On orthogonal decomposition of homogeneous polynomials

by

A. Prószyński (Toruń)

Abstract. The paper is concerned with the study of the orthogonal decomposition of forms (homogeneous polynomials in the sense of N. Roby). The first three sections yields some basic definitions and lemmas. Then the following results are proved:

(1) Any form over a Prüfer ring admits the canonical decomposition into an orthogonal sum of forms of special types (Theorem 4.6).

(2) There exist numerous indecomposable forms of degree $\geqslant 3$ (Section 5).

(3) The orthogonal decomposition of non-degenerate forms of degree $\geqslant 3$ is unique (Corollary 6.4).

Moreover, Section 6 yields some structural information related to categories of forms.

0. Preliminaries. In this paper all rings and algebras are commutative and have the unit element 1; all modules are unitary. For any R-module M denote $M\otimes. = M\otimes_{R^\cdot}$, and, moreover

$$D(M) = \{r \in R |\ rm = 0 \text{ for some } 0 \neq m \in M\},$$

$$E(M) = M[T_1, T_2, \ldots] = M\otimes R[T_1, T_2, \ldots] = M\otimes E(R).$$

Note also the following well-known

LEMMA 0.1. *If* $m>1$ *then*

$$\left(\binom{m}{1}, \ldots, \binom{m}{m-1}\right) = \begin{cases} (1) & \text{if } m \text{ is not the power of a prime,} \\ (p) & \text{if } m = p^n. \end{cases}$$

Moreover, if $m = p^n$ *then* $p^2 \mid \binom{m}{i}$ *iff* $p^{n-1} \nmid i$.

1. Modules of degree m. We recall some ideas contained in [6] and introduce some natural definitions.

For any R-module X consider the functor $X\otimes.$ from the category of all (commutative) R-algebras to the category of sets. Any natural transformation $F = (F_A): X\otimes. \to M\otimes.$ is called a *polynomial* on (X, M). It is called a *form of degree m*

iff $F_A(\underline{x}a) = F_A(\underline{x})a^m$ for any R-algebra A, $a \in A$, and $\underline{x} \in X \otimes A$. Then we have the formula

$$(1.1) \qquad F_A(x_1 \otimes a_1 + \ldots + x_n \otimes a_n) = \sum_{m_1+\ldots+m_n=m} F_{m_1,\ldots,m_n}(x_1, \ldots, x_n) \otimes a_1^{m_1} \ldots a_n^{m_n}$$

where $F_{m_1,\ldots,m_n}: X^n \to M$ are uniquely determined by F. In particular, $PF = F_{1,\ldots,1}$ is the symmetric m-linear form associated with F. (We assume in this paper that $m > 0$.)

There exists a one-to-one correspondence between forms of degree 1 (resp. 2) and linear (resp. quadratic) mappings given by $F \mapsto F_m$, $m = 1, 2$. Let f be an R-homomorphism. Then f corresponds to $F = f \otimes .$, and we abbreviate this to $F = f$.

Now introduce the category $R\text{-Mod}_M^m$ as follows:

(a) Objects of $R\text{-Mod}_M^m$ are modules of degree m over M, i.e., pairs (X, F) where X is an R-module and F is a form of degree m on (X, M).

(b) $f: (X, F) \to (Y, G)$ in $R\text{-Mod}_M^m$ iff $f: X \to Y$ is R-linear and $F = G \circ f$. (In the case where $f: X \subset\to Y$ we write $f: (X, F) \subset\to (Y, G)$ and $F = G|_X$.)

There exists a functor $\perp: R\text{-Mod}_M^m \times R\text{-Mod}_M^m \to R\text{-Mod}_M^m$ defined by

$$(X, F) \perp (Y, G) = (X \oplus Y, F \perp G), \quad f \perp g = f \oplus g,$$

where

$$(F \perp G)_A(\underline{x}+\underline{y}) = F_A(\underline{x}) + G_A(\underline{y}) \quad \text{for any } \underline{x} \in X \otimes A \text{ and } \underline{y} \in Y \otimes A.$$

Let $(X, F) \in \mathrm{Ob}\, R\text{-Mod}_M^m$. A decomposition $X = Y \oplus Z$ is called *orthogonal* iff $(X, F) = (Y, G) \perp (Z, H)$ where (Y, G), $(Z, H) \in \mathrm{Ob}\, R\text{-Mod}_M^m$. Since $m > 0$, it follows that $G = F|_Y$ and $H = F|_Z$. Then we write $X = Y \perp Z$ and $F = G \perp H$.

Assume that X is a free R-module with a fixed basis $\{e_1, \ldots, e_n\}$. It is known from [6] that any form F on (X, M) corresponds to an ordinary form with coefficients in M, namely

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

We write briefly

$$F = \sum F_{m_1,\ldots,m_n}(e_1, \ldots, e_n) \otimes T_1^{m_1} \ldots T_n^{m_n}.$$

In this correspondence, the operation $\perp$ acts as follows: if $F \in M[T_1, \ldots, T_n]$ and $G \in M[T_{n+1}, \ldots, T_k]$ have the same degree, then

$$F \perp G = F(T_1, \ldots, T_n) + G(T_{n+1}, \ldots, T_k) \in M[T_1, \ldots, T_k].$$

Similarly, the usual orthogonal decomposition of forms is a special case of the above definition.

Let $(X, F) \in \mathrm{Ob}\, R\text{-Mod}_M^m$ and $(X, G) \in \mathrm{Ob}\, R\text{-Mod}_K^k$. Then we obtain $(X, F \cdot G) \in \mathrm{Ob}\, R\text{-Mod}_M^{m+k}$ where $(F \cdot G)_A = F_A \cdot G_A$. This corresponds to the ordinary multiplication of forms in the case of $X = R^n$.

2. The orthogonality relation. Let $(X, F) \in \mathrm{Ob}\, R\text{-Mod}_M^m$. We say that elements $x_1, x_2 \in X$ are *orthogonal* (in (X, F)) iff the conditions of the following lemma are satisfied.

LEMMA 2.1. *The following conditions are equivalent*:

(1) $F_A(x_1 \otimes a_1 + x_2 \otimes a_2 + \underline{x}) = F_A(x_1 \otimes a_1 + \underline{x}) + F_A(x_2 \otimes a_2 + \underline{x}) - F_A(\underline{x})$ *for any* R*-algebra* A, $a_1, a_2 \in A$, $\underline{x} \in X \otimes A$.

(2) $F_{E(R)}(x_1 \otimes T_1 + x_2 \otimes T_2 + \underline{x}) = F_{E(R)}(x_1 \otimes T_1 + \underline{x}) + F_{E(R)}(x_2 \otimes T_2 + \underline{x}) - F_{E(R)}(\underline{x})$ *where* $\underline{x} = x_3 \otimes T_3 + \ldots + x_n \otimes T_n \in E(X)$.

(3) $F_{m_1,\ldots,m_n}(x_1, x_2, X, \ldots, X) = 0$ *if* $n \geq 2$ *and* $m_1, m_2 > 0$.

Proof. (1)$\Leftrightarrow$(2) is evident since F is a natural transformation.

(2)$\Leftrightarrow$(3) Consider the endomorphisms $u_i: E(R) \to E(R)$ given by $u_i(T_i) = 0$ and $u_i(T_j) = T_j$ for $j \neq i$. Let $u_{12} = u_1 \circ u_2$ and $t = x_1 \otimes T_1 + \ldots + x_n \otimes T_n$. Then

$$\begin{aligned} &F_{E(R)}(x_1 \otimes T_1 + x_2 \otimes T_2 + \underline{x}) - F_{E(R)}(x_1 \otimes T_1 + \underline{x}) - F_{E(R)}(x_2 \otimes T_2 + \underline{x}) + F_{E(R)}(\underline{x}) \\ &\quad = F_{E(R)}(t) - F_{E(R)}((1 \otimes u_1)(t)) - F_{E(R)}((1 \otimes u_2)(t)) + F_{E(R)}((1 \otimes u_{12})(t)) \\ &\quad = (1 \otimes 1 - 1 \otimes u_1 - 1 \otimes u_2 + 1 \otimes u_{12}) F_{E(R)}(t) \\ &\quad = \sum_{m_1, m_2 > 0} F_{m_1,\ldots,m_n}(x_1, \ldots, x_n) \otimes T_1^{m_1} \ldots T_n^{m_n} \end{aligned}$$

by Formula (1.1). This completes the proof.

Observe that in the case of $m = 1$ all elements are orthogonal, and in the case of $m = 2$ we obtain an ordinary orthogonality relation in a quadratic module.

We call subsets $E_1, E_2 \subset X$ orthogonal iff all pairs e_1, e_2, $e_1 \in E_1$, $e_2 \in E_2$, are orthogonal. The following lemma explains connection with the orthogonal decomposition.

LEMMA 2.2. *If* $X = Y \oplus Z$ *then* $X = Y \perp Z$ *iff* Y, Z *are orthogonal.*

Proof. Let $X = Y \perp Z$ and let A be an R-algebra, $a, b \in A$, $y \in Y$, $z \in Z$, $\underline{y} \in Y \otimes A$, $\underline{z} \in Z \otimes A$. Then

$$\begin{aligned} &F_A(y \otimes a + z \otimes b + (\underline{y}+\underline{z})) - F_A(y \otimes a + (\underline{y}+\underline{z})) - F_A(z \otimes b + (\underline{y}+\underline{z})) + F_A(\underline{y}+\underline{z}) \\ &\quad = F_A(y \otimes a + \underline{y}) + F_A(z \otimes b + \underline{z}) - F_A(y \otimes a + \underline{y}) - F_A(\underline{z}) - F_A(\underline{y}) - \\ &\qquad - F_A(z \otimes b + \underline{z}) + F_A(\underline{y}) + F_A(\underline{z}) = 0. \end{aligned}$$

Conversely, let Y, Z be orthogonal. We must prove that $F_A(\underline{y}+\underline{z}) = F_A(\underline{y}) + F_A(\underline{z})$ for any $\underline{y} = y_1 \otimes a_1 + \ldots + y_k \otimes a_k \in Y \otimes A$ and $\underline{z} = z_1 \otimes b_1 + \ldots + z_n \otimes b_n \in Z \otimes A$. Applying induction on $k+n$, we compute

$$\begin{aligned} &F_A((y \otimes a + \underline{y}) + (z \otimes b + \underline{z})) \\ &\quad = F_A(y \otimes a + z \otimes b + (\underline{y}+\underline{z})) \\ &\quad = F_A(y \otimes a + \underline{y}+\underline{z}) + F_A(z \otimes b + \underline{y}+\underline{z}) - F_A(\underline{y}+\underline{z}) \\ &\quad = F_A(y \otimes a + \underline{y}) + F_A(\underline{z}) + F_A(\underline{y}) + F_A(z \otimes b + \underline{z}) - F_A(\underline{y}) - F_A(\underline{z}) \\ &\quad = F_A(y \otimes a + \underline{y}) + F_A(z \otimes b + \underline{z}). \end{aligned}$$

This completes the proof.

The orthogonal complement $E^\perp$ of the subset $E \subset X$ is the set of all $x \in X$ which are orthogonal to E. Its fundamental properties are described in the following

LEMMA 2.3.

(1) *$E^\perp$ is a submodule of X,*

(2) $E^\perp = R(E)^\perp$,

(3) $E_1 \subset E_2 \Rightarrow E_1^\perp \supset E_2^\perp$,

(4) $E \subset E^{\perp\perp}$, $E^\perp = E^{\perp\perp\perp}$,

(5) $(\bigcup E_i)^\perp = \bigcap E_i^\perp$.

Proof. It suffices to prove only (1). Let $x_1, x_2 \in E^\perp$ and let $r_1, r_2 \in R$. Then for any $e \in E$, $a, b \in A$, and $\underline{x} \in X \otimes A$

$$\begin{aligned} &F_A((r_1x_1+r_2x_2)\otimes a+e\otimes b+\underline{x}) \\ &= F_A(x_1\otimes r_1a+x_2\otimes r_2a+e\otimes b+\underline{x}) \\ &= F_A(x_1\otimes r_1a+x_2\otimes r_2a+\underline{x})+F_A(x_2\otimes r_2a+e\otimes b+\underline{x})-F_A(x_2\otimes r_2a+\underline{x}) \\ &= F_A((r_1x_1+r_2x_2)\otimes a+\underline{x})+F_A(e\otimes b+\underline{x})-F_A(\underline{x}). \end{aligned}$$

Hence $r_1x_1+r_2x_2 \in E^\perp$.

Here is an application. The fundamental property of non-singular quadratic forms is the following: if $f\colon (X, F) \to (Y, G)$ in $R\text{-Mod}_R^2$ and (X, F) is non-singular, then f is injective and $Y = f(X) \perp f(X)^\perp$. (For the proof see [1].) The following proposition shows that there are no forms of degree $m \geqslant 3$ satisfying an analogous property.

PROPOSITION 2.4. *Let $(X, F) \in \operatorname{Ob} R\text{-Mod}_M^m$ where $m \geqslant 3$ and $\operatorname{Hom}_R(X, M) \neq 0$. Then there exists an injection $(X, F) \subset\!\to (Y, G)$ such that X is a direct but not an orthogonal summand of Y.*

Proof. Let $e_2, \ldots, e_m$ form a basis of R^{m-1} and let $Y = X \oplus R^{m-1}$. Write

$$f_1\colon Y \xrightarrow{p} X \xrightarrow{f} M \quad \text{where} \quad 0 \neq f \in \operatorname{Hom}_R(X, M) \text{ and } p \text{ is the projection},$$

$$f_i = \text{the projection } Y \to Re_i \approx R, \quad i = 2, \ldots, m,$$

$$G = (F \perp 0)+f_1 \ldots f_m = (F \perp 0)+(f_1\otimes .) \ldots (f_m\otimes .).$$

Observe that $(X, F) \subset\!\to (Y, G)$ in $R\text{-Mod}_M^m$. Suppose that X is an orthogonal summand of Y. Then $e_2 \in X+X^\perp$ and hence $x'+e_2 \in X^\perp$ for some $x' \in X$. This means that

$$\begin{aligned} &G_{E(R)}(x\otimes T_1+(x'+e_2)\otimes T_2+\underline{y}) \\ &\qquad = G_{E(R)}(x\otimes T_1+\underline{y})+G_{E(R)}((x'+e_2)\otimes T_2+\underline{y})-G_{E(R)}(\underline{y}) \end{aligned}$$

for any $x \in X$ and any $\underline{y} \in E(Y)$. Putting $\underline{y} = e_3\otimes T_3+\ldots+e_m\otimes T_m$, we obtain

$$\begin{aligned} &F_{E(R)}(x\otimes T_1+x'\otimes T_2)+(f(x)\otimes T_1+f(x')\otimes T_2)(1\otimes T_2) \ldots (1\otimes T_m) \\ &= F_{E(R)}(x\otimes T_1)+(f(x)\otimes T_1)(0\otimes T_2)(1\otimes T_3) \ldots (1\otimes T_m)+F_{E(R)}(x'\otimes T_2) \\ &\quad +(f(x')\otimes T_2)(1\otimes T_2) \ldots (1\otimes T_m) \end{aligned}$$

and hence

$$F_{E(R)}(x\otimes T_1+x'\otimes T_2)+f(x)\otimes T_1 \ldots T_m = F_{E(R)}(x\otimes T_1)+F_{E(R)}(x'\otimes T_2).$$

Since $m \geqslant 3$, it follows that $f(x) = 0$ for any $x \in X$. This contradiction completes the proof.

3. The operations rad **and** ker. Let $(X, F) \in \operatorname{Ob} R\text{-Mod}_M^m$. The submodule $\operatorname{rad}(X) = X^\perp$ is called the *radical* of X.

LEMMA 3.1. *The following conditions are equivalent*:

(1) $x \in \operatorname{rad}(X)$,

(2) $F_A(x\otimes a+\underline{x}) = F_A(x\otimes a)+F_A(\underline{x})$ *for any R-algebra A, $a \in A$, $\underline{x} \in X \otimes A$,*

(3) $F_{E(R)}(x\otimes T_1+\underline{x}) = F_{E(R)}(x\otimes T_1)+F_{E(R)}(\underline{x})$ *where* $\underline{x} = x_2\otimes T_2+\ldots+x_n\otimes T_n \in E(X)$,

(4) $F_{m_1,\ldots,m_n}(x, X, \ldots, X) = 0$ *if $n \geqslant 2$ and $m_1, m_2 > 0$.*

Proof. The implications (2)⇒(3)⇒(4)⇒(1) are evident.

(1)⇒(2) Let $\underline{x} = x_1\otimes a_1+\ldots+x_n\otimes a_n = x_1\otimes a_1+\underline{y}$. Then by induction on n we get

$$\begin{aligned} F_A(x\otimes a+\underline{x}) &= F_A(x\otimes a+x_1\otimes a_1+\underline{y}) = F_A(x\otimes a+\underline{y})+F_A(x_1\otimes a_1+\underline{y})-F_A(\underline{y}) \\ &= F_A(x\otimes a)+F_A(\underline{y})+F_A(\underline{x})-F_A(\underline{y}) = F_A(x\otimes a)+F_A(\underline{x}). \end{aligned}$$

Write $K(X) = \{x \in X \mid F_R(x) = 0\}$ and $\ker(X) = \operatorname{rad}(X) \cap K(X)$.

LEMMA 3.2. *The following conditions are equivalent*:

(1) $x \in \ker(X)$,

(2) $F_A(x\otimes a+\underline{x}) = F_A(\underline{x})$ *for any R-algebra A, $a \in A$, $\underline{x} \in X \otimes A$,*

(3) $F_{E(R)}(x\otimes T_1+\underline{x}) = F_{E(R)}(\underline{x})$ *where $\underline{x} = x_2\otimes T_2+\ldots+x_n\otimes T_n \in E(X)$,*

(4) $F_{m_1,\ldots,m_n}(x, X, \ldots, X) = 0$ *if $n \geqslant 1$ and $m_1 > 0$.*

Proof. Observe that $F_R = F_m$ and $F_A(x\otimes a) = F_R(x)\otimes a^m$. Hence (4)⇒(1)⇒(2)⇒(3) are evident. (3)⇒(4) follows from Formula (1.1).

$\operatorname{Ker}(X)$ is called the *kernel* of X. It is a submodule of X by (2) and is characterized by the following

LEMMA 3.3. *Let Y be a submodule of X and let $f\colon X \to X/Y$ be the natural homomorphism. Then the following conditions are equivalent*:

(1) $Y \subset \ker(X)$,

(2) *there exists a form $\overline{F}$ (evidently unique) of degree m on $(X/Y, M)$ such that $f\colon (X, F) \to (X/Y, \overline{F})$ in $R\text{-Mod}_M^m$.*

Moreover, $\operatorname{rad}(X/Y) = \operatorname{rad}(X)/Y$ *and* $\ker(X/Y) = \ker(X)/Y$. *In particular,* $\ker(X/\ker(X)) = 0$.

Proof. The exact sequence $0 \to Y \subset \xrightarrow{i} X \xrightarrow{f} X/Y \to 0$ induces the following diagram:

$$X \oplus Y \underset{(1,0)}{\overset{(1,i)}{\rightrightarrows}} X \xrightarrow{f} X/Y. \tag{3.1}$$

It is easy to see that f is surjective, and, for any $x_1, x_2 \in X$, $f(x_1) = f(x_2)$ iff there exists an element $(x, y) \in X \oplus Y$ such that $(1, i)(x, y) = x_1$ and $(1, 0)(x, y) = x_2$. This means that (3.1) is an exact sequence in the sense of Grothendieck (see [6], p. 278). Then Theorem IV.4 [6] implies that (2) is equivalent to the condition $F \circ (1, i) = F \circ (1, 0)$, which means that $F_A(\underline{x}+\underline{y}) = F_A(\underline{x})$ for any R-algebra A, any $\underline{y}$ in the image of $Y \otimes A$ in $X \otimes A$, and $\underline{x} \in X \otimes A$. This is equivalent to (1). The last part of our lemma is evident.

Let $(X, F) \in \operatorname{Ob} R\text{-Mod}_M^m$. For any submodule $Y \subset X$ we have defined $Y^\perp \subset X$. On the other hand, we have $(Y, F|_Y^*) \in \operatorname{Ob} R\text{-Mod}_M^m$ and $\operatorname{rad}(Y)$, $\ker(Y) \subset Y$.

Lemma 3.4. *If Y is a submodule of X, then* $Y^\perp \cap Y \subset \operatorname{rad}(Y)$. *Moreover, if* $X = Y \perp Z$ *then*

$$\operatorname{rad}(Y) = Y^\perp \cap Y = \operatorname{rad}(X) \cap Y, \tag{1}$$

$$Y^\perp = \operatorname{rad}(Y) \perp Z, \tag{2}$$

$$\operatorname{rad}(X) = \operatorname{rad}(Y) \perp \operatorname{rad}(Z). \tag{3}$$

Proof. The formula $Y^\perp \cap Y \subset \operatorname{rad}(Y)$ follows immediately from Lemma 2.1 (3). Let $X = Y \perp Z$.

(1) Evidently $\operatorname{rad}(Y) \supset Y^\perp \cap Y \supset \operatorname{rad}(X) \cap Y$. Let $y \in \operatorname{rad}(Y)$. Then

$$F_A(y \otimes a + (\underline{y}+\underline{z})) = F_A(y \otimes a + \underline{y}) + F_A(\underline{z}) = F_A(y \otimes a) + F_A(\underline{y}) + F_A(\underline{z}) = F_A(y \otimes a) + F_A(\underline{y}+\underline{z})$$

for any $a \in A$, $\underline{y} \in Y \otimes A$, $\underline{z} \in Z \otimes A$. Hence $y \in \operatorname{rad}(X) \cap Y$.

(2) Evidently $Y^\perp \supset \operatorname{rad}(Y) \perp Z$. Let $x \in Y^\perp$. Then $x = y+z$ where $y \in Y$ and $z \in Z \subset Y^\perp$. Hence $y \in Y \cap Y^\perp = \operatorname{rad}(Y)$.

(3) $\operatorname{rad}(X) = (Y+Z)^\perp = Y^\perp \cap Z^\perp = \operatorname{rad}(Y) \perp \operatorname{rad}(Z)$ by (2).

Lemma 3.5. *If $X = Y \perp Z$ then* $\ker(Y) = \ker(X) \cap Y$. *Moreover, if* $\operatorname{rad}(Y) = \ker(Y)$, *then* $\ker(X) = \ker(Y) \perp \ker(Z)$.

Proof. The first formula follows from Lemma 3.4. By the same lemma $\operatorname{rad}(X) = \operatorname{rad}(Y) \perp \operatorname{rad}(Z)$. Let $x = y+z$ where $y \in \operatorname{rad}(Y)$ and $z \in \operatorname{rad}(Z)$. If $\operatorname{rad}(Y) = \ker(Y)$ then $F_R(x) = F_R(y) + F_R(z) = F_R(z)$. Hence $x \in \ker(X)$ iff $z \in \ker(Z)$.

Lemma 3.6.

$$\operatorname{rad} \circ \operatorname{rad} = \operatorname{rad}, \quad \ker \circ \ker = \ker \circ \operatorname{rad} = \operatorname{rad} \circ \ker = \ker.$$

Proof.

$$\operatorname{rad}(X) = \operatorname{rad}(X) \cap (\operatorname{rad}(X))^\perp \subset \operatorname{rad}(\operatorname{rad}(X)) \subset \operatorname{rad}(X),$$

$$\ker(X) = \ker(X) \cap (\ker(X))^\perp \subset \operatorname{rad}(\ker(X)) \subset \ker(X),$$

$$\ker(\operatorname{rad}(X)) = \operatorname{rad}(\operatorname{rad}(X)) \cap K(\operatorname{rad}(X)) = \operatorname{rad}(X) \cap K(X) = \ker(X),$$

$$\ker(\ker(X)) = \operatorname{rad}(\ker(X)) \cap K(\ker(X)) = \ker(X) \cap K(X) = \ker(X).$$

It is well known that in the case of $m = 2$ we have $Y^\perp \cap Y = \operatorname{rad}(Y)$ for any submodule $Y \subset X$. For $m \geqslant 3$ it is false in general.

Example 3.7. Let $X = R^2 = Re \oplus Re'$, $Y = Re$, $M = R$, $F = T_1^{m-1}T_2$, $m \geqslant 3$, $(m-1) \notin D(R)$. Since $F|_Y = 0$, it follows that $\operatorname{rad}(Y) = Y$. On the other hand, if $re \in Y^\perp \cap Y$ then

$$F_{E(R)}(re \otimes T_1 + e \otimes T_2 + e' \otimes T_3) = F_{E(R)}(re \otimes T_1 + e' \otimes T_3) + F_{E(R)}(e \otimes T_2 + e' \otimes T_3) - F_{E(R)}(e' \otimes T_3),$$

i.e., $(rT_1+T_2)^{m-1}T_3 = (rT_1)^{m-1}T_3 + T_2^{m-1}T_3$. Hence $(m-1)r = 0$, $re = 0$. This means that $Y^\perp \cap Y = 0$.

Let $(X, F) \in \operatorname{Ob} R\text{-Mod}_M^m$. The module X (the form F) is called

(a) *non-degenerate* iff $\operatorname{rad}(X) = 0$,

(b) *totally isotropic* iff $\operatorname{rad}(X) = X$,

(c) *totally singular* iff $\ker(X) = X$ (i.e. iff $F = 0$),

(d) *anisotropic* iff $K(X) = 0$.

(Compare also [2] and [5] in the case of $m = 2$.) From the above lemmas follows

Corollary 3.8.

(1) *If $X = Y \perp Z$, then X is non-degenerate (totally isotropic, totally singular) iff Y and Z are non-degenerate (totally isotropic, totally singular, respectively).*

(2) *If $X = Y \perp Z$ and Y is non-degenerate then $Y^\perp = Z$.*

(3) *If $Y \subset X$ and $Y \subset Y^\perp$ then Y is totally isotropic.*

(4) $\operatorname{rad}(X)$ *is totally isotropic and* $\ker(X)$ *is totally singular.*

It is clear that any $(X, F) \in \operatorname{Ob} R\text{-Mod}_M^1$ is totally isotropic. Hence in general $\ker(X) \neq \operatorname{rad}(X)$. For $m \geqslant 2$ we prove

Proposition 3.9. *Let $m \geqslant 2$ and let M be an R-module. If*

(1) *m is not the power of a prime or*

(2) *$m = p^n$ and $p \notin D(M)$, for some prime p,*

then $\ker(X) = \mathrm{rad}(X)$ *for any* $(X, F) \in \mathrm{Ob}\,R\text{-Mod}_M^m$. *In particular,* F *is totally isotropic iff it is totally singular.*

Proof. Let $(X, F) \in \mathrm{Ob}\,R\text{-Mod}_M^m$ and let $x \in \mathrm{rad}(X)$. Then

$$F_{E(R)}(x\otimes T_1 + x\otimes T_2) = E_{E(R)}(x\otimes T_1) + F_{E(R)}(x\otimes T_2),$$

$$F_R(x)\otimes(T_1+T_2)^m = F_R(x)\otimes T_1^m + F_R(x)\otimes T_2^m,$$

$$\binom{m}{i} F_R(x) = 0 \quad \text{for} \quad 0<i<m.$$

Hence $x \in \ker(X)$ by Lemma 0.1.

If $m = p^n$ and $p \in D(M)$, then there exist non-zero totally isotropic forms in $R\text{-Mod}_M^m$. They are described in

PROPOSITION 3.10. *Suppose that* $(X, F) \in \mathrm{Ob}\,R\text{-Mod}_M^m$ *where* $m = p^n \geqslant 2$ *and* X *is a free* R*-module of rank* N. *Then the following conditions are equivalent*:

(1) F *is totally isotropic,*

(2) *for any basis* $\{e_1, \ldots, e_N\}$ *of* X, F *has the form*

$$F = a_1\otimes T_1^m + \ldots + a_N\otimes T_N^m, \quad pa_j = 0, \quad j = 1, \ldots, N,$$

(3) F *has the above form for some basis of* X.

Proof. (1)⇒(2) Let $\{e_1, \ldots, e_N\}$ be a basis of X. Since F is totally isotropic, it follows that

$$F_{E(R)}(e_1\otimes T_1 + \ldots + e_N\otimes T_N) = F_R(e_1)\otimes T_1^m + \ldots + F_R(e_N)\otimes T_N^m.$$

Moreover, the above proof shows that $pF_R(x) = 0$ for any $x \in X$.

(3)⇒(1) Let $F = a_1\otimes T_1^m + \ldots + a_N\otimes T_N^m$ and $pa_j = 0$, for some basis $\{e_1, \ldots, e_N\}$ of X. Let $x_1, \ldots, x_n \in X$, $x_i = \sum_j r_{ij}e_j$. Then

$$F_{E(R)}(x_1\otimes T_1 + \ldots + x_n\otimes T_n) = F_{E(R)}\Big(\sum_j e_j\otimes\Big(\sum_i r_{ij}T_i\Big)\Big)$$

$$= \sum_j a_j\otimes\Big(\sum_i r_{ij}T_i\Big)^m = \sum_j a_j\otimes\Big(\sum_i r_{ij}^m T_i^m\Big)$$

since $\binom{m}{k} a_j = 0$ for $0<k<m$. Hence

$$F_{E(R)}(x_1\otimes T_1 + \ldots + x_n\otimes T_n) = F_{E(R)}(x_1\otimes T_1) + F_{E(R)}(x_2\otimes T_2 + \ldots + x_n\otimes T_n)$$

and therefore F is totally isotropic.

4. The canonical decomposition. In this section we give some generalization of the "radical splitting" (see for example [4], [5]).

PROPOSITION 4.1. *If* $(X, F) \in \mathrm{Ob}\,R\text{-Mod}_M^m$, *then the following conditions are equivalent*:

(1) $\mathrm{rad}(X)$ *is a direct summand of* X,

(2) *there exists an orthogonal decomposition* $X = Y \perp Z$ *such that* Y *is non-degenerate and* Z *is totally isotropic.*

Moreover, $Z = \mathrm{rad}(X)$ *for any decomposition in* (2).

Proof. If $X = Y\oplus\mathrm{rad}(X)$, then evidently $X = Y \perp \mathrm{rad}(X)$. Moreover, $\mathrm{rad}(X)$ is totally isotropic, and $\mathrm{rad}(Y) = \mathrm{rad}(X) \cap Y = 0$. Conversely, suppose that $X = Y \perp Z$, Y is non-degenerate, and Z is totally isotropic. Then $\mathrm{rad}(X) = \mathrm{rad}(Y) \perp \mathrm{rad}(Z) = Z$. Hence $\mathrm{rad}(X)$ is a direct summand of X.

PROPOSITION 4.2. *If* $(X, F) \in \mathrm{Ob}\,R\text{-Mod}_M^m$, *then the following conditions are equivalent*:

(1) $\ker(X)$ *is a direct summand of* X,

(2) *there exists an orthogonal decomposition* $X = Y \perp Z$ *such that* $\ker(Y) = 0$ *and* Z *is totally singular.*

Moreover, for any decomposition in (2), $Z = \ker(X)$, *and* Y *is uniquely determined up to an isometry. More precisely,* $(Y, F|_Y) \approx (X/\ker(X), \bar{F})$ *in* $R\text{-Mod}_M^m$.

Proof. If $X = Y\oplus\ker(X)$, then evidently $X = Y \perp \ker(X)$. Moreover, $\ker(X)$ is totally singular, and $\ker(Y) = \ker(X) \cap Y = 0$. Conversely, let $X = Y \perp Z$, $\ker(Y) = 0$, $\ker(Z) = Z$. Since $\ker(Z) = \mathrm{rad}(Z)$, it follows that $\ker(X) = \ker(Y) \perp \ker(Z) = Z$. In particular, $\ker(X)$ is a direct summand of X. Moreover, the natural homomorphism $f\colon X \to X/\ker(X)$ induces the isomorphism $f'\colon Y \to X/\ker(X)$. Lemma 3.3 shows that $f'\colon (Y, F|_Y) \xrightarrow{\approx} (X/\ker(X), \bar{F})$ in $R\text{-Mod}_M^m$.

Observe that the above two propositions describe the same decomposition in the case where the assumption of Proposition 3.9 is satisfied. Then this decomposition is unique up to an isometry. However, if $m = p^n \geqslant 2$ and $p \in D(M)$, then the decomposition in Proposition 4.1 is, in general, not unique. This follows from.

EXAMPLE 4.3. Let $m = p^n \geqslant 2$ and let R be a field of characteristic p ($R = \boldsymbol{Z}_2$ in the case of $m = 2$). Let $(X, F) = (Y, G) \perp (Z, H)$ where $Y = Re_1\oplus\ldots\oplus Re_m$, $Z = Re_{m+1}$, $G = T_1 \ldots T_m$, $H = T_{m+1}^m$. Then $X = Re_1\oplus\ldots\oplus Re_{m+1}$ and $F = T_1 \ldots T_m + T_{m+1}^m$. Observe that G is non-degenerate by Corollary 5.2 and H is totally isotropic by Proposition 3.10. Hence $X = Y \perp Z$ is the decomposition from Proposition 4.1. In particular, $Z = \mathrm{rad}(X)$.

Let $e_i' = e_i + e_{m+1}$, $i = 1, \ldots, m$, $e_{m+1}' = e_{m+1}$. Then

$$F_{E(R)}(e_1'\otimes T_1 + \ldots + e_{m+1}'\otimes T_{m+1})$$

$$= F_{E(R)}(e_1\otimes T_1 + \ldots + e_m\otimes T_m + e_{m+1}\otimes(T_1 + \ldots + T_{m+1}))$$

$$= T_1 \ldots T_m + (T_1 + \ldots + T_{m+1})^m = (T_1 \ldots T_m + T_1^m + \ldots + T_m^m) + T_{m+1}^m.$$

Let $Y' = Re'_1 \oplus \ldots \oplus Re'_m$. Then $X = Y' \perp Z$ where $Z = \operatorname{rad}(X)$, and hence it is the decomposition from Proposition 4.1. Moreover, $G' = F|_{Y'} = T_1 \ldots T_m + T_1^m + \ldots + T_m^m$ in the basis $\{e'_1, \ldots, e'_m\}$. We prove that G and G' are not isomorphic. It suffices to show that G' is not a product of linear forms. Suppose that $G' = (T_1 - a_2 T_2 - \ldots - a_m T_m) G''$. Putting $T_1 = S_1 + a_2 S_2 + \ldots + a_m S_m$ and $T_i = S_i$ for $i \geqslant 2$, we obtain

$$S_1|G' = S_1 \ldots S_m + S_1^m + \sum_{i=2}^{m} a_i S_2 \ldots S_i^2 \ldots S_m + \sum_{i=2}^{m} (a_i^m + 1) S_i^m .$$

If $m > 2$ then $a_i = 0$ and $a_i^m + 1 = 0$ for $i = 2, \ldots, m$ — a contradiction. For $m = 2$ we have $S_1|S_1 S_2 + S_1^2 + (a_2^2 + a_2 + 1) S_2^2$, and hence $a_2^2 + a_2 + 1 = 0$. This is impossible in Z_2.

Now we begin the proof that the above decompositions exist over Prüfer rings. We first prove

LEMMA 4.4. *Suppose that $(X, F) \in \operatorname{Ob} R\text{-Mod}_M^m$, R is an integral domain, and M is a torsion-free R-module. Then $X/\operatorname{rad}(X)$ and $X/\ker(X)$ are also torsion-free.*

Proof. Let $r\bar{x} = 0$ in $X/\operatorname{rad}(X)$ and $0 \neq r \in R$. Then $rx \in \operatorname{rad}(X)$ and hence

$$r^m F_{E(R)}(x \otimes a + \underline{x}) = F_{E(R)}(rx \otimes a + r\underline{x}) = F_{E(R)}(rx \otimes a) + F_{E(R)}(r\underline{x})$$
$$= r^m \left(F_{E(R)}(x \otimes a) + F_{E(R)}(\underline{x})\right)$$

for any $a \in E(R)$ and $\underline{x} \in E(X)$. Since $E(M)$ is torsion-free, it follows that $x \in \operatorname{rad}(X)$, i.e., $\bar{x} = 0$. The proof of the second part is similar.

It is known that R is a Prüfer ring iff R is an integral domain and any finitely generated torsion-free R-module is projective (see for example [3], Ch. VII, Proposition 4.1). Hence we obtain

COROLLARY 4.5. *Suppose that $(X, F) \in \operatorname{Ob} R\text{-Mod}_M^m$, R is a Prüfer ring, M is a torsion-free R-module, and X is a finitely generated R-module. Then*

(1) *$\operatorname{rad}(X)$ and $\ker(X)$ are direct summands of X,*

(2) *if $\ker(X) = 0$ then X is projective.*

From the above facts immediately follows

THEOREM 4.6. *Suppose that $(X, F) \in \operatorname{Ob} R\text{-Mod}_M^m$, R is a Prüfer ring, M is a torsion-free R-module, and X is a finitely generated R-module. (The last assumption can be omitted if R is a field.) Then there exists an orthogonal decomposition $X = X_1 \perp X_2 \perp X_3$ such that*

(1) *X_1 is non-degenerate,*

(2) *X_2 is totally isotropic and anisotropic,*

(3) *X_3 is totally singular.*

Any such decomposition has the following properties:

(a) *X_1 and X_2 are projective.*

(b) *$X_2 \perp X_3 = \operatorname{rad}(X)$ and $X_3 = \ker(X)$.*

(c) *$X_1 \perp X_2$ and X_2 are uniquely determined up to an isometry.*

(d) *If m is not a power of a prime or $m = p^n \geqslant 2$ and $\operatorname{char}(R) \neq p$, then $X_2 = 0$.*

In this case, the above decomposition is unique up to an isometry.

5. Construction of indecomposable forms. Multiplication gives us some examples of indecomposable forms. Namely

THEOREM 5.1. *Suppose that $D(R) = D(M) = 0$, $X \neq 0$, $m, k > 0$, $(X, G) \in \operatorname{Ob} R\text{-Mod}_M^m$, $(R, H) \in \operatorname{Ob} R\text{-Mod}_R^k$, $\ker(G) = 0$, $\ker(H) = 0$. Define $(Y, F) \in \operatorname{Ob} R\text{-Mod}_M^{m+k}$ as follows: $Y = X \oplus R$, $F = (G \perp 0) \cdot (0 \perp H)$. Then F is non-degenerate. Moreover, if one of the following conditions is satisfied:*

(i) *G is non-degenerate,*

(ii) *$m > k$,*

(iii) *$m > 1$ and $k \neq 0$ in R,*

then F is indecomposable.

Proof. Observe that $D(X) = 0$ by Lemma 4.4. Moreover, $H_A(a) = ra^k$ where $r \neq 0$, and hence $F_A(\underline{x} + a) = G_A(\underline{x}) ra^k$. Since $D(E(M)) = 0$, it suffices to put $r = 1$.

(1) Let $x_1 + r_1$ and $x_2 + r_2$ be orthogonal in (Y, F). We prove that x_1, x_2 are orthogonal in (X, G) and $r_1 x_2 + r_2 x_1 = 0$. Observe that

$$G_A(x_1 \otimes a_1 + x_2 \otimes a_2 + \underline{x})(r_1 a_1 + r_2 a_2 + a)^k$$
$$= G_A(x_1 \otimes a_1 + \underline{x})(r_1 a_1 + a)^k + G_A(x_2 \otimes a_2 + \underline{x})(r_2 a_2 + a)^k - G_A(\underline{x}) a^k \tag{5.1}$$

for any $a_1, a_2, a \in A$, $\underline{x} \in X \otimes A$. Put $A = E(R)$, $a_1 = T_1$, $a_2 = T_2$, $\underline{x} = x_3 \otimes T_3 + \ldots + x_n \otimes T_n$, $a = T_{n+1}$. Comparing the coefficients at T_{n+1}^k, we obtain

$$G_{E(R)}(x_1 \otimes T_1 + x_2 \otimes T_2 + \underline{x}) = G_{E(R)}(x_1 \otimes T_1 + \underline{x}) + G_{E(R)}(x_2 \otimes T_2 + \underline{x}) - G_{E(R)}(\underline{x}) .$$

This means that x_1, x_2 are orthogonal in (X, G).

Now we prove that $r_1 x_2 + r_2 x_1 = 0$. Suppose that $r_1, r_2 \neq 0$. Let $A = E(R)$, $a_1 = r_2 T_1$, $a_2 = r_1 T_1$, $a = -r_1 r_2 T_1$, and $\underline{x} = x_3 \otimes T_3 + \ldots + x_n \otimes T_n$ in (5.1). Then we obtain

$$G_{E(R)}((r_1 x_2 + r_2 x_1) \otimes T_1 + \underline{x})(r_1 r_2 T_1)^k = -G_{E(R)}(\underline{x})(-r_1 r_2 T_1)^k .$$

Since $D(E(M)) = 0$, it follows that

$$G_{E(R)}((r_1 x_2 + r_2 x_1) \otimes T_1 + \underline{x}) = (-1)^{k+1} G_{E(R)}(\underline{x}) . \tag{5.2}$$

Suppose that k is even. Applying the endomorphism $u: E(R) \to E(R)$ which carries T_1 in 0, and T_i in T_i for $i > 1$, we obtain $G_{E(R)}(\underline{x}) = -G_{E(R)}(\underline{x})$. Hence for any k, (5.2) shows that $r_1 x_2 + r_2 x_1 \in \ker(G) = 0$.

Suppose that $r_1 = 0$ and $r_2 \neq 0$. Let $A = E(R)$, $a_1 = T_1$, $a_2 = -T_2$, and $a = r_2 T_2$. Then (5.1) shows that

$$G_{E(R)}(x_1 \otimes T_1 + \underline{x})(r_2 T_2)^k = G_{E(R)}(\underline{x})(r_2 T_2)^k .$$

Since $D(E(M)) = 0$, it follows that $x_1 \in \ker(G) = 0$. In particular $r_1 x_2 + r_2 x_1 = 0$.

(2) If $x+r \in \operatorname{rad}(F)$, then $Rx = 0 = rX$ by (1) and hence $x+r = 0$. This means that F is non-degenerate.

(3) Suppose that $Y = V_1 \perp V_2$ where $V_1, V_2 \neq 0$. It follows from (1) that $V_1, V_2 \not\subset X, R$. Hence there exist $x_i + r_i \in V_i$, $i = 1, 2$, such that $x_i, r_i \neq 0$. Let $x \in X$ and $x = y+z$ where $y+r \in V_1$ and $z+s \in V_2$. It follows from (1) that $r_1 x_2 = -r_2 x_1$ is orthogonal to y and z. Hence $x_1, x_2 \in \operatorname{rad}(G)$ by Lemma 4.4. This is impossible if G is non-degenerate. Put $A = E(R)$, $a_1 = T_1$, $a_2 = T_2$, $a = 0$, and $\underline{x} = 0$ in (5.1). Since x_1, x_2 are orthogonal, it follows that

$$\begin{aligned}(G_{E(R)}(x_1 \otimes T_1) + G_{E(R)}(x_2 \otimes T_2))(r_1 T_1 + r_2 T_2)^k \\ = G_{E(R)}(x_1 \otimes T_1)(r_1 T_1)^k + G_{E(R)}(x_2 \otimes T_2)(r_2 T_2)^k .\end{aligned}$$

This means that

$$G_R(x_1) \otimes T_1^m((r_1 T_1 + r_2 T_2)^k - (r_1 T_1)^k) + G_R(x_2) \otimes T_2^m((r_1 T_1 + r_2 T_2)^k - (r_2 T_2)^k) = 0.$$

Let $m > k$. Comparing the coefficients at $T_1^m T_2^k$ and at $T_1^k T_2^m$, we obtain $r_2^k G_R(x_1) = r_1^k G_R(x_2) = 0$. Hence $x_1, x_2 \in \ker(G) = 0$, but this is impossible.

Let now $m > 1$. Comparing the coefficients at $T_1^{m+k-1} T_2$ and at $T_1 T_2^{m+k-1}$, we obtain $k r_1^{k-1} r_2 G_R(x_1) = k r_1 r_2^{k-1} G_R(x_2) = 0$. If $k \neq 0$ in R, then $x_1, x_2 \in \ker(G) = 0$, and this is also impossible. This completes the proof.

COROLLARY 5.2. *Let $D(R) = D(M) = 0$, $N \geqslant 2$, $m \geqslant 3$. Then there exists a non-degenerate indecomposable form of degree m on (R^N, M).*

Proof. Since $R \subset\!\!\to M$, we can assume that $M = R$. Define the form $F_{m,N}$ of degree $m \geqslant 2$ in $R[T_1, \ldots, T_N]$ in the following way:

(a) $F_{2,2n} = T_1 T_2 + \ldots + T_{2n-1} T_{2n}$, $F_{2,2n+1} = F_{2,2n} + T_{2n+1}^2$, $F_{m,1} = T_1^m$;

(b) $F_{m+1,N+1} = F_{m,N} T_{N+1}$.

Observe that $K(T_1^m) = 0$ and hence $\ker(F_{m,1}) = 0$. Moreover, $T_1 T_2$ is non-degenerate and hence $\ker(F_{2,N}) = 0$ by Lemma 3.4 and 3.5. It follows from Theorem 5.1 that $F_{m,N}$ are non-degenerate and indecomposable for any $m \geqslant 3$ and $N \geqslant 2$.

Consider monomials $T_1^{m_1} \ldots T_N^{m_N} \in R[T_1, \ldots, T_N]$ where $m_1, \ldots, m_N > 0$. 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 evidently orthogonal. Hence we can assume that R is connected.

PROPOSITION 5.3. *If R is connected, then the only decomposable monomials are*

(1) *$T_1 T_2$ if 2 is invertible in R,*

(2) *$T_1^{p^n} T_2^{p^n}$, where $p \neq 2$ is a prime, if R is a Z_p-algebra.*

Proof. Observe that the above forms are decomposable. In fact, the invertible change of variables $T_1 = S_1 + S_2$, $T_2 = S_1 - S_2$ gives us

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

Conversely, let $F = T_1^{m_1} \ldots T_N^{m_N} \in R[T_1, \ldots, T_N]$, where $m_i > 0$, be decomposable. Since R is connected, it follows that F is decomposable over all R-algebras. We first prove that $F = T_1^m T_2^m$ where $m = p^n$, p is a prime, and $n \geqslant 0$. Accordingly we consider F over some quotient field of R.

Since $\ker(T_i^{m_i}) = 0$, it follows from Theorem 5.1 that $T_1^{m_1} T_2^{m_2}$ is non-degenerate and $T_1^{m_1} \ldots T_N^{m_N}$ is indecomposable for $N \geqslant 3$. Moreover, $T_1^{m_1} T_2^{m_2}$ is indecomposable if $m_1 \neq m_2$. Hence $F = T_1^m T_2^m$. Let $m = p_1^{i_1} \ldots p_s^{i_s}$ be the canonical decomposition of m in Z. If $s > 1$, then $\operatorname{rad}(T_1^m) = \ker(T_1^m) = 0$ by Proposition 3.9, and hence $T_1^m T_2^m$ is indecomposable by Theorem 5.1. Therefore $m = p^n$.

Let $F = T_1^m T_2^m$, $m = p^n$, and $n > 0$ (the case $m = 1$ is well-known). It follows from Theorem 5.1 that $p = 0$ in R/I for any $I \in \operatorname{Spec}(R)$, and hence p is nilpotent in R. Suppose that $p = 2$. We can assume that R is a field. Then $2m = 2^{n+1}$, $2 = 0$ in R, and F is diagonal. Hence F is totally isotropic by Proposition 3.10. On the other hand, F is non-degenerate by Theorem 5.1. This contradiction shows that $p \neq 2$.

Suppose that $p \neq 0$ in R. Since p is nilpotent in R, it follows that $p \neq 0$ in $R/(p^2)$. Hence we can assume that $p \neq 0$ in R, $p^2 = 0$ in R, and, evidently, that R is local. Since F is decomposable it follows that there exists such invertible change of variables $T_1 = rS_1 + sS_2$, $T_2 = tS_1 + uS_2$, that

$$\begin{aligned}(5.3)\qquad T_1^m T_2^m &= (rS_1+sS_2)^m(tS_1+uS_2)^m = (rtS_1^2 + suS_2^2 + (ru+st)S_1S_2)^m \\ &= (rt)^m S_1^{2m} + (su)^m S_2^{2m} .\end{aligned}$$

Since F is non-degenerate over K, the quotient field of R, it follows that r, s, t, u are invertible in R. Since $p^2 = 0$ in R, it follows from Lemma 0.1 that the coefficient at $(S_1^2)^{m_1}(S_2^2)^{m_2}(S_1S_2)^{m_3}$ in (5.3) is zero if at least one of the m_i's is different from kp^{n-1}. Put $m' = p^{n-1}$ and compare the coefficients at $S_1^{m'} S_2^{2m-m'}$ in (5.3). This gives us

$$\binom{m}{m'}(ru+st)^{m'}(su)^{m-m'} = 0 .$$

Observe that $\binom{m}{m'} = pk$, where $p \nmid k$ and hence k is invertible in R. Since su is also invertible, it follows that

$$p(ru+st)^{m'} = 0.$$

From the above facts we immediately obtain

$$(rt)^m S_1^{2m} + (su)^m S_2^{2m} = (rtS_1^2 + suS_2^2)^m + (ru+st)^m S_1^m S_2^m .$$

Since m is odd, it follows that

$$\binom{m}{i}(rt)^i(su)^{m-i} = 0, \quad 0 < i < m .$$

Moreover, r, s, t, u are invertible in R, and hence $p = 0$ in R by Lemma 0.1. This contradiction shows that R is a Z_p-algebra.

6. The uniqueness of the orthogonal decomposition. Let $(X, F) \in \mathrm{Ob}\, R\text{-Mod}_M^m$. Put $a_i = T_i$ for $i<k$, $a_k = T_k+T_{k+1}$, and $a_i = T_{i+1}$ for $i>k$ in (1.1). This gives us the formula

$$F_{m_1,\dots,m_{k-1},i,j,m_{k+1},m_n}(x_1, \dots, x_k, x_k, \dots, x_n) = \binom{i+j}{i} F_{m_1,\dots,m_{k-1},i+j,m_{k+1},\dots,m_n}(x_1, \dots, x_n).$$

An easy induction shows that

$$PF(\underbrace{x_1, \dots, x_1}_{m_1}, \dots, \underbrace{x_n, \dots, x_n}_{m_n}) = m_1! \dots m_n!\, F_{m_1,\dots,m_n}(x_1, \dots, x_n)$$

for any $m_1, \dots, m_n$. Applying Lemma 2.1, we obtain

COROLLARY 6.1. *Let $(X, F) \in \mathrm{Ob}\, R\text{-Mod}_M^m$, $m \geqslant 2$, and $(m-1)! \notin D(M)$. Then x_1, x_2 are orthogonal in (X, F) iff $PF(x_1, x_2, X, \dots, X) = 0$.*

The following facts show a difference between the cases $m = 2$ and $m \geqslant 3$.

PROPOSITION 6.2. *Let $(X, F) \in \mathrm{Ob}\, R\text{-Mod}_M^m$, $m \geqslant 3$, and $(m-1)! \notin D(M)$. 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 $E \subset X$.*

Proof. Let $x \in E^\perp$ and $e \in E$. Then $x = x_i + y_i$, $e = x' + y'$ where $x_i, x' \in X_i$, $y_i, y' \in Y_i = X_1 \perp \dots \perp \hat{X}_i \perp \dots \perp X_n$. Observe that

$$\begin{aligned} PF(x_i, e, X, \dots, X) &= PF(x_i, x', X_i, \dots, X_i) + PF(0, y', Y_i, \dots, Y_i) \\ &= PF(x_i, x', X_i, \dots, X_i) + PF(y_i, y', 0, \dots, 0) \\ &= PF(x, e, X_i, \dots, X_i) = 0 \end{aligned}$$

since $m \geqslant 3$. Hence $x_i \in E^\perp$ by Corollary 6.1. This completes the proof.

THEOREM 6.3. *Let $(X, F) \in \mathrm{Ob}\, R\text{-Mod}_M^m$, $m \geqslant 3$, $(m-1)! \notin D(M)$, and let F be non-degenerate. Suppose that $X = X_1 \perp \dots \perp X_n$ where $X_i \neq 0$ are indecomposable. Then any orthogonal summand Y of X has the form $Y = X_{i_1} \perp \dots \perp X_{i_s}$, $i_1 < \dots < i_s$.*

Proof. Let $X = Y \perp Z$. It follows from Corollary 3.8 (2) and Proposition 6.2 that $X_i = (Y \cap X_i) \perp (Z \cap X_i)$. Since X_i is indecomposable, it follows that $X_i \subset Y$ or $X_i \subset Z$. For example, let $X_1, \dots, X_s \subset Y$ and $X_{s+1}, \dots, X_n \subset Z$. Then $Y = X_1 \perp \dots \perp X_s$.

COROLLARY 6.4. *Let $(X, F) \in \mathrm{Ob}\, R\text{-Mod}_M^m$, $m \geqslant 3$, $(m-1)! \notin D(M)$, and let F be non-degenerate. Suppose that*

$$X = X_1 \perp \dots \perp X_n = Y_1 \perp \dots \perp Y_k$$

where X_i, $Y_j \neq 0$ are indecomposable. Then $k = n$ and $Y_j = X_{s(j)}$ for some permutation $s \in S_n$.

Observe that the assumption $(m-1)! \notin D(M)$ is necessary. In fact, let R be a field, $\mathrm{char}(R) = p \neq 0, 2$, and $m-1 = p^n$, $n>0$. Then $T_1^m + T_2^m \in R[T_1, T_2]$ is non-degenerate by Proposition 3.9 and Corollary 3.8 (1). Moreover, if $T_1 = S_1 + S_2$ and $T_2 = S_1 - S_2$, then

$$T_1^m + T_2^m = (S_1+S_2)(S_1^{m-1} + S_2^{m-1}) + (S_1-S_2)(S_1^{m-1} - S_2^{m-1}) = 2S_1^m + 2S_2^m.$$

Let us now define a full subcategory $\underline{R\text{-Mod}}_M^m$ of $R\text{-Mod}_M^m$ as follows: $(X, F) \in \mathrm{Ob}\, \underline{R\text{-Mod}}_M^m$ iff X is a finitely generated projective R-module and F is non-degenerate. In the rest of this section we assume that

(1) $m \geqslant 3$ and $(m-1)! \notin D(M)$,

(2) $R = R_1 \times \dots \times R_s$ where R_i are connected rings.

Denote $r(P) = \mathrm{rank}(P_1) + \dots + \mathrm{rank}(P_s)$ for any finitely generated projective R-module $P = P_1 \times \dots \times P_s$. It is easy to see that $r(P \oplus Q) = r(P) + r(Q)$ and $r(P) = 0 \Rightarrow P = 0$. Hence the standard verification shows that any object of $\underline{R\text{-Mod}}_M^m$ can be decomposed into a finite orthogonal sum of indecomposable objects. This decomposition is unique by Corollary 6.4. In particular, we obtain

COROLLARY 6.5. *$\underline{R\text{-Mod}}_M^m$ has the cancellation property:*

$$F \perp G \approx F' \perp G', \quad F \approx F' \Rightarrow G \approx G'.$$

Isomorphism classes of objects in $\underline{R\text{-Mod}}_M^m$ constitute a set, denoted by $\mathscr{F}_M^m$. The indecomposable objects define its subset $(F_w)_{w \in W}$. It is easy to see that

COROLLARY 6.6. *$(\mathscr{F}_M^m, \perp)$ is a commutative free semigroup, and $K_0(\underline{R\text{-Mod}}_M^m, \perp)$ is the free abelian group on the set $(F_w)_{w \in W}$.*

Now we begin the study of the automorphisms in $\underline{R\text{-Mod}}_M^m$. Let $(X, F) \in \mathrm{Ob}\, \underline{R\text{-Mod}}_M^m$. Observe that the permutation group S_n acts on the group $\mathrm{Aut}(F)_n = \mathrm{Aut}(F) \times \dots \times \mathrm{Aut}(F)$ (n-times) in the following way:

$$(f_1, \dots, f_n)^s = (f_{s(1)}, \dots, f_{s(n)}) \quad \text{for} \quad s \in S_n.$$

Hence we can form the semi-simple product $S_n \dot{\times} \mathrm{Aut}(F)_n$. On the other hand, any $s \in S_n$ induces the automorphism

$$\bar{s}\colon (X_1, F) \perp \dots \perp (X_n, F) \to (X_1, F) \perp \dots \perp (X_n, F),$$

where $X_i = X$, defined by $\bar{s}(x_1, \dots, x_n) = (x_{s^{-1}(1)}, \dots, x_{s^{-1}(n)})$. Since $\bar{s}(X_i) = X_{s(i)}$, it follows that the mapping $s \mapsto \bar{s}$ is injective (if, evidently, $X \neq 0$). We prove the following

THEOREM 6.7 *There exists a natural group isomorphism*

$$\times_{w \in W} (S_{n_w} \dot{\times} \mathrm{Aut}(F_w)_{n_w}) \approx \mathrm{Aut}\Big(\perp_{w \in W} n_w F_w\Big)$$

defined by

$$(s_w; f_{w1}, \dots, f_{wn_w})_{w \in W} \mapsto \perp_{w \in W} \bar{s}_w \circ (f_{w1} \perp \dots \perp f_{wn_w}).$$

Proof. Let F_w be defined on X_w and let X_{wi} be copies of X_w. Then $F = \perp n_w F_w$ is defined on $X = \perp (X_{w1} \perp \ldots \perp X_{wn_w})$. Let $f \in \mathrm{Aut}(F)$. Then

$$X = \perp (f(X_{w1}) \perp \ldots \perp f(X_{wn_w}))$$

and hence $f(X_{wi}) = X_{ws_w(i)}$ for the unique system of permutations $s_w \in S_{n_w}$. Write $f_{wi} = f|_{X_{wi}} \in \mathrm{Aut}(F_w)$. It is easy to prove that the mapping

$$\mathrm{Aut}(F) \to \times (S_{n_w} \dot{\times} \mathrm{Aut}(F_w)_{n_w}), \quad f \mapsto (s_w; f_{w1}, \ldots, f_{wn_w})_{w \in W}$$

is a group homomorphism which is inverse to the above. This completes the proof.

The above theorem makes possible the computation of the K_1-group (see [1]) of $\underline{R\text{-Mod}}_M^m$. Write

$$A_w = \mathrm{Aut}(F_w)/[\mathrm{Aut}(F_w), \mathrm{Aut}(F_w)],$$

$$Z_2 = \text{the multiplicative group } \{1, -1\}.$$

THEOREM 6.8. *There exists a unique group isomorphism*

$$K_1(\underline{R\text{-Mod}}_M^m, \perp) \approx \bigoplus_{w \in W} (Z_2 \oplus A_w)$$

which carries $[(F_w, f)]$ *in* $(1, \bar{f}) \in Z_2 \oplus A_w$ *and* $[(F_w \perp F_w, \bar{t})]$ *in* $(-1, \bar{1}) \in Z_2 \oplus A_w$, *where* $1 \neq t \in S_2$.

Proof. Define the group homomorphism u: $\mathrm{Aut}(\perp n_w F_w) \to \bigoplus (Z_2 \oplus A_w)$ in the following way: if $f \in \mathrm{Aut}(\perp n_w F_w)$, then $f = \perp \bar{s}_\omega \circ (f_{w1} \perp \ldots \perp f_{wn_w})$ by Theorem 6.7, and we put

$$u(f) = (\mathrm{sgn}(s_w), \overline{f_{w1}} \ldots \overline{f_{wn_w}})_{w \in W}.$$

Since $\bigoplus (Z_2 \oplus A_w)$ is commutative, it follows that $u(gfg^{-1}) = u(f)$. Hence for any $(X, F) \in \mathrm{Ob}\,\underline{R\text{-Mod}}_M^m$ we obtain a properly defined homomorphism

$$u(F)\colon \mathrm{Aut}(F) \to \bigoplus (Z_2 \oplus A_w), \quad u(F)(f) = u(hfh^{-1}),$$

where h denotes some isomorphism $F \to \perp n_w F_w$. It is easy to prove that

$$u(F \perp G)(f \perp g) = u(F)(f) \cdot u(G)(g). \tag{1}$$

Since also

$$u(F)(fg) = u(F)(f) \cdot u(F)(g), \tag{2}$$

it follows that there exists a group homomorphism

$$K_1(\underline{R\text{-Mod}}_M^m, \perp) \to \bigoplus (Z_2 \oplus A_w), \quad [(F, f)] \mapsto u(F)(f).$$

Evidently, the images of the generators $[(F_w, f)]$, $[(F_w \perp F_w, \bar{t})]$ of $K_1(\underline{R\text{-Mod}}_M^m, \perp)$ are the generators $(1, \bar{f})$, $(-1, \bar{1})$ of $\bigoplus (Z_2 \oplus A_w)$. Moreover relations in

$K_1(\underline{R\text{-Mod}}_M^m, \perp)$ show that there exists a homomorphism $\bigoplus (Z_2 \oplus A_w) \to K_1(\underline{R\text{-Mod}}_M^m, \perp)$ which carries $(1, \bar{f})$ and $(-1, \bar{1}) \in Z_2 \oplus A_w$ into $[(F_w, f)]$ and $[(F_w \perp F_w, \bar{t})]$, respectively. This completes the proof.

References

[1] H. Bass, *Lectures on Topics in Algebraic K-theory*, Tata Institute of Fundamental Research, Bombay 1967.

[2] N. Bourbaki, *Algèbre*, Chap. 9, Paris 1959.

[3] H. Cartan and S. Eilenberg, *Homological Algebra*, Princeton 1956.

[4] O. T. O'Meara, *Introduction to Quadratic Forms*, Berlin 1963.

[5] A. Prószyński, *On quadratic forms over S-rings*, Bull. Acad. Polon. Sci. 20 (1972), pp. 121–129.

[6] N. Roby, *Lois polynômes et lois formelles en théorie des modules*, Ann. Éc. Norm. Sup. 80, (1963), pp. 213–348.

INSTITUTE OF MATHEMATICS, POLISH ACADEMY OF SCIENCES

Accepté par la Rédaction le 22. 9. 1975