Chapter 13. Decomposition of Projective Modules

MODERN CLASSICAL ALGEBRA

Professor J. C. Moore

Chapter 13: Decomposition of Projective Modules.

1. The Prime Spectrum

Let R be a commutative ring, $\mathfrak{P}$ the set of prime ideals in R and $\mathfrak{M}$ the set of maximal ideals in R. We define a topology in $\mathfrak{P}$. Each ideal I in R determines a closed set

$$W(I) = \{p \in \mathfrak{P} \mid p \supset I\} .$$

If $\{I_j\}$ is a family of ideals in R, then

$$W(I_j) \cup W(I_k) = W(I_j \cap I_k)$$
$$\bigcap_j W(I_j) = W(\sum_j I_j)$$

are closed. $\mathfrak{P}$ resp. $\mathfrak{M}$ endowed with this topology are called the prime spectrum resp. maximal ideals spectrum of R.

Proposition 1.1 R has non-trivial idempotents if and only if its prime spectrum is disconnected.

Proof: Suppose $e \in R$ is a non-trivial idempotent. Let $A = \{p \in \mathfrak{P} \mid e \in p\}$, $B = \{p \in \mathfrak{P} \mid 1-e \in p\}$, $I = \bigcap_{p \in A} p$, $J = \bigcap_{p \in B} p$. We have $A, B \neq \emptyset$, $A \cap B = \emptyset$ and $A \cup B = \mathfrak{P}$, the latter because $e(1-e) = 0 \in p$ implies $e \in p$ or $1-e \in p$ for $p \in \mathfrak{P}$. Clearly $A = W(I)$ and $B = W(J)$. Thus $\mathfrak{P} = A \cup B$ is disconnected. Conversely, suppose $\mathfrak{P} = W(I) \cup W(J)$ and $W(I) \cap W(J) = \emptyset$, i.e. $I + J = R$ and $I \cap J \subset \sqrt{0}$. Pick $x \in I$ and $y \in J$ such that $x + y = 1$. $(xy)^n = 0$ for some n since $xy \in \sqrt{0}$. We claim $Rx^k + Ry^k = R$ for every integer $k \geqq 0$. For if not $Rx^k + Ry^k$ would be contained in some maximal ideal M, say $M \in W(I)$; then $y^k \in M$. Since also $x^i y^{k-i} \in M$ for $i > 0$, $(x + y)^k = 1 \in M$, a contradiction. Thus $1 = ax^n + by^n$ for suitable $a, b \in R$. Let $e = ax^n$; then $e^2 = e$ and $e \neq 0$ or 1.

A topological space E is noetherian if the descending chain condition holds for closed sets. Suppose now E is noetherian. A closed set $W \neq \emptyset$ is irreducible if whenever $W = W_1 \cup W_2$, W_1 and W_2 closed, then $W = W_1$ or $W = W_2$. Every closed set $W \neq \emptyset$ in E is union of a finite number of irreducible closed sets; these irreducible closed sets are uniquely determined by W. The verification of this statement is immediate.

Let W be an irreducible closed set, and

$$W < W_1 < W_2 < \cdots < W_n$$

a chain of closed sets ($<$ stands for proper inclusion). n is called the height of the chain. The supremum over the heights of all such chains is called the height of W, $ht(W)$. In general, if W is any closed set, $ht(W)$ is the infimum of the heights of the irreduciple components of W. We let $ht(\emptyset) = \infty$.

$$\sup\{ht(W) \mid W \neq \emptyset \text{ is closed in } E\}$$

is the dimension of the noetherian space E.

The prime spectrum and the maximal ideal spectrum of a noetherian ring R are noetherian. The irreducible closed sets in $\mathcal{P}$ are of the form $W(p)$ where p is prime; for if A is closed, let $p = \bigcap_{q \in A} q$; clearly p is prime and $A = W(p)$.

<u>Proposition 1.2</u> Let R be a commutative noetherian ring, and P a projective module over R. $\operatorname{rank}_p P$ depends only on the connected component of p in $\mathcal{P}$.

Proof: $p,q \in \mathcal{P}$ are in the same connected component of $\mathcal{P}$ if and only if there is a chain of closed sets $W_o,\ldots,W_n$ such that $W_i \cap W_{i+1} \neq \emptyset$ and $q \in W_o$, $Q \in W_n$. For if p and q are in the same connected component W of $\mathcal{P}$, consider an irreducible decomposition of W into irreducible closed sets. These irreducible closed sets can be arranged into a chain with the desired properties because W is not the union of two disjoint closed subsets different from W. For the converse note that an irreducible closed set is connected. Suppowe $W_i = W(p_i)$ with p_i being prime ideals. If $W_i \cap W_{i+1} \neq \emptyset$, then there is a maximal ideal p in this intersection, $p \supset p_i, p_{i+1}$. In general, if p and q are prime and $p \supset q$, then $\operatorname{rank}_p P = \operatorname{rank}_q P$ because P_p is free and $(P_p)_q = P_q$.

<u>Corollary 1.3</u> For a noetherian ring R the following are equivalent:

(1) R is coherent.

(2) R contains no non-trivial idempotents.

(3) The prime spectrum of R is connected.

(4) For any projective R-module P, $\operatorname{rank}_p P$ is independent of the prime ideal p.

Clearly $(2) \Rightarrow (3) \Rightarrow (4) \Longrightarrow (1) \Rightarrow (2)$.

2. J.-P. Serre's Structure Theorem

Our aim is the following structure theorem [Module projectifs et espaces fibrés à fibre vectorielle; exposé 23 in Séminaire Dubreiel-Pisot 11 (1957/58)].

<u>Theorem 2.1</u> Suppose R is a commutative noetherian ring with connected prime spectrum. Every finitely generated projective R-module P is of the form $F \oplus P'$ where F is free and P' is projective of rank $\leqq \dim \mathfrak{M}$ ($\leqq$ Krull dimension of R).

Let P be a finitely generated Projective module over R. We write $P(p)$ for P/pP and $p \in \mathfrak{M}$. Each element $s \in P$ induces an element in $P(p)$ which we will denote by $s(p)$. $s_1, \ldots, s_k$ are called linearly independent at $p \in \mathfrak{M}$ if $s_1(p), \ldots, s_k(p)$ are linearly independent in the vector space $P(p)$ over the field $R(p)$.

<u>Proposition 2.2</u> Let $s \in P$;

$$\begin{aligned} \varphi \ : R &\longrightarrow P \\ r &\longrightarrow rs \end{aligned}$$

is an isomorphism of R onto a direct summand of P if and only if $s(p) \neq 0$ for $p \in \mathfrak{M}$.

Proof: Let $I = \operatorname{im} \varphi$. Suppose $s(p) = 0$ for some $p \in \mathfrak{M}$, but $P = I \oplus Q$. Then $I \subset pP = pI \oplus pQ$. Consequently $I \subset pI$, or $I = pI$, which is impossible because I is free. Converesely, suppose $s(p) \neq 0$ for all $p \in \mathfrak{M}$. Let $J = \text{Kernel}\ (\varphi)$. $0 \longrightarrow J \longrightarrow R \longrightarrow P$ is exact, so by localization,

$$0 \longrightarrow J_p \longrightarrow R_p \longrightarrow P_p$$

is exact for $p \in \mathfrak{M}$. P_p is free, say with generators $y_1,\dots,y_r$, and let $s(\rho) = \Sigma\, x_i y_i$. Then $r\cdot x_i = 0$ for $r \in J_p$. Since not all $x_i \in p_p$, one of them is a unit, thus $r = 0$. Hence $J_p = 0$ for $p \in \mathfrak{M}$ which implies $J = 0$. Therefore $0 \longrightarrow R \longrightarrow P \longrightarrow P/I \longrightarrow 0$ is exact. It remains to be shown that P/I is projective. By hypothesis on s,

$$\begin{tikzcd}
0 \arrow[r] & R/p \otimes R \arrow[r] \arrow[d, equal] & R/p \otimes P \arrow[r] \arrow[d, equal] & R/p \otimes P/I \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & R(p) \arrow[r] & P(p) \arrow[r] & P/I(p) \arrow[r] & 0
\end{tikzcd}$$

is exact for $p \in \mathfrak{M}$. Thus since R/p is a field,

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Hom}_{R/p}(P/I(p),R/p) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_{R/p}(P(p),R/p) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_{R/p}(R/p,R/p) \arrow[r] \arrow[d, "\cong"] & 0 \\
0 \arrow[r] & \mathrm{Hom}_R(P/I,R/p) \arrow[r] & \mathrm{Hom}_R(P,R/p) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}_R(R,R/p) \arrow[r] \arrow[d, "\cong"] & 0 \\
 & & R/p \otimes \mathrm{Hom}.(P,R) \arrow[r] & R/p \otimes R \arrow[r] & 0
\end{tikzcd}$$

is exact for $p \in \mathfrak{M}$. Hence $\mathrm{Hom}(P,R) \longrightarrow R$ is onto, i.e. φ has a left inverse.

In order to prove the theorem it suffices now to show

<u>Lemma 2.3</u> Let h be a non-negative integer such that $h \leqq \mathrm{rank}_p P$ for $p \in \mathfrak{M}$; then there is $s \in P$ and a closed subset F of of height $\geqq h$ such that $s(p) \neq 0$ for $P \notin F$.

In fact, if $\mathrm{rank}_p P > \dim \mathfrak{M}$ for all $p \in \mathfrak{M}$, we can take $h = \dim_p P$ (supposing the prime spectrum of R is connected so that $\dim_p P$ is independent of the prime p). Then $\mathrm{ht}(F) > \dim \mathfrak{M}$, i.e. $F = \emptyset$, and we can apply proposition 2.2.

In order to be able to prove the lemma by induction on h, we have to prove a more general statement (lemma 2.6).

<u>Lemma 2.4</u> Let $F \subset \mathfrak{M}$ be such that $s_1, \ldots, s_k \in P$ are linearly dependent exactly at $p \in F$, then F is closed.

Proof: Let Q be a projective such that $P \oplus Q = E$ is a free module of finite rank. Pick a basis for E; this gives a basis for the homogeneous part $E_k(E)$ of degree k of the exterior algebra over E. Let I be the ideal of R generated by the coeficients of $s_1 \wedge s_2 \wedge \ldots \wedge s_k$ in this basis. Now $s_1(p) \wedge \ldots \wedge s_k(p) = 0$ if and only if $p \supset I$, i.e. $F = W(I)$.

<u>Lemma 2.5</u> Suppose $p_1, \ldots, p_k \in \mathfrak{M}$ are distinct, and $v_i \in P(p_i)$, $1 \leqq i \leqq k$. Then there exists $s \in P$ such that $s(p_i) = v_i$, $1 \leqq i \leqq k$.

Proof: Let $I_i = \bigcap_{j \neq i} p_j$; then $\Sigma I_i = R$. So there are $\varepsilon_i \in I_i$ with $\Sigma \varepsilon_i = 1$. Pick $s_i \in P$ with $s_i(p_i) = v_i$ and let $s = \Sigma s_i \varepsilon_i$.

<u>Lemma 2.6</u> Let $s_1, \ldots, s_k$ be linearly dependent exactly at $p \in F \subset \mathfrak{M}$. Suppose $p_1, \ldots, p_k \in F$, $v_i \in P(p_i)$ $i = 1, \ldots, k$, and h is a non-negative integer such that $h + k \leqq \dim_p P$ for all $p \in \mathfrak{M}$. Then there is $s \in P$ and a closed set $E \subset \mathfrak{M}$ such that

1) $s(p_i) = v_i$,

2) $s_1, \ldots, s_k, s$ are linearly dependent exactly at $F \cup E$,

3) $ht(E) \geqq h$.

Proof: We proceed by induction on h. This is trivial for $h = 0$: we solve first 1), and let E be the set where $s_1, \ldots, s_k, s$ are linearly dependent. Now suppose $h > 0$, and the lemma holds for $h - 1$. Let $u \in P$ and $G \subset \mathfrak{M}$ be a closed set such that 1) $u(p_i) = v_i$, 2) $s_1, \ldots, s_k, u$ are linearly dependent exactly at $F \cup G$, 3) $ht(G) \geqq h - 1$. Let $G_1, \ldots, G_m$ be the irreducible components of G of height $h-1$. Pick

$$p_\alpha \in G_\alpha - (F \cup \bigcup_{\beta \neq \alpha} G_\beta) .$$

$s_1(p_\alpha),\ldots,s_k(p_\alpha)$ are linearly independent in $P(p_\alpha)$, but $u(p_\alpha)$ depends linearly on them. Since $h > 0$, $\dim P(p_\alpha) = \operatorname{rank}_{p_\alpha} P > k$. So there are $w_\alpha \in P(p_\alpha)$ linearly independent of $s_1(p_\alpha),\ldots,s_k(p_\alpha)$. Using the induction hypothesis again, we can find $t \in P$ and a closed set $H \subset \mathfrak{M}$ such that

1) $t(p_i) = 0$, $t(p_\alpha) = w_\alpha$

2) $s_1,\ldots,s_k,u,t$ are linearly dependent exactly at $p \in F \cup G \cup H$,

3) $\operatorname{ht}(H) \geq h - 1$.

Let $H_1,\ldots,H_r$ be the irreducible components of H of height $h-1$. Choose

$$q_\beta \in H_\beta - (F \cup G \cup \bigcup_{\gamma \neq \beta} H_\gamma) .$$

$s_1(q_\beta),\ldots,s_k(q_\beta)$, $u(q_\beta)$ are linearly independent, and $t(q_\beta)$ depends linearly on these elements, say

$$u(q_\beta) = \delta_\beta \cdot t(q_\beta) \bmod (s_1(q_\beta),\ldots,s_k(q_\beta)) .$$

Pick $f \in R$ such that

$$f(p_\alpha) = 1 \quad \text{and} \quad f(q_\beta) \neq \delta_\beta .$$

Define $s = u - ft$. Let E' be the set where $s_1,\ldots,s_k,s$ are linearly dependent. Define E to be union of the irreducible components of E' which are not in F.

1) and 2) are fulfilled by construction. Let E_0 be an irreducible component of E. $E_0 \subset G \cup H$, so $\operatorname{ht}(E_0) \geq h - 1$.

Suppose $ht(E_o) = h-1$, then $E_o = G_\alpha$ or $E_o = H_\beta$ for some α or β . Suppose $E_o = G_\alpha$; $s(p_\alpha) = u(p_\alpha) - t(p_\alpha)$ depends linearly on $s_1(p_\alpha),\ldots,s_k(p_\alpha)$ by definition of E_o . On the other hand, $u(p_\alpha)$ depends linearly on $s_1(p_\alpha),\ldots,s_k(p_\alpha)$ by construction of G_α . Hence $t(p_\alpha) = w_\alpha$ depends linearly on $s_1(p_\alpha),\ldots,s_k(p_\alpha)$, a contradiction to the definition of w_α . Suppose $E_o = H_\beta$. $s(q_\beta) = 0 \bmod (s_1(q_\beta), \ldots, s_k(q_\beta))$ by construction of E_o . On the other hand $s(q_\beta) = u(q_\beta) - f(q_\beta) \cdot t(q_\beta) \neq 0 \bmod (s_1(q_\beta),\ldots,s_k(q_\beta))$ by definition of H_β . Hence $ht(E_o) \neq h-1$, i.e. $ht(E_o) > h-1$. This shows $ht(E) > h-1$.

3. C. S. Seshadri's Theorem

C. S. Seshadri's theorem [Triviality of vector bundles over the affine space K^2, Proceedings of the National Academy of Science, vol. 44 (1958)] states that every finitely generated projective module over the polynomial ring $A[t]$ over a principal ideal ring A, is a free module. Or, more generally:

<u>Theorem 3.1</u>. Suppose R is a Dedekind domain, and P a finitely generated projective $R[x]$-module of rank n. Then there is a free $R[x]$-module F of rank $n-1$ and an ideal I in R such that $P = F \oplus (R[x] \otimes I)$.

Before we can prove this theorem, we have to recall some properties of matrices.

<u>Lemma 3.2.</u> Let K be a field. Every $n \times n$ matrix D with coefficients in $K[x]$ and determinant 1 is product of $n \times n$ matrices of the form

$$D_{ij}(p) = \begin{array}{c} \hphantom{1\;0\;\cdots\;\cdots\;} j \hphantom{\;\cdots\;\cdots\;0} \\ \begin{vmatrix} 1 & 0 & \cdots & \cdots & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & \cdots & \cdots & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & 0\;1\;0 & \cdots & p & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \vdots & \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \end{vmatrix} \end{array} \begin{matrix} \\ \\ \\ \\ i \\ \\ \\ \end{matrix}$$

where $p \in K[x]$ and $i \neq j$.

Proof: Multiplying D on the right with $D_{ij}(p)$ means: adding to the j-th column of D the i-th column multiplied by p. Multiplying D on the right by $D_{ij}(-1)D_{ji}(1)D_{ij}(-1)$ means: interchanging the i-th and j-th column and multiplying the j-th column by -1. Similarly with respect to rows of D and multiplication on the left. With these operations D can be transformed into a diagonal matrix $D' = ADB$, A and B being product of matrices $D_{ij}(p)$ (notice that $[D_{ij}(p)]^{-1} = D_{ij}(-p)$). Since $\det D = 1$, also $\det D' = 1$, i.e. the entries in D' are elements of the field K. Now

$$D' = \begin{vmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{vmatrix}$$

$$= \begin{vmatrix} \lambda_1 & & & & 0 \\ & \lambda_2 \cdots \lambda_n & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & & & & \\ & (\lambda_3 \cdots \lambda_n)^{-1} & & & \\ & & (\lambda_1\lambda_2)^{-1} & & \\ & & & \ddots & \\ 0 & & & & 1 \end{vmatrix} \cdot \begin{vmatrix} 1 & & & & & & 0 \\ & 1 & & & & & \\ & & \lambda_1\lambda_2\lambda_3 & & & & \\ & & & \lambda_4 \cdots \lambda_n & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & & & & 1 \end{vmatrix} \cdots$$

and a two-by-two matrix $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ with $xy = 1$ is easily seen to be a product of matrices $D_{ij}(p)$. Therefore D' is again product of matrices $D_{ij}(\alpha)$, $\alpha \in K$.

Let R be a Dedekind domain, p a prime ideal in R. Suppose P is a finitely generated projective R-module, say $P = \sum_1^n \oplus I_j$ where I_j are ideals in R. $\overline{P} = P/pP = \Sigma \oplus \overline{I}_j$ is R/p-free with free generators $\overline{e}_1, \ldots, \overline{e}_n$, where $e_j \in I_j$ and $\overline{e}_j$ generates $\overline{I}_j$.

<u>Lemma 3.3.</u> Every automorphism of $\overline{P}[x] = R/p[x] \otimes_{R/p} \overline{P}$ of determinant 1 is induced by an automorphism of $P[x] = R[x] \otimes_R P$.

Proof: It suffices to prove this for an automorphism with matrix $D_{ij}(\bar{q})$, $\bar{q} = \Sigma \bar{c}_k x^k \in R/p[x]$. Lift each $\bar{c}_k$ to an element c_k of $I_i I_j^{-1}$ via the natural morphism

$$I_i I_j^{-1} = I_i \otimes \mathrm{Hom}(I_j, R) \longrightarrow R/p \otimes I_i \otimes R/p \otimes \mathrm{Hom}(I_j, R)$$
$$\longrightarrow \bar{I}_i \otimes \mathrm{Hom}(\bar{I}_j, R/p) \quad = \quad R/p \ .$$

Define $q = \Sigma c_k x^k$; clearly $D_{ij}(q)$ acting on $\Sigma \oplus I_k$ induces $D_{ij}(\bar{q})$. $D_{ij}(q)$ has the inverse $D_{ij}(-q)$, so defines an automorphism.

Proof of the theorem: P is a finitely generated projective $R[x]$-module of rank n . Consider all submodules L of P which are isomorphic to a module of the form $\sum_1^n \oplus I_k$, I_k being an extended ideal (i.e. $I_k = R[x] \otimes I_k'$ and I_k' is an an ideal in R). Let K be the field of fractions of R . Since $K \otimes_R L \cong K \otimes_R P$ and P is finitely generated, we can find $r \in R[x]$ such that $r \neq 0$ and $rP \subset L$. Now let L be a maximal submodule of P of this kind (which exists because P is noetherian), and suppose $L \neq P$. Let p be a prime ideal in R which divides the annihilator $A \neq 0$ of P/L . The morphism $j: L \longrightarrow L/pL \longrightarrow P/pP$ has kernel $L \cap pP$. Let N and I be the kernel and image of $i: L/pL \longrightarrow P/pP$.

$$0 \longrightarrow N \longrightarrow L/pL \xrightarrow{i} I \longrightarrow 0$$

splits over the principal ideal domain $R/p[x]$ (because I is free over $R/p[x]$ as a submodule of the free module P/pP) . We claim that $N \neq 0$. For, otherwise, i is one-to-one, i.e. $L \cap pP = pL$, and thus $p(p^{-1}A)P \subset L \cap pP = pL$, $p^{-1}AP \subset L$. This is a contradiction because A was the annihilator of P/L . We select now a basis

$\bar{e}_1,\ldots,\bar{e}_n$ for L/pL such that $\bar{e}_1,\ldots\bar{e}_s$ $(s \geqq 1)$ is a basis for N and $i(\bar{e}_{s+1}),\ldots,i(\bar{e}_n)$ is a basis for I. Since $L = \Sigma \oplus I_j$, I_j are extended ideals, we can chose a basis $\bar{\varepsilon}_1,\ldots,\bar{\varepsilon}_n$ for L/pL such that $\bar{\varepsilon}_j$ is a generator of $\bar{I}_j = I_j/pI_j$. Let $\bar{T}$ be the automorphism of L/pL which corresponds to the change of bases $(\bar{\varepsilon}_j) \longrightarrow (\bar{e}_j)$. We may assume that $\det \bar{T} = 1$ (changing $\bar{\varepsilon}_1$ by a factor if necessary). Let T be an automorphism of L inducing $\bar{T}$. Define $I_j' = TI_j \subset P$; then $L = \Sigma \oplus I_j'$. Moreover, $I_k' \subset pP$ for $1 \leqq k \leqq s$. Thus $L' = \sum_1^s p^{-1} I_k' \oplus \sum_{s+1}^n I_j' \subset P$ and $L \subset L'$, a contradiction to the maximality of L.

Hence $L = P$; P is of the form $P' \otimes R[x]$, P' being a finitely generated projective R-module of rank n. The assertion follows now from the decomposition theorem for P' (Proposition 5.6 of Chapter).

4. The Krull-Schmidt Theorem

In the following Λ will always denote a (not necessarily commutative) ring.

Definition 4.1. A (left) Λ-module A is said to be indecomposable if A is not the direct sum of two non-zero Λ-modules.

The following lemma is easily verified:

Lemma 4.2. A is indecomposable if and only if the ring $\mathrm{Hom}\,(A,A)$ has no non-trivial idempotents.

Recall that a ring Λ is local if the set of non-units is an ideal in Λ ; or Λ possesses a unique maximal (two-sided) ideal which contains all right and left ideals of Λ . In the beginning of this section we will not assume that a local ring is noetherian. The following theorem is well-known from the theory of groups with operators:

Theorem 4.3. Suppose the left Λ-module M admits two decompositions

$$M = \sum_{i=1}^{s} \oplus M_i \quad \text{and} \quad M = \sum_{j=1}^{t} \oplus N_j \,, \qquad s \leqq t \,,$$

into indecomposable submodules M_i (resp. N_j) . If $\mathrm{Hom}(M_i,M_i)$, $1 \leqq i \leqq s$, is a local ring then $s = t$ and $M_i \cong N_j$ after suitable reordering.

Proof: We proceed by induction. Suppose $M_i \cong N_i$ for $i \leqq r-1$ and

$$M = N_1' \oplus \dots \oplus N_k' \oplus M_{k+1} \oplus \dots \oplus M_s \quad \text{for} \quad k \leqq r\text{-}1 \,,$$

where N_i' is a submodule of M isomorphic to N_j . Consider

$$M = N_1' \oplus \dots \oplus N'_{r-1} \oplus M_r \oplus \dots \oplus M_s \,.$$

Let $\pi_1, \ldots, \pi_s$ be the projections determined by this decomposition, and $\eta_1, \ldots, \eta_t$ the idempotents of $\mathrm{Hom}(M,M)$ determined by the representation $M = \Sigma \oplus N_j$. Evidently $\pi_r = \pi_r \circ \Sigma \eta_j = \Sigma \pi_r \circ \eta_j$. $\pi_r \circ \eta_j = \pi_r \circ \pi_j \circ \eta_j = 0$ for $j \leqq r-1$, hence

$$\pi_r = \pi_r \circ \eta_r + \ldots + \pi_r \circ \eta_t .$$

We operate now in M_r; here $1 = \pi_r = \pi_r \circ \eta_r + \ldots + \pi_r \circ \eta_t$. Since $\mathrm{Hom}(M_r, M_r)$ is a local ring, one of the $\pi_r \circ \eta_j$, say $\pi_r \circ \eta_r$ is an automorphism of M_r. We show $N_r \cong M_r$ under η_r^{-1}, and that (+) holds for $k = r$.

Since $\pi_r \eta_r$ is an automorphism of M_r, $\eta_r \colon M_r \longrightarrow N_r$ is a monomorphism. Let $\overline{N}_r = \eta_r(M_r)$ and let K be the kernel of $\pi_r \colon N_r \longrightarrow M_r$; we have $\overline{N}_r \cap K = (0)$. If $y \in N_r$, $\pi_r(y) = \pi_r \eta_r(x)$ for some $x \in M_r$ ($\pi_r \circ \eta_r$ being an automorphism of M_r). Thus

$$y = (y - \eta_r(x)) + \eta_r(x), \; y - \eta_r(x) \in K , \; \eta_r(x) \in \overline{N}_r \;;$$

i.e. $N_r = K \oplus \overline{N}_r$. But N_r is indecomposable, hence $N_r = \overline{N}_r$. This implies that $\eta_r \colon M_r \longrightarrow N_r$ is an isomorphism. It is now easily verified that

$$\pi_1 + \ldots + \pi_{r-1} + \eta_r^{-1} \circ \pi_r + \pi_{r+1} + \ldots + \pi_s$$

maps M isomorphically onto $N_1 \oplus \ldots \oplus N_r \oplus M_r \oplus \ldots \oplus M_s$.

The following proposition guarantees the existence of such decompositions in certain cases:

Proposition 4.4. Suppose Λ satisfies the ascending or the descending chain condition on left ideals. Then every finitely generated (left) Λ-module admits a decomposition into a finite direct sum of indecomposable modules.

Proof: Let A be a finitely generated Λ-module. If A is not indecomposable, $A = A_1 \oplus A_2$ and $A_i \neq 0$. If A_i is not indecomposable, $A_i = A_{i1} \oplus A_{i2}$ and $A_{ij} \neq 0$; etc. Since A satisfies the ascending (descending) chain condition, we conclude easily that this process must stop after a finite number of steps.

Definition 4.5. We say that the Krull-Schmidt theorem holds for a left Λ-module A if A is the direct sum of indecomposable modules, the sum being unique up to order and isomorphism.

We give an example:

Lemma 4.6. Suppose Λ satisfies the descending chain condition for left ideals. Let R be the radical of Λ (Definition 8.28 of Chapter 9). Every idempotent of Λ/R is induced by an idempotent of Λ.

Proof: R is nilpotent by Theorem 8.35 of chapter 9, say $R^m = 0$. Let $\bar{e} \in \Lambda/R$ be an idempotent, say induced by $g \in \Lambda$. Then $z = g^2 - g \in R$. Now define g_n and $z_n \in R^{2n}$ by induction:

$$g_0 = g, \quad z_0 = z;$$
$$g_n = g_{n-1} + z_{n-1} - 2g_{n-1}z_{n-1},$$
$$z_n = g_n^2 - g_n = 4z_{n-1}^3 - 3z_{n-1}^2 \in R^{2n}.$$

Thus $z_m = 0$, or $g_m^2 = g_m = e$ is idempotent and induces $\bar{e}$.

Corollary 4.7. Suppose Λ is noetherian and satisfies the descending chain condition for left ideals. Then the Krull-Schmidt theorem holds for finitely generated left Λ-modules.

Proof: In view of Theorem 4.3 it suffices to prove that the non-units in $\mathrm{Hom}(M,M)$, M finitely generated and indecomposable, form an ideal.

that $(\delta,x) \longrightarrow \delta x$ and $(x,y) \longrightarrow x + y$ from $L \times A$ resp. $A \times A$ into A is continuous; if A is an algebra then $(x,y) \longrightarrow xy$ is also continuous.

Lemma 4.8. 1) If L is a complete local ring then each finitely generated left Λ-module A is also complete. 2) The completion $\bar{L}$ of any local ring L is again a local ring with maximal ideal $\bar{p} = p\bar{L}$; we have $L/P \cong \bar{L}/\bar{P}$.

Proof: 1) This is obvious if A is free. Now let $A = F/B$ where F is free and of finite rank. The canonical map $\pi \colon F \longrightarrow A$ is easily seen to be continuous. Now let $(a_n) \subset A$ be a Cauchy sequence, say $a_n - a_{n+1} \in p^n A$ (after passing to a subsequence). By induction find $b_n \in F$ with $\pi(b_n) = a_n$ such that $b_n - b_{n+1} \in p^n F$; first find $b'_{n+1} \in F$ with $\pi(b'_{n+1}) = a_{n+1}$; now $b_n - b'_{n+1} - c \in p^n F$ for some $c \in B$; define $b_{n+1} = b'_{n+1} + c$. (b_n) is Cauchy in F , thus converges to $b \in F$. Since π is continuous, $a_n \longrightarrow \pi(b)$ in A .

2) $\bar{L}$ is clearly a ring. If $\bar{x} \in \bar{L}$ is not a unit then there is a sequence of non-units $x_n \in L$ converging to $\bar{x}$ (continuity of $y \longrightarrow y^{-1}$ in L) . From this remark it is obvious that the non-units in $\bar{L}$ form an ideal which is equal to the closure $\bar{p}$ of p . $p\bar{L}$ is an $\bar{L}$-module, hence complete, hence closed in $\bar{L}$, i.e. $p\bar{L} = \bar{p}$. $L \longrightarrow \bar{L}$ induces $L/P \xrightarrow{i} \bar{L}/\bar{P}$, and the image is dense in $\bar{L}/\bar{P}$. $\bar{L}/\bar{P}$ has the discrete topology, hence $\mathrm{im}(i) = \bar{L}/\bar{P}$.

Now we can prove Lemma 4.6 for our new setting:

Lemma 4.9. Let Λ be any finitely generated L-algebra, where L is a complete local ring with maximal ideal p . Every idempotent $\bar{e} \in \Lambda/p\Lambda$ is induced by an idempotent $e \in \Lambda$.

Proof: The proof is almost the same as that of lemma 4.6;
$z_n = g_n^n - g_n \in p^{2n}\Lambda$, thus $z_n \longrightarrow 0$, and $g_{n+1} - g_n = z_n(1-2g_n) \in p^{2n}\Lambda$, thus (g_n) is Cauchy and converges therefore to an element $e \in \Lambda$. $e^2 - e = \lim z_n = 0$. Since $\pi\colon \Lambda \longrightarrow \Lambda/p\Lambda$ is continuous, $\pi(e) = \lim \pi(g_n) = \bar{e}$.

Proposition 4.10. Let Λ be any finitely generated L-algebra, L being a complete local ring. The Krull-Schmidt theorem holds for finitely generated Λ-modules.

Proof: Since Λ is noetherian proposition 4.4 applies. Thus we need only check the hypothesis of Theorem 4.3. Let M be a finitely generated indecomposable left Λ-module. Hom(M,M) has no non-trivial idempotents (Lemma 4.2). Let R be the radical of Hom(M,M). Notice that the image of R in Hom(M,M)/pHom(M,M) is the radical of Hom(M,M)/pHom(M,M), and pHom(M,M) $\subset$ R ; for if P is a maximal ideal in Hom(M,M) and pHom(M,M) $\not\subset$ P, then pA = A where A = Hom(M,M)/P ; hence A = 0 by Nakayama's lemma (Proposition 4.I of Chapter 5), a contradiction. Hom(M,M)/pHom(M,M) is finite dimensional over L/p, hence satisfies the descending chain condition. Thus every idempotent in Hom(M,M)/R comes from an idempotent in Hom(M,M)/pHom(M,M) (Lemma 4.6). Lemma 4.9 shows that every idempotent in Hom(M,M)/pHom(M,M) comes from an idempotent in Hom(M,M). Hence Hom(M,M)/R has no non-trivial idempotents. Hom(M,M)/R is finite dimensional over L/p. Thus Hom(M,M)/R is semi-simple, hence a division ring, or R is a maximal ideal in Hom(M,M), i.e. the only maximal ideal in Hom(M,M).

5. R. G. Swan's Decomposition Theorem
The General Case

Reference: Induced Representations and Projective Modules, by R. G. Swan, Annals of Mathematics, vol. 71 (1960).

We stick to the notation used in section 6 of chapter 12.

Let L be a complete local ring, π a finite group and $P(L\pi)$ the Grothendieck group associated to the class of all finitely generated projective left $L\pi$-modules.

<u>Proposition 5.1</u>. $P(L\pi)$ is free abelian with one generator for each isomorphism class of indecomposable projectives.

Proof: Let F be the free abelian group with the isomorphism classes of finitely generated indecomposable projectives as generators. Let $[P] \in P(L\pi)$, say $P = \Sigma \oplus P_i$ is a decomposition of P into indecomposable projectives according to Proposition 4.10. Define $\sigma[P] = \Sigma[P_i] \in F$. If $0 \longrightarrow P' \longrightarrow P \longrightarrow P'' \longrightarrow 0$ is an exact sequence of finitely generated $L\pi$-projectives, then $P = P' \oplus P''$. Thus the uniqueness part of Proposition 4.10 shows that the map $\sigma\colon P(L\pi) \longrightarrow F$ is well defined. σ is onto and has an obvious inverse, i.e. $P(L\pi) \cong F$.

<u>Corollary 5.2</u>. If P and P' are finitely generated $L\pi$-projectives and $[P] = [P']$ in $P(L\pi)$ then $P \cong P'$.

<u>Theorem 5.3.</u> Suppose L is a complete local domain, K its field of fractions, and π a finite group of order prime to the characteristic of K. $j_*\colon P(L\pi) \longrightarrow P(K\pi)$ (the map induced by $j\colon L \longrightarrow K$, $j_*[P] = [K \otimes P]$) is a monomorphism.

Proof: 1) Suppose π is abelian. Let $L\pi = \Sigma \oplus I_i$ be a decomposition of $L\pi$ into indecomposable ideals (Theorem 4.10). Any indecomposable finitely generated projective is isomorphic to one of the I_i as follows easily from the uniqueness of decompositions. We have $1 = \Sigma e_i, e_i \in I_i$, $e_i e_j = \delta_{ij} e_j$ where δ_{ij} is the Kronecker symbol. Suppose $j_*([P] - [P']) = 0$, i.e. $[K \otimes P] = [K \otimes P']$, hence $K \otimes P \cong K \otimes P'$ by Corollary 7.2 of chapter 12. If $P = I_i \oplus P_1$ then $e_i P \neq 0$, thus $e_i(K \otimes P) \cong e_i(K \otimes P') \neq 0$, or $e_i P' \neq 0$; hence $P' \cong I_i \oplus P_1'$ ($e_i I_j = \delta_{ij} I_j$ since $L\pi$ is commutative!); etc. Thus $P \cong P'$.

2) Let π be any group of order n; then $n^2 \in G_C(Z\pi)$ by Corollary 7.10 of chapter 12, i.e. there are cyclic subgroups $\pi_k \subset \pi$ and $x_k \in G(Z\pi_k)$ such that

$$n^2 = \Sigma\, i^*_k(x_k)\ ,\ i_k\colon \pi_k \subset \pi\ .$$

If $x \in P(L\pi)$ and $j_*(x) = 0$ then (Proposition 6.7 of chapter 12)

$$j_*(x_k i_k^*(x)) = j_*(x_k) i_k^* j_*(x) = 0\ ,$$

or $x_k i_k^*(x) = 0$ by 1); thus

$$(i_k)_*(x_k i_k^*(x)) = (i_k)_*(x_k)\cdot x = 0\ ,$$
$$n^2 \cdot x = 0\ ,$$

which implies $x = 0$ since $P(L\pi)$ is free.

Let R be a Dedekind domain, π a finite group of order n prime to the characterisitic of the field of fractions K of R. Suppose P is a finitely generated projective $R\pi$-module such that $K \otimes P$ is free over $K\pi$. If $\mathrm{char}(K) \neq 0$ then $[A] = [B]$ in $G(K\pi)$ or $G(R/p\pi)$ (p a prime ideal in R) implies $A \cong B$ (Corollary 7.2 of Chapter 12). Thus, chasing the diagram in Theorem 4.6 of chapter 12, we find that

P/pP is free. This result, the main lemma for the decomposition theorem of Swan, is needed without the restriction $\mathrm{char}(K) \neq 0$. It is this fact which made necessary Theorem 5.3 and thus the whole machinery of sections 6 and 7 of chapter 12.

Lemma 5.4. Suppose P is $R\pi$-projective and finitely generated. If $P \otimes K$ is $K\pi$-free then P/pP is $R/p\pi$-free for any prime ideal p in R.

Proof: Let L be the completion of R_p, the localization of R at p, and $\bar{K}$ the quotient field of L. We have $R/p \cong R_p/pR_p \cong L/pL$ (Lemma 4.8). Let $\bar{P} = L \otimes_R P$; then

$$\bar{K} \otimes_L \bar{P} \cong \bar{K} \otimes_R P \cong \bar{K} \otimes_K K \otimes_R P$$

is $\bar{K}\pi$-free. By Theorem 5.3, $\bar{P}$ is free. Consequently $P/pP \cong R/p \otimes_R P \cong L/pL \otimes_R P \cong L/pL \otimes_L L \otimes_R P \cong L/pL \otimes_L \bar{P}$ is free over $(L/pL)\pi \cong R/p\pi$.

Lemma 5.5. If A is a finitely generated torsion free (hence projective) R-module, then

$$\mathrm{rank}_R A = \mathrm{rank}_{R/p} A/pA$$

(where $\mathrm{rank}_R A$ means the rank of A at the prime 0).

This is immediate if we write A as the sum of $\mathrm{rank}_R A$ ideals.

If A is a $R\pi$-module and $B \subset A$ a submodule of A, then let

$$B: A = \{r \in R \mid rA \subset B\}.$$

Proposition 5.6. Let P be a finitely generated $R\pi$-module such that $K \otimes_R P$ is $K\pi$-free. Let $\mathfrak{a}$ be any non-zero ideal in R. P contains a free $R\pi$-module F such that

$$(F: P, \mathfrak{a}) = 1.$$

Proof: First suppose $\mathfrak{A} = p$ is prime. P/pP is free. Let $\bar{a}_1,\dots,\bar{a}_k$ be a basis for P/pP $(nk = \text{rank}_R P)$. The submodule F of P generated by $a_1,\dots,a_k$ is free: $F/pF = P/pP$, so $\text{rank}_R F = \text{rank}_{R/p} F/pF = \text{rank}_{R/p} P/pP = n\cdot k$. It is easily checked that $(F:P,p) = 1$. In general, $\mathfrak{A} = \Pi p_i$. The last step can be modified. Let $\bar{a}^i_1,\dots,\bar{a}^i_k$ be a basis for P/p_iP, and $\alpha_i \in R$ such that $\alpha_i = \delta_{ij} \bmod(p_j)$ (lemma 2.5). Define $a_s = \Sigma\, \alpha_i a^i_s$, $s = 1,\dots,k$.

Corollary 5.7. P can also be embedded into a free $R\pi$-module F such that $(P\colon F, \mathfrak{A}) = 1$.

Let $a \in \mathfrak{A}$ and $b \in F\colon P$ such that $a + b \equiv 1$, F being the module of Proposition 5.2. Now $(bP{:}F, \mathfrak{A}) = 1$ and $P \cong bP$.

Lemma 5.8. Suppose I is an ideal in $R\pi$ and $(I\colon R\pi, n) = 1$. Then I is $R\pi$-projective.

Proof: $R\pi/I$ is a direct summand of $R\pi \overset{\pi}{\otimes}_R R\pi/I$: Let $k\cdot n + b = 1$, $k \in R$ and $b \in I\colon R\pi$. Define

$$R\pi/I \xrightarrow{\eta} R\pi \overset{\pi}{\otimes}_R R\pi/I \qquad R\pi \overset{\pi}{\otimes}_R R\pi/I \xrightarrow{\varphi} R\pi/I$$
$$a = kn\cdot a \longrightarrow k\cdot \sum_{x\in\pi} x \otimes a \qquad\qquad x \otimes a \longrightarrow a$$

Clearly $\varphi \circ \eta = 1_{R\pi/I}$. Choose a projective resolution of $R\pi/I$ over R

$$0 \longrightarrow A \longrightarrow P \longrightarrow R\pi/I \longrightarrow 0\,,$$

P finitely generated. Then

$$0 \longrightarrow R\pi \overset{\pi}{\otimes}_R A \longrightarrow R\pi \overset{\pi}{\otimes}_R P \longrightarrow R\pi \overset{\pi}{\otimes}_R R\pi/I \longrightarrow 0$$

is a projective resolution over $R\pi$ (chapter 12, lemma 6.6). Hence $R\pi/I$ (a direct summand of $R\pi \overset{\pi}{\otimes}_R R\pi/I$) has homological dimension ≤ 1 over $R\pi$. Since $0 \longrightarrow I \longrightarrow R\,\pi \longrightarrow R\,\pi/I \longrightarrow 0$

is exact, I must be projective [Proposition 1.2, chapter 10].

<u>Proposition 5.9.</u> Suppose P is a finitely generated projective $R\pi$-module such that $K \otimes_R P$ is $K\pi$-free. Let $\mathfrak{b}$ be a non-zero ideal in R. Then $P = \Sigma \oplus I_j$, where I_j are projective ideals in $R\pi$ with $(I_j\colon R\pi, \mathfrak{b}) = 1$.

Proof: Let $\mathfrak{a} = n \cdot \mathfrak{b} \neq 0$ and F the free $R\pi$-module of Corollary 5.3, say with basis $(e_1, \ldots, e_k)$. Define a map

$$\varphi\colon F \longrightarrow R\pi$$

$$\Sigma \delta_j e_j \longrightarrow \delta_1 .$$

φP is an ideal I_1 in $R\pi$, and $I_1\colon R\pi \supset P\colon F$. So $I_1\colon R\pi$ is prime to n and $\mathfrak{b}$. Since I_1 is projective (lemma 5.4), $P = I_1 \oplus P'$. We may also assume that $K \otimes_R I_j = K\pi$. If R is a field, P is free by assumption and there is nothing to prove. Otherwise we can choose $\mathfrak{b} \neq R$; then $R\pi/I_j$ is an R-torsion module, i.e. $K \otimes_R R\pi/I_j = 0$, or $K \otimes_R I_j = K \otimes_R R\pi = K\pi$.

<u>Theorem 5.10</u>. Let R be a Dedekind domain, π a finite group of order n prime to the characteristic of K (the field of fractions of R), and P a finitely generated projective $R\pi$-module such that $K \otimes_R P$ is $K\pi$-free. Suppose $\mathfrak{a}$ is a non-zero ideal in R. Then $P \cong F \oplus I$, where F is $R\pi$-free and I is an ideal in $R\pi$ with $(I\colon R\pi, \mathfrak{a}) = 1$.

Proof: It suffices to show that if I and J are projective ideals in $R\pi$ with $K \otimes_R I \cong K \otimes_R J \cong K\pi$, then $I \oplus J \cong R\pi \oplus L$, L being an ideal of $R\pi$ such that $(L\colon R\pi, \mathfrak{a}) = 1$.

Let $\mathfrak{b} = I: R\pi$. J is isomorphic to an ideal J' having the property $(J': R\pi, \mathfrak{a}\mathfrak{b}) = L$. We replace J by J' . So there are $a \in I: R\pi$ and $b \in J: R\pi$ so that $a + b = 1$. Let $F = R\pi\cdot e_1 \oplus R\pi\cdot e_2$ be a free module of rank 2, and $A = Ie_1 \oplus Je_2$. Then $A \cong I \oplus J$, and $A: F$ is prime to $\mathfrak{a}$ because $(I: R\pi\cdot J: R\pi, \mathfrak{a}) = 1$. Define a new basis for F , $f_1 = ae_1 + be_2$ and $f_2 = e_1 - e_2$. $f_1 \in A$, thus $A = R\pi f_1 + Lf_2$ where

$$L = \{\delta \in R\pi \mid \delta f_2 \in A\} .$$

$L: R\pi = A: F$ is prime to $\mathfrak{a}$ and $I \oplus J \cong R\pi \oplus L$.

6. R. G. Swan's Decomposition Theorem
The Case of Characteristic 0

We are going to prove

Theorem 6.1. Suppose R is a Dedekind domain of characteristic 0, π a finite group of order n , and P a finitely generated projective $R\pi$-module. Assume that no prime dividing the order n of π is a unit in R . Then $K \otimes_R P$ is $K\pi$-free, K being the field of fractions of R .

The proof consists of several steps.

1) If L is a field of characteristic $p \neq 0$ and π a finite group of order p^e , then $L\pi$ is a (non-commutative) local ring. For, if $x \in L\pi$, then $x^{p^e} \in L$; thus x is a non-unit in $L\pi$ if and only if $x^{p^e} = 0$. $\{x \in L\pi, x^{p^e} = 0\}$ is the only maximal ideal in $L\pi$.

2) $n \mid \mathrm{rank}_R P$. Suppose $n = p^e\cdot m$ and $(p,m) = 1$. Let σ be a Sylow subgroup of π of order p^e . p lies in a prime ideal q of R. P/qP is projective over the local ring $R/q\pi$; hence P/qP is $R/q\sigma$-free [chapter 4, theorem 4.6]. Therefore

$$p^e \mid \mathrm{rank}_{R/q} P/qP = \mathrm{rank}_R P .$$

3) For any $R\pi$-module A let $A^{\pi} = \{a \in A | xa = a$ for all $x \in \pi\}$. We have $K \otimes_R A^{\pi} = (K \otimes_R A)^{\pi}$.

4) If π is cyclic, then $\mathrm{rank}_R P = n \cdot \mathrm{rank}_R P^{\pi}$.

Proof: First suppose $n = p$ is prime. Let q be a prime ideal containing p. As in 2), P/qP is $R/q\pi$-free, say generated by $\bar{a}_1, \ldots, \bar{a}_k$. As in proposition 5.6 we see that the submodule F of P generated by $a_1, \ldots, a_k$ is free, and $(F: P, q) = 1$. P/F is a torsion module over R. Let $r \in R - \{0\}$ with $rP \subset F$; then $rP^{\pi} \subset F^{\pi}$, so P^{π}/F^{π} is a torsion module over R, too. Consequently $K \otimes_R P = K \otimes_R F$ and $K \otimes_R P^{\pi} = K \otimes_R F^{\pi}$. In general, we proceed by induction. Let $\sigma < \pi$, $\sigma \neq \{1\}$, be a proper subgroup of π. P is projective over $R\sigma$ ($R\pi$ being free over $R\sigma$); thus $\mathrm{rank}_R P = [\sigma: 1] \cdot \mathrm{rank}_R P^{\sigma}$ by induction hypothesis. P^{σ} is projective over $R\pi/\sigma$ because $(R\pi)^{\sigma} = R\pi/\sigma$; thus again by induction hypothesis, $\mathrm{rank}_R P^{\sigma} = [\pi: \sigma] \cdot \mathrm{rank}_R (P^{\sigma})^{\pi/\sigma} = [\pi: \sigma] \cdot \mathrm{rank}_R P^{\pi}$.

5) The theorem holds for π a cyclic group.

Proof: By 2) there is a free $R\pi$-module F with $\mathrm{rank}_R F = \mathrm{rank}_R P$; hence $K \otimes_R F = K \otimes_R P$ if we can show that the number k of occurrences of a simple module M in a Jordan-Hoelder decomposition of $K \otimes_R P$ does only depend on $\mathrm{rank}_R P$. For any $K\pi$-modules A, B, we make $\mathrm{Hom}_K(A,B)$ into a $K\pi$-module setting $x \cdot f = x \circ f \circ x^{-1}$ for $x \in \pi$, $f \in \mathrm{Hom}_K(A,B)$. Let $M^* = \mathrm{Hom}_K(M,K)$, and choose an $R\pi$-module A, torsion free over R, so that $M^* = K \otimes_R A$ (chapter 12, lemma 7.5). We have

$$\sum_{1}^{k} \mathrm{Hom}_{K\pi}(M,M) = \mathrm{Hom}_{K\pi}(M, K \otimes_R P) = (M^* \overset{\pi}{\otimes}_K (K \otimes_R P))^{\pi}$$
$$= K \otimes_R (A \overset{\pi}{\otimes}_R P)^{\pi} \quad \text{by 3).}$$

$A \overset{\pi}{\otimes}_R P$ is projective (chapter 12, lemma 6.6). Hence

$$k \cdot \dim_K \mathrm{Hom}_{K\pi}(M,M) = n^{-1} \cdot \mathrm{rank}_R(A \overset{\pi}{\otimes}_R P) = n^{-1} \cdot \mathrm{rank}_R A \cdot \mathrm{rank}_R P \quad .$$

6) Proof of the Theorem. Let χ be the character defined by $K \otimes_R P$ (chapter 12, proposition 7.4). $\chi(1) = \mathrm{rank}_R P$, and $\chi(x) = 0$ for $x \in \pi$, $x \neq 1$ since $K \otimes_R P$ is free over $K(x)$ by 5). 2) assures the existence of a free $R\pi$-module F such that $\mathrm{rank}_R F = \mathrm{rank}_R P$, so $\chi_{K\otimes F} = \chi_{K\otimes P}$, or

$$K \otimes_R F \cong K \otimes_R P$$

by (chapter 12, theorem 7.3).

Theorem 5.10 now implies:

<u>Theorem 6.2</u>. Suppose R is a Dedekind domain of characteristic 0 , π a finite group, and P a finitely generated projective $R\pi$-module. If no prime dividing the order of π is a unit in R , then P has a decomposition

$$P = F \oplus I \, ,$$

where F is a free $R\pi$-module, and I is an ideal in $R\pi$.