ZESZYTY NAUKOWE WYŻSZEJ SZKOŁY PEDAGOGICZNEJ W BYDGOSZCZY
Problemy Matematyczne 1983/84 z.5/6

ANDRZEJ PRÓSZYŃSKI
WSP w Bydgoszczy

ON ORTHOGONAL DECOMPOSITION OF HIGHER DEGREE FORMS x)

1. What is a higher degree form ? At first we recall what is a quadratic form over a commutative ring R. The most known definitions are following:

(1) Most essential : It is a homogeneous polynomial over R of degree 2 .

(2) Most comfortable: It is a symmetric bilinear mapping $B: M\times M \longrightarrow N$, for some R-modules M,N.

(3) Most general: It is a mapping of R-modules $Q: M \longrightarrow N$ such that

1° $Q(rx) = r^2Q(x)$ for any $r \in R$, $x \in M$,

2° $B(x,y) := Q(x+y)-Q(x)-Q(y)$ is R-bilinear .

The first definition is good if $M=R^n$ and $N=R$. The second is good if $2 \in U(R)$; then $Q(x)=B(x,x)/2$.

A form of degree m is defined by the following evident generalizations:

(1′) Most essential: It is a homogeneous polynomial over R of degree m.

(2′) Most comfortable: It is a symmetric m-linear mapping $P: M \times \dots \times M \longrightarrow N$ for some R-modules M,N.

The first definition will be good in the free case, and the second in the case if $m! \in U(R)$. The simple generalization of (3) gives us so called m-applications (see the next paper) , but that definition is not compatible with (1′)- higher degree forms are not mappings in general! Hence we must look for another ways to obtain the most general definition.

---

x) Lecture given in Montpellier, October 1979

Recall the following fact contained in [1]:

<u>**Theorem.**</u> Let $Q\colon M \longrightarrow N$ be a quadratic form over R. For any commutative R-algebra A there exists the unique quadratic form $Q_A\colon M \otimes_R A \longrightarrow N \otimes_R A$ over A such that $Q_A(x \otimes 1) = Q(x) \otimes 1$, $B_{Q_A}(x \otimes 1, y \otimes 1) = B_Q(x,y) \otimes 1$.

For any R-algebra homomorphism $u\colon A \longrightarrow B$ the following diagram:

$$\begin{tikzcd} M \otimes A \arrow[r, "Q_A"] \arrow[d, "1 \otimes u"'] & N \otimes A \arrow[d, "1 \otimes u"] \\ M \otimes B \arrow[r, "Q_B"] & N \otimes B \end{tikzcd}$$

is commutative.

This allows us to introduce the following, contained in [5],

<u>Definition.</u> A <u>polynomial law</u> on (M,N) is a system $F=(F_A)$ of mappings $F_A\colon M \otimes A \longrightarrow N \otimes A$ for any (commutative) R-algebra A, such that for any R-algebra homomorphism $u\colon A \longrightarrow B$ the following diagram:

$$\begin{tikzcd} M \otimes A \arrow[r, "F_A"] \arrow[d, "1 \otimes u"'] & N \otimes A \arrow[d, "1 \otimes u"] \\ M \otimes B \arrow[r, "F_B"] & N \otimes B \end{tikzcd}$$

is commutative. In other words, F is a natural transformation of functors $M \otimes -$, $N \otimes -\colon R\text{-Alg} \longrightarrow \text{Set}$.

Now the most general definition of a <u>form of degree m</u> on (M,N) is following:

(3′) It is a polynomial law $F\colon M \otimes - \longrightarrow N \otimes -$ such that $F_A(\underline{x}a) = F_A(\underline{x})a^m$ for any A, $a \in A$ and $\underline{x} \in M \otimes A$.

<u>Corollary.</u> Any form F of degree m on (M,N) has the following shape:

$$F_A(x_1 \otimes a_1 + \ldots + x_n \otimes a_n) = \sum_{m_1+\ldots+m_n=m} F_{m_1,\ldots,m_n}(x_1,\ldots,x_n) \otimes a_1^{m_1} \ldots a_n^{m_n}$$

where $F_{m_1,\dots,m_n} : M^n \longrightarrow N$ are uniquely determined by F.
In particular

a) $F_R = F_m : M \longrightarrow N$ is the mapping induced by F,

b) $PF = F_{1,\dots,1}$ is tne symmetric m-linear form associated with F (we will assume that $m > 0$).

It can be proved (see [5])that (3′) is compatible with (1′), (2′) and (3)in the following way:

(1′): If $\{e_1,\dots,e_n\}$ is a fixed basis of M then F corresponds to the ordinary form:

$$F_{R[T_1,\dots,T_n]}(e_1 \otimes T_1 + \dots + e_n \otimes T_n) =$$
$$= \sum F_{m_1,\dots,m_n}(e_1,\dots,e_n) \otimes T_1^{m_1} \dots T_n^{m_n} .$$

(2′): If $m! \in U(R)$ then $F_{m_1,\dots,m_n}(x_1,\dots,x_n) =$
$$= PF(\underbrace{x_1,\dots,x_1}_{m_1},\dots,\underbrace{x_n,\dots,x_n}_{m_n})/m_1!\dots m_n!$$

(3): For m=2 F is given by $Q=F_2$ and $B=F_{1,1}=B_Q$.

2. <u>Orthogonality</u>. Let M be a fixed R-module. A <u>module of degree m</u> is a pair (X,F) where F is a form of degree m on (X,M). We define the <u>orthogonal product</u>:

$(X,F) \perp (Y,G) := (X \oplus Y, F \perp G)$

where, in the natural way, $(F \perp G)_A(\underline{x}+\underline{y}) = F_A(\underline{x}) + G_A(\underline{y})$. In the case of (1′)this gives us the familiar operation:

$$(F(T_1,\dots,T_n),\ G(S_1,\dots,S_k)) \longmapsto F(T_1,\dots,T_n) + G(S_1,\dots,S_k)$$
$$\in R[T_1,\dots,T_n,S_1,\dots,S_k] .$$

For the work with the orthogonal decomposition we need a good orthogonality relation in any (X,F). The word „good'' means that:

(i) The relation is symmetric.

(ii) $E^{\perp}$ is a submodule of X for any subset E of X.

(iii) If $X = Y \oplus Z$ then $X = Y \perp Z$ iff Y and Z are orthogonal.

(iv) For m=2 we obtain the usual orthogonality relation.

The above properties are satisfied (for the proofs we refer to [4])if we introduce the following

__Definition.__ $x, y \in X$ are __orthogonal__ (in (X,F)) iff the following equivalent conditions are satisfied:

(a) $F_A(x \otimes a + y \otimes b + \underline{x}) = F_A(x \otimes a + \underline{x}) + F_A(y \otimes b + \underline{x}) - F_A(\underline{x})$
for any A, a, $b \in A$ and $\underline{x} \in X \otimes A$.

(b) $F_{m_1, \dots, m_n}(x, y, X, \dots, X) = 0$ for $n \geqslant 2$ and $m_1, m_2 > 0$.

(c) (If we assume that $m \geqslant 2$ and $(n-1) \notin \mathfrak{z}(M)$=the set of all zero divisors in M) $PF(x, y, X, \dots, X) = 0$.

Moreover, we define $\mathrm{rad}(X) = X^{\perp}$ and $\ker(X) = \mathrm{rad}(X) \cap \{x \in X; F_R(x) = 0$

$(X,F)$is called __non-degenerate__ iff $\mathrm{rad}\,(X) = 0$.

__Remark.__ For a submodule Y of X we have in general only $Y^{\perp} \cap Y \subset \mathrm{rad}(Y)$ $(=\mathrm{rad}(Y, F|Y))$, but the equality holds if Y is an orthogonal summand of X. Other __elementary__ properties of $\perp$ are the same as in the quadratic case (see [4]).

The following questions arise:

1° Description of indecomposable forms.

2° The uniqueness of the orthogonal decomposition.

For example, nonsingular quadratic spaces are indecomposable only in dimensions ≤ 2 and satisfy the Witt cancellation property, but the orthogonal decomposition is __not__ unique in general (even up to an isomorphism). It follows from the next two sections that the situation is quite different for $m \geqslant 3$.

__3. Indecomposable forms.__ Many examples of indecomposable forms are given by the multiplication. The following results (see [4]) were first proved in [2] over such fields that the definition (2') can be used.

__Theorem.__ Let R be a domain, $F \in R[T_1, \dots, T_n]_m$ and $m, n, k \geqslant 1$. If $\ker(F) = 0$ then $F(T_1, \dots, T_n)T_{n+1}^k \in R[T_1, \dots, T_{n+1}]_{m+}$ is non-degenerate. Moreover, this form is indecomposable, if one of the following conditions is satisfied:

(a) F is non-degenerate (b) $m > k$ or (c) $m > 1$ and $k \neq 0$ in R.

__Corollary.__ Let R be a domain. For any $m \geqslant 3$ and $n \geqslant 2$ there exists a non-degenerate indecomposable form $F_{mn} \in R[T_1, \dots, T_n]_m$.

__Proof.__ Define F_{mn} for $m \geqslant 2$ and $n \geqslant 1$ in the following way:

$F_{m1}=T_1^m$, $F_{2,2k}$ is hyperbolic, $F_{2,2k+1}=F_{2,2k}+T^2_{2k+1}$ (all kernels are zero), $F_{m+1,n+1}=F_{mn}T_{n+1}$.
Next apply the above theorem.

Let us consider the monomials $T_1^{m_1}\dots T_n^{m_n}\in R[T_1,\dots,T_n]$ where $m_1,\dots,m_n>0$. Which of them are decomposable ?
If $R=R_1\times R_2$ then the canonical decomposition $R^n=R_1^n\times R_2^n$ is orthogonal. Hence we can assume that R is connected.

<u>Theorem.</u> If R is connected then decomposable monomials over R can be only the following ones:
1) T_1T_2 (iff $2\in U(R)$)
2) $T_1^{p^n}\ T_2^{p^n}$ where $p\neq 2$ is a prime (iff char $(R)=p$).

They can be decomposed in the following way:

$$T_1^{p^n}\ T_2^{p^n}=(S_1+S_2)^{p^n}\ (S_1-S_2)^{p^n}=S_1^{2p^n}-S_2^{2p^n}\ .$$

<u>4. The uniqueness of the decomposition.</u> The following results were first proved in [3] for symmetric m-linear mappings and are true for forms of degree $m\geqslant 3$ is we assume that $(m-1)!\notin\mathfrak{Z}(M)$ (then the definition (c) can be used).
<u>Lemma .</u> If $X=X_1\perp\dots\perp X_n$ then $E^\perp=(X_1\cap E^\perp)\perp\dots\perp(X_n\cap E^\perp)$ for any $E\subset X$.
<u>Proof.</u> Let $x\in E^\perp$ and $x=y+z$ where $y\in Y=X_i$ and $z\in Z=X_1\perp\dots\perp\hat{X}_i\perp\dots\perp X_n$. We must prove that $y\in E^\perp$. For, let $e\in E$ and $e=y'+z'$ as above. Then:

$$PF(y,e,X,\dots,X)=PF(y,y',Y,\dots,Y)+PF(0,z',Z,\dots,Z)\overset{!}{=}PF(y,y',Y,\dots,Y)$$
$$+\ PF(z,z',0,\dots,0)=\ PF\ (x,e,Y,\dots,Y)=0.$$

<u>Theorem.</u> Suppose that (X,F) is non-degenerate and $X=X_1\perp\dots\perp X_n$ where X_i are indecomposable. Then any orthogonal summand Y of X has the form $Y=X_{i_1}\perp\dots\perp X_{i_s}$, $i_1<\dots<i_s$. In particular, $X=X_1\perp\dots\perp X_n$ is the unique decomposition with indecomposable summands.
<u>Proof.</u> Let $X=Y\perp Z$. Then $X_i=(Y\cap X_i)\perp(Z\cap X_i)$ by the lemma and hence $X_i\subset Y$ or $X_i\subset Z$.
If $X_1,\dots,X_s\subset Y$ and $X_{s+1},\dots,X_n\subset Z$ then $Y=X_1\perp\dots\perp X_s$.

Remark. The above is false if $m=2$ or $(m-1)! \in \mathfrak{Z}(M)$. For example, let R be a field of characteristic $p \neq 0,2$ and $m=p^n+1$. Then $T_1^m + T_2^m$ is non-degenerate and isomorphic to $(S_1+S_2)^m + (S_1-S_2)^m = 2S_1^m + 2S_2^m$.

Let us consider only such (X,F) that F is non-degenerate and X is finitely generated (resp. finitely generated and projective). Let R be noetherian (resp. $R=R_1 \times \ldots \times R_s$ where R_i are connected). Then for any (X,F) there exists the unique decomposition $X=X_1 \perp \ldots \perp X_n$ with indecomposable summands. In particular, the cancellation property is satisfied.

REFERENCES

[1] BOURBAKI N., Algèbre, Chap. 9, Paris 1959

[2] GILPIN M., Products of symmetric forms, J. Algebra 33(3), 1975, p. 430-434

[3] HARRISON D.K., A Grothendieck ring of higher degree forms, J. Algebra 35, 1975, p. 123-138

[4] PRÓSZYŃSKI A., On orthogonal decomposition of homogeneous polynomials, Fund. Math. XCVIII, 1978, p. 201-217

[5] ROBY N., Lois polynômes et lois formelles en théorie des modules, Ann.Ec.Norm. Sup. 80, 1963 , p.213-348

O ROZKŁADZIE ORTOGONALNYM FORM WYŻSZYCH STOPNI

Streszczenie

Praca stanowi tekst referatu wygłoszonego w Montpellier. Zawiera twierdzenia o rozkładzie ortogonalnym form wyższych stopni, zasadniczo różne od faktów znanych z teorii form kwadratowych.