it is

i) 2-nondegenerate and
ii) $\dim_R(V) \leq \dim_R(\mathrm{Cent}(V))$.

We will show that i) can be replaced here by

i') (V,Θ) has only trivial 2-zeros.

Lemma 4.3: Let (V,Θ) be an indecomposable maximal space. Then there is a finite field extension K of R and a linear form ψ on K such that K together with

$$\Psi(a_1,\dots,a_r) = \psi(a_1\cdot\dots\cdot a_r)$$

is a symmetric space isomorphic to (V,Θ). Furthermore $\dim_R(V) = \dim_R(\mathrm{Cent}(V))$.

Proof: By 4.1 $\mathrm{Cent}(V) = K$ is a field and V is a vector space over K. Since $V \neq 0$ we get from the dimension condition for maximal spaces that V must be one-dimensional over K. So there is a linear isomorphism

$$\phi : K \longrightarrow V,\ \phi(1) = v$$

which induces the structure Ψ of a maximal space on K. Then

$$\Psi(a_1,\dots,a_r) = \Theta(\phi(a_1),\dots,\phi(a_r)) = \Theta(a_1(v),\dots,a_r(v)) =$$

$$\Theta(a_1\cdot\dots\cdot a_r(v),v,\dots,v) = \Psi(a_1\cdot\dots\cdot a_r,1,\dots,1) = \psi(a_1\cdot\dots\cdot a_r)$$

for a suitably defined linear form ψ on K.

Lemma 4.4: Let K be a finite field extension of R and let ψ be a non-zero linear form on K. Then (K,Ψ) is an indecomposable maximal space with

$$\Psi(a_1,\ldots,a_r) = \psi(a_1 \ldots a_r)$$

and K is s-nondegenerate for all $s \leq r - 1$.

Proof: K is s-nondegenerate for all $s \leq r - 1$. Furthermore as in the proof of 3.10 $K \cong \mathrm{Cent}(K)$ and thus is indecomposable. Hence K is a maximal space.

Theorem 4.5: Let (V,Θ) be a maximal space. Then $\dim_R(V) = \dim(\mathrm{Cent}(V))$ and (V,Θ) is s-nondegenerate for all $s \leq r - 1$. Thus (V,Θ) has only trivial 2-zeros.

Proof: V can be decomposed into indecomposable spaces. By lemma 4.2 each indecomposable component is 2-nondegenerate. By 4.3 and 3.1 one of the components (and hence all) are maximal spaces. This implies the claim on the equality of the dimensions. Again using 4.3 all the indecomposable components are defined on finite field extensions K_i of R. By 4.4 these are all s-nondegenerate and by 4.2 V is then s-nondegenerate.

Corollary 4.6: (V_i,Θ_i), $i = 1,2$ are maximal spaces if and only if $V_1 \perp V_2$ is maximal.

Proof follows form the fact that V is maximal if and only if all its indecomposable components are maximal.

Let (V,Θ) be a maximal space. We call (V,Θ) *bimaximal* if

$$r \cdot \dim_R(V_i) \leq |\mathrm{Aut}(V_i,\Theta_i)|$$

for all indecomposable components (V_i,Θ_i) of (V,Θ). Clearly a space is bimaximal if and only if all its indecomposable components are bimaximal.

Corollary 4.7: (V_i,Θ_i) $i = 1,2$ are bimaximal spaces if and only if $V_1 \perp V_2$ is bimaximal.

Theorem 4.8: Let (V,Θ) be a indecomposable bimaximal space. Then the center $K = \mathrm{Cent}(V)$ is a Galois field extension

of R which contains a primitve r-th root of unity and $r \cdot \dim_R(V) = |\mathrm{Aut}(V,\Theta)|$. Furthermore the r-form on K ($\cong$ V) is defined by an element $b \in U(K)$ as $b \cdot \mathrm{tr}$ such that

$$\sigma(b) \cdot b^{-1} \in U(K)^r \text{ for all } \sigma \in \mathrm{Aut}(K/R).$$

Proof: We use the notation of lemma 4.3. Let $f \in \mathrm{Aut}(K,\Psi)$. Then

$$\psi(f(a_1)\cdot\ldots\cdot f(a_r)) = \psi(a_1\cdot\ldots\cdot a_r) = \psi(f(a_1 \cdot a_2)\cdot f(1)\cdot\ldots\cdot f(a_r)),$$

hence $f(a_1a_2)f(1) = f(a_1)f(a_2)$. Define $\sigma(a) = f(a) \cdot f(1)^{-1}$, then $\sigma \in \mathrm{Aut}(K/R)$. The relation between f and σ can also be expressed by

$$(*) \qquad f(a) = \sigma(a) \cdot f(1).$$

Let f_i, i = 1,2 be in $\mathrm{Aut}(K,\Psi)$ and σ_i be the corresponding elements in $\mathrm{Aut}(K/R)$. Then $f_1f_2(a) = f_1(\sigma_2(a)f_2(1)) = \sigma_1(\sigma_2(a)f_2(1))f_1(1) = \sigma_1\sigma_2(a)\sigma_1f_2(1)f_1(1) = \sigma_1\sigma_2(a)f_1f_2(1)$. Thus we get a group homomorphism $\eta : \mathrm{Aut}(K,\Psi) \longrightarrow \mathrm{Aut}(K/R)$. Now let ξ_r be an r-th root of unity K. Then ξ_r defines an automorphism of (K,Ψ) since $\Psi(\xi_r a_1,\ldots,\xi_r a_r) = \Psi(\xi_r^r a_1\cdot\ldots\cdot a_r) = \Psi(a_1,\ldots,a_r)$. Then $\eta(\xi_r)(a) = \xi_r a \cdot (\xi_r 1)^{-1} = a$ hence the group $\mu_r(K)$ of r-th roots of unity is contained in the kernel of η. Conversely let $f \in \mathrm{Ker}(\eta)$. Then $f(a) = a \cdot f(1)$ by (*), hence f is K-linear. So we get

$$\Psi(f(1)^r,a_2,\ldots,a_r) = \psi(f(1) \cdot f(a_2)\cdot\ldots\cdot f(a_r)) = \Psi(1,a_2,\ldots,a_r)$$

hence $f(1)^r = 1$, so

$$\mathrm{Ker}(\eta) = \mu_r(K).$$

This defines a short exact sequence of groups

$$a \longrightarrow \mu_r(K) \longrightarrow \mathrm{Aut}(K,\Psi) \longrightarrow \mathrm{Aut}(K/R).$$

We have $|\mu_r(K)| \leq r$, $|\mathrm{Aut}(K/R)| \leq \dim_R(K)$ and by hypothesis $r \cdot \dim_R(K) \leq |\mathrm{Aut}(K,\Psi)|$. This together with the short exact sequence can only hold if equality holds everywhere. So we get K over R Galois, K contains a primitive r-th root of unity and the last map in the short exact sequence is an epimorphism.

In particular (K,Ψ) is separable and we may apply theorem 3.12 to get $\Psi(a_1,\ldots,a_r) = tr(b \cdot a_1 \ldots a_r)$. Let $f \in Aut(K,\Psi)$ and $\eta(f) = \sigma \in Aut(K/R)$. Then $tr(ba_1\ldots a_r) = tr(b\sigma(a_1)f(1)\ldots\sigma(a_r)f(1))$ (by (*)) $= tr(\sigma^{-1}(bf(1)^r) \cdot a_1\ldots a_r)$ for all $a_i \in K$. Hence $\sigma(b) \cdot b^{-1} = f(1)^r \in U(K)^r$.

Corollary 4.9: Let (V,θ) be a bimaximal space. Then (V,θ) is separable.

Theorem 4.10: Let K be a finite Galois extension of R, which contains a primitive r-th root of unity. Let $b \in U(K)$ such that $\sigma(b)/b \in U(K)^r$ for all $\sigma \in Aut(K/R)$. Then $(K,\langle b\rangle_r)$ is a bimaximal space.

Proof: By lemma 4.4 and lemma 3.10 $(K,\langle b\rangle_r)$ is an indecomposable maximal space. We compute $Aut(K,\langle b\rangle_r)$. Let $\sigma \in Aut(K/R)$ and $\sigma(b)/b = c^r$. Define $K \longrightarrow K$ by $f(a) = \sigma(a) \cdot c$. Then $tr(bf(a_1)\cdot\ldots\cdot f(a_r)) = tr(b\sigma(a_1)\ldots\sigma(a_r) \cdot \sigma(b)/b) = tr(\sigma(ba_1\ldots a_r)) = tr(ba_1\ldots a_r)$ and $f \in Aut(K,\Psi)$. Different pairs $(\sigma,\xi_r \cdot c)$ define different automorphisms f, so $r \cdot \dim_R(K) \leq |Aut(K,\Psi)|$.

Theorem 4.11: Let V,W be bimaximal. Then $V \otimes W$ is bimaximal.

Proof: Without loss of generality we can assume V and W indecomposable. By theorem 4.8 we may assume indecomposable bimaximal spaces $(K,\langle b\rangle_r)$ and $(L,\langle d\rangle_r)$ with Galois extensions K and L of R both being subfields of a separable closure of R. Let $K \cdot L$ be the compositum of K and L and $M = K \cap L$. Since K and L are linearly disjoint over M we get $Aut(K \cdot L/K) \cong Aut(L/M)$ by restriction of the automorphisms to L. We identify both sets along this map. Furthermore $Aut(M/R) \cong Aut(L/R)/Aut(K \cdot L/K)$. Let $\phi_1,\ldots,\phi_s \in Aut(L/R)$ be a complete set of representatives for the element of $Aut(M/R)$. Then every element of $Aut(L/R)$ can be written uniquely as $\tau = \rho \circ \phi_i$ where $\rho \in Aut(K \cdot L/R)$.

Furthermore there is an isomorphism

$$\lambda : K \otimes_R L \cong \Pi_{\{\phi_1,\ldots,\phi_s\}} K \cdot L,$$

defined by $\lambda(x \otimes y) = \Sigma x \cdot \phi_i(y)$. The copies of $K \cdot L$ are symmetric spaces by $(b \cdot \phi_i(d)) \cdot tr$ for $i = 1,\ldots,s$. Since $Aut(K/R) \cong Aut(K \cdot L/R)/Aut(K \cdot L/K)$ every element in $Aut(K \cdot L/R)$ can also be written uniquely as (σ,ρ) with $\sigma \in Aut(K/R)$ and $\rho \in Aut(L/M) \cong Aut(K \cdot L/K)$ with

$$(\sigma,\rho)(x \cdot y) = \sigma(x) \cdot \sigma\rho(y)$$

where σ stands also for a fixed chosen representative in $Aut(K \cdot L/R)$. Thus we get

$$\frac{(\sigma,\rho)(b \cdot \phi_i(d))}{b \cdot \phi_i(d)} = \frac{\sigma(b) \cdot \sigma\rho\phi_i(d)}{b \cdot \phi_i(d)} = \frac{\sigma(b)}{b} \cdot \frac{\sigma\rho\phi_i(d)}{d} \cdot \frac{d}{\phi_i(d)} \in U(K \cdot L)^r.$$

To show that λ is an isomorphism of symmetric spaces let $x_j \otimes y_j \in K \otimes_R L$, $j = 1,\ldots,r$. Then

$$\begin{aligned}
&\Psi(\lambda(x_1 \otimes y_1),\ldots,\lambda(x_r \otimes y_r)) \\
&= \Sigma_{i_1,\ldots,i_r} \Psi(x_1\phi_{i_1}(y_1),\ldots,x_r\phi_{i_r}(y_r)) \\
&= \Sigma_i \Psi(x_1\phi_i(y_1),\ldots,x_r\phi_i(y_r)) \\
&= \Sigma_i tr(b \cdot x_1 \cdot \ldots \cdot x_r \cdot \phi_i(d \cdot y_1 \cdot \ldots \cdot y_r) \\
&= \Sigma_i \Sigma_{(\sigma,\rho)} \sigma(bx_1 \ldots x_r)\sigma\rho\phi_i(dy_1 \ldots y_r) \\
&= \Sigma_\sigma \Sigma_\tau \sigma(bx_1 \ldots x_r)\tau(dy_1 \ldots y_r) \\
&= tr(bx_1 \ldots x_r) \cdot tr(dy_1 \ldots y_r) \\
&= \Psi(x_1 \otimes y_1,\ldots,x_r \otimes y_r).
\end{aligned}$$

This together with the previous observation on the elements of the form $b \cdot \phi_i(d)$ and theorem 4.10 shows that $K \otimes_R L$ is again an orthogonal sum of bimaximal spaces.

For the rest of this section assume that there is a primitive r-th root of unity ξ_r in R. We are going to develop the theory of Witt rings for bimaximal spaces essentially in the same way as for separable spaces in section 3.

Theorem 4.12: The isomorphism classes of bimaximal spaces form a sub-semiring $P_r^{bim}(R)$ of $P_r^{sep}(R)$ containing $P_r^D(R)$.

Lemma 4.13: Let H be a finite subgroup of $G_r(R)$ and let u be a bimaximal class in $P_r(R)$. Then the (unique) decomposition $u = u_H \perp t_H(u)$ has bimaximal factors.

Theorem 4.14: Let H be a finite subgroup of $G_r(R)$. Then the set $Y_r(R,H)$ of H-equivalence classes in $W_r(R,H)$ whose unique H-reduced representative is bimaximal, is a subring of $W_r(R,H)$.

Proof: Observe using the assumption that R contains a primitive r-th root of unity, that every symmetric class of the form $\langle\alpha\rangle$ in $G_r(R)$ is bimaximal. Then the proof of theorem 3.8 can be easily modified for this case.

Corollary 4.15: There is a sequence of commutative subrings

$$W_r^D(R,H) \subseteq Y_r(R,H) \subseteq Z_r(R,H) \subseteq W_r(R,H).$$

Theorem 3.18 can also be applied to bimaximal indecomposable spaces of the form $(K,\langle b\rangle_r)$. Observe that $\sigma(b)/b = c^r = (c^t)^s$ for an element $c \in U(R)$. So we get

Theorem 4.16: The ring homomorphism $\Omega : W_r(R,H) \longrightarrow W_s(R,H)$ for $r = st$, $s > 2$ restricts to a ring homomorphism $Y_r(R,H) \longrightarrow Y_s(R,H)$.

5. Witt Rings over finite fields

Let K be a finite separable field extension of R. Then by theorem 3.12 all the representatives b of an element $\bar{b}$ of $U(K)/U(K)^r$ define the same indecomposable separable space $(K,\langle b\rangle_r)$ of degree r (up to isomorphims).

Furthermore the automorphism group $G = \mathrm{Aut}(K/R)$ acts on $U(K)/U(K)^r$ and all elements of the same orbit under this action define isomorphic spaces. Different orbits determine nonisomorphic space, hence

Proposition 5.1: There is a one-to-one correspondence between the isomorphism classes of indecomposable separable spaces with center K of degree r and the orbits under G in $U(K)/U(K)^r$.

Let p be a prime and $R = GF(p^m)$, $K = GF(p^{mn})$. Let $2 < r < p$, $s := (p^m-1,r)$, and $t := (p^{mn}-1,r)$.

Define g to be a generator of the cyclic group U(K). Since g has multiplicative order $p^{mn} - 1$ we get $U(K)/U(K)^r = \{1,\bar{g},\ldots,\bar{g}^{t-1}\} \cong \mathbb{Z}/(t)$. For ϕ the Frobenius map on K we have $\phi^m(x) = x^{p^m} = x$ for precisely the elements $x \in F$. The action of ϕ^m on K translates into multiplication by p^m on $\mathbb{Z}/(t)$. The elements fixed under the multiplication by p^m (and by powers p^{mi} of it) form the kernel of the multiplication by $p^m - 1$, denoted by $(\mathbb{Z}/(t))^G$.

The following sequence of cyclic groups is exact

$$0 \longrightarrow (\mathbb{Z}/(t))^G \longrightarrow \mathbb{Z}/(t) \xrightarrow{p^m-1} \mathbb{Z}/(t)$$

and the image of $p^m - 1$ is $(p^m - 1,t)/(t) = (s)/(t)$, hence $(\mathbb{Z}/(t))^G \cong \mathbb{Z}/(s)$.

Translated back into terms of Galois fields we get $(U(K)/U(K)^r)^G = \{1,\bar{g}^u,\ldots,\bar{g}^{(s-1)u}\}$ where $t = su$. These are precisely the elements which each form an orbit of length 1.

Theorem 5.2: Two indecomposable separable spaces $(K,\langle g^{iu}\rangle_r)$ and $(K,\langle g^{ju}\rangle_r)$ with $0 \leq i,j < s$ are isomorphic iff $i = j$. There are at least s and at most t isomorphism classes of indecomposable separable spaces of degree r over R with center K.

The following examples illustrate this situation. Let $p = 7$, $m = 1$, $n = 3$ and $r = 4$ then there are precisely two distinct indecomposable separable spaces over GF(7) of degree 4 with center $GF(7^3)$. For $p = 7$, $m = 1$, $n = 2$ and $r = 4$ there are precisely three distinct indecomposable separable spaces over GF(7) of degree 4 with center $GF(7^2)$ coming from the orbits (in $\mathbb{Z}/(4) \cong U(K)/U(K)^4$)

$$\{\overline{0}\},\ \{\overline{1},\overline{3}\},\ \text{and}\ \{\overline{2}\},$$

i.e. $(GF(7^2),\langle 1\rangle_4)$, $(GF(7^2),\langle g\rangle_4)$, and $(GF(7^2),\langle g^2\rangle_4)$, where g is a generator of $U(GF(7^2))$.

To see which of these spaces are bimaximal we first observe that $K = GF(p^{mn})$ contains a primitive r-th root of unity iff $r/(p^{mn}-1)$ iff $p^{mn} \equiv 1 \bmod(r)$. So the last congruence is a necessary condition for any of the spaces $(K,\langle b\rangle_r)$ to be bimaximal. But then $t = (p^{mn}-1,r) = r$ so by applying theorems 4.8 and 4.10 we get that the one-element orbits in $\mathbb{Z}/(r)$ under G are precisely the bimaximal spaces hence

Corollary 5.3: If $p^{mn} \equiv 1 \bmod(r)$ with $2 < r < p$ and g is a generator of U(K) then there are precisely s non-isomorphic indecomposable bimaximal spaces $(K,\langle g^{iu}\rangle_r)$, $0 \leq i < s$ with center K, where $s = (p^m-1,r)$ and $su = r$.

Corollary 5.4: If $p^m \equiv 1 \bmod(r)$ then all separable spaces of degree r are bimaximal and for each K there are precisely r indecomposable bimaximal spaces with center K.

Let us assume $p^m \equiv 1 \bmod(r)$, $2 < r < p$ and take $H := U(R)/(U(R))^r$. We want to determine the Witt rings $Z_r(R,H) = Y_r(R,H)$. Observe first that for any $n \geq 1$ and $K = GF(p^{mn})$ we have $|U(K)/U(R)| = (p^{mn}-1)/(p^m-1) = (p^m)^{n-1}+\ldots+(p^m)^0 \equiv 1+\ldots+1 = n \bmod(r)$.
Furthermore observe the general fact that the sequence of cyclic groups

$$U(R)/(U(R))^r \longrightarrow U(K)/(U(K))^r \longrightarrow (U(K)/U(R))/(U(K)/U(R))^r \longrightarrow 1$$

is exact. The last cyclic group has order $q := (r,n) = (r,|U(K)/U(R)|)$. The first map defines the action of H on $U(K)/(U(K))^r = (U(K)/(U(K))^r)^G$, i.e. on the indecomposable bimaximal spaces. The action is given through the image of $U(R)/(U(R))^r$ which consists of the elements $\{1,\bar{g}^q,\bar{g}^{2q},\ldots,\bar{g}^{r-q}\} = C_{r/q}$ where g is a cyclic generator of U(K) and $q = (n,r)$. So there are q orbits under the action of H, each orbit having r/q elements. The spaces corresponding to the elements of one orbit add up to an H-space in $P_r^{bim}(R)$. If we define $\mathbb{Z}[\zeta_k] := \mathbb{Z}[C_k]/(\sum x | x \in C_k)$ (for $k \neq 1$ this is an isomorphism anyway, for k = 1 this give the zero ring) then the part of $Y_r(R,H)$ defined by K is $\sum_{i=0}^{q-1} \mathbb{Z}[\zeta_{r/q}]. (K,<g^i>_r)$. So we get

Theorem 5.5: If $p^m \equiv 1 \bmod(r)$, $2 < r < p$, $R = GF(p^m)$ and $H = G_r(R)$. If furthermore $y_n^i := (GF(p^{mn}),<g_n^i>_r)$ for fixed chosen generators g_n of $U(GF(p^{mn}))$, then

$$Y_r(R,H) = Z_r(R,H) = \sum_{n\geq 1} \sum_{i=1}^{(n,r)} \mathbb{Z}[\zeta_{r/(n,r)}]y_n^i.$$

Corollary 5.6: Under the hypotheses of theorem 5.5 if r is prime then

$$Y_r(R,H) = \sum_{\substack{n\geq 1 \\ r\nmid n}} \mathbb{Z}[\zeta_r]y_n^\circ.$$

The multiplication is given by

$$y_n^\circ y_m^\circ = (n,m)y^\circ_{[n,m]} \text{ for all } m,n \text{ with } r \nmid n,\ r \nmid m.$$

BIBLIOGRAPHY

[1] D.K. HARRISON, A Grothendieck Ring of Higher Degree Forms, J. Algebra 35 (1975), 123 - 138.

[2] E. WITT, Theorie der quadratischen Formen in beliebigen Körpern, J. reine Angew. Math. 176 (1937), 31 - 44.

Received: December 1986