2) Il teor. delle due basi non afferma che tutte le basi di H si ottengono correlandole ad una base di M.

ESEMPIO.

A parte quello appena visto, in cui $\{g_1, g_2\}$ non può essere vista come ottenuta da una base $\{w_1, w_2\}$ di $\mathbb{Z}^2$ scrivendo

$$g_1 = d_1 w_1 \qquad g_2 = d_2 w_2 \qquad (d_1, d_2 \in \mathbb{Z})$$

(perché?)

si consideri $H = \langle (0,2,3), (0,2,1) \rangle \leq \mathbb{Z}^3$.

Mostrare che non esiste una base $\{v_1, v_2, v_3\}$ di $\mathbb{Z}_3$ tale che

$$(0,2,3) = d_1 v_1 \quad \text{e} \quad (0,2,1) = d_2 v_2 \qquad (d_1, d_2 \in \mathbb{Z})$$

Siamo ora interessati a vedere che cosa succede passando al quoziente di A-moduli liberi f.g.

TEOR. 24 Sia A un P.I.D. e M un A-modulo LIBERO con base $\{e_1, \dots, e_s\}$. Siano $d_1, \dots, d_t$ elementi NON NULLI di A con $t \leq s$. Si denoti con H il sottomodulo

$$H = \langle d_1 e_1, \dots, d_t e_t \rangle.$$

Allora

$$\frac{M}{H} = \langle [H+e_1] \rangle \oplus \langle [H+e_2] \rangle \oplus \dots \oplus \langle [H+e_s] \rangle.$$

Inoltre

$$\mathrm{Ann}\,[H+e_i] = \begin{cases} (d_i) & \text{se } i \leq t \\ (0) & \text{se } i > t \end{cases}$$

e quindi

$$\frac{M}{H} \simeq \frac{A}{(d_1)} \oplus \dots \oplus \frac{A}{(d_t)} \oplus A^{s-t}.$$

NOTA: in base al Teor. 23, dato un sottomodulo H dell'A-modulo LIBERO M, è sempre possibile trovare una base di M per la quale la base di H si presenti in questa forma.

DIM. È ovvio che $\frac{M}{H} = \sum_1^s \langle [H+e_i] \rangle$.

Mostro che la somma è diretta usando PROP. D3'. Considero un elem. $a[H+e_i]$ di $\langle [H+e_i] \rangle$: se appartiene a $\sum_{j \neq i} \langle [H+e_j] \rangle$ esistono $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_s$ t.c.

$$a[H+e_i] = \sum_{j \neq i} a_j [H+e_j] \Rightarrow a e_i - \sum_{j \neq i} a_j e_j \in H \Rightarrow$$

$$a e_i - \sum_{j \neq i} a_j e_j = \sum_1^t b_k d_k e_k$$

Poiché $\{e_1, \dots, e_s\}$ è una base,

se $i > t$ si ha $a = 0$

se $i \leq t$ si ha $a = b_i d_i$ e quindi

$$a[H+e_i] = [H + b_i(d_i e_i)] = [H]$$

Quindi in entrambi i casi

$$a[H+e_i] = [H],$$

e quindi la somma è diretta.

Inoltre: $a[H+e_i] = [H]$, cioè $a \in \mathrm{Ann}\,[H+e_i]$ se e solo se

$$a e_i = \sum_{k=1}^t b_k d_k e_k$$

da cui:

se $i > t$ allora $a = 0 \Rightarrow \mathrm{Ann}\,[H+e_i] = (0)$

se $i \leq t$ allora $a = b_i d_i \Rightarrow a \in (d_i) \Rightarrow$

$\Rightarrow \mathrm{Ann}\,[H+e_i] \subseteq (d_i)$

e visto che l'inclusione opposta è ovvia:

$$\mathrm{Ann}\,[H+e_i] = (d_i).$$

Per la PROP. 19, $\langle [H+e_i] \rangle \simeq \frac{A}{\mathrm{Ann}\,[H+e_i]}$ e quindi

$$M \simeq \frac{A}{(d_1)} \oplus \dots \oplus \frac{A}{(d_t)} \oplus \underbrace{A \oplus \dots \oplus A}_{s-t \text{ volte}}$$

c.v.d.

5. A-MODULI FIN. GEN. su un P.I.D.: TEOR. di STRUTTURA

Abbiamo ora gli strumenti per conseguire uno dei nostri obiettivi:

TEOR. 25 (TEOREMA DI STRUTTURA)

Sia A un P.I.D. e M un A-modulo finitamente generato.

Allora M è somma diretta di moduli ciclici.

DIM. Sia $M = \langle m_1, \dots, m_s \rangle$.

1° CASO: $\{m_1, \dots, m_s\}$ LINEARMENTE INDIPENDENTI $\Rightarrow M$ LIBERO

$\Rightarrow$ per la PROP. 12 c) risulta $\boxed{M = \bigoplus_{i=1}^{s} \langle m_i \rangle}$

2° CASO: $\{m_1, \dots, m_s\}$ NON INDIPENDENTI

Sia $\{e_1, \dots, e_s\}$ la BASE STANDARD di A^s: definisco la corrispondenza

$$\sigma(e_i) = m_i \qquad \forall i = 1, \dots, s$$

e la estendo per linearità a un omomorfismo di A-moduli

$$\sigma : A^s \to M$$

che è ovviamente suriettivo, per cui $\frac{A^s}{\ker\sigma} \simeq M$ (pag. 9)

e l'isomorfismo agisce così:

$$[\ker\sigma + v] \mapsto \sigma(v)$$

DIAGRAMMA COMMUTATIVO CORRISPONDENTE:

$$\begin{tikzcd} A^s \arrow[r, "\sigma"] \arrow[dr, "\text{omom. canonico}"'] & M \\ & \frac{A^s}{\ker\sigma} \arrow[u, "\text{isomorfismo}"'] \end{tikzcd}$$

Per il teor. 23 (delle due basi) esistono una base $\{v_1, \dots, v_s\}$ di A^s e t elementi non nulli di A, $d_1, \dots d_t$ tali che $\{d_1 v_1, \dots, d_t v_t\}$ sia una base di $\ker\sigma$.

Per il teor. 24 si ha

$$\frac{A^s}{\ker\sigma} = \bigoplus_{i=1}^{s} \langle [\ker\sigma + v_i] \rangle$$

e per l'isomorfismo:

$$\boxed{M = \langle \sigma(v_1) \rangle \oplus \langle \sigma(v_2) \rangle \oplus \dots \oplus \langle \sigma(v_s) \rangle}$$

e ancora $\quad \mathrm{Ann}\,[\ker\sigma + v_i] = \mathrm{Ann}\,(\sigma(v_i)) = \begin{cases} (d_i) & \text{se } i \le t \\ (0) & \text{se } i > t \end{cases}$

e quindi

$$M \simeq \frac{A}{(d_1)} \oplus \dots \oplus \frac{A}{(d_t)} \oplus A^{s-t}$$

c.v.d.

NOTA 1. Può succedere che qualche $d_i \in A$ sia invertibile. In tal caso $(d_i) = A$ e quindi il corrispondente $\langle \sigma(v_i) \rangle$ è nullo $\Rightarrow$ gli addendi risultano in tal caso meno di s.

NOTA 2. La dimostrazione è conclusa già dove mostrato che M è somma diretta di sottomoduli ciclici ma l'ultima rappresentazione (SOMMA diretta ESTERNA) è più comoda.

OSSERVAZIONE. La scomposizione trovata nel teor. 25 in generale non è unica poiché non è unica la Δ del teor. delle due basi. Ad es. se $N = \begin{pmatrix} 2 & 12 \\ 4 & 3 \end{pmatrix} \in M_{2,2}(\mathbb{Z})$ si può avere

$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} N \begin{pmatrix} 1 & -6 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -21 \end{pmatrix}$$

e anche

$$\begin{pmatrix} 0 & 1 \\ 1 & 10 \end{pmatrix} N \begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 42 \end{pmatrix}$$

Imponendo un vincolo ulteriore nel processo di diagonalizzazione possiamo però ottenere un teorema di unicità:

Premessa:

> TEOR. 22' (Riduzione a forma normale di Smith: enunciato forte). Sia A un P.I.D. e $N \in Mat_{s,t}(A)$. Allora N è equivalente a $\Delta = diag(d_1, \dots, d_n)$, ove $n = min(s,t)$ e $\forall i = 1, \dots, n-1$ si ha
> $$d_i \mid d_{i+1}.$$

La Δ è detta FORMA NORMALE di SMITH di N.
I d_i della forma normale sono detti FATTORI INVARIANTI della matrice N su A e sono univocamente determinati a meno di fattori invertibili di A.

Oss. Gli eventuali d_i invertibili precedono tutti gli altri; gli eventuali d_i nulli seguono tutti gli altri.

Attraverso il teor. 22' possiamo rileggere il teor. di struttura:

TEOR. 25'. Se M è un modulo fin. generato su un P.I.D. A si ha
$$M \simeq \frac{A}{(d_1)} \oplus \dots \oplus \frac{A}{(d_r)} \oplus A \oplus \dots \oplus A$$
ove $\forall i = 1, \dots, r$ si ha $d_i \neq 0$ e non invertibile in A e
$$d_i \mid d_{i+1} \qquad \forall i = 1, \dots, r-1.$$

I d_i sono detti INVARIANTI di TORSIONE di M

Sono univocamente determinati da M:
1) gli annullatori dei sottomoduli del tipo $\frac{A}{(d_i)}$
2) il numero di addendi della scomposizione
3) il rango della componente libera $A \oplus \dots \oplus A$.

Precisiamo il concetto di TORSIONE:

In generale (anche senza l'ipotesi A P.I.D.) valgono le

DEF. 26 Sia M un A-modulo.
Un elemento $m \in M$ è detto ELEMENTO di TORSIONE se esiste $a \in A$, $a \neq 0$ t.c. $am = 0$
cioè se $Ann(m) \neq (0)$
M è detto MODULO di TORSIONE se ogni suo elemento è di torsione.
M è detto PRIVO di TORSIONE se non contiene elem. di torsione diversi da 0.

ESERCIZIO. Sia A un <u>dominio</u> e M un A-modulo. Detto T l'insieme degli elementi di torsione di M provare che
1) T è un sottomodulo di M
2) $\frac{M}{T}$ è privo di torsione

OSSERVAZIONE. Se A è un <u>dominio</u>, allora
a) M A-modulo libero $\Rightarrow$ M privo di torsione (esercizio)
b) esistono A-moduli <u>privi di torsione</u>, ma <u>non liberi</u>.
Esempio: $A = \mathbb{Z}[x]$, $M = \langle 2, x \rangle$ ideale pensato come A-modulo.
Ma:
c) se A è un <u>P.I.D.</u>, M privo di torsione implica M libero poiché vale il teor. di struttura:
$$T \simeq \frac{A}{(d_1)} \oplus \dots \oplus \frac{A}{(d_r)} \quad e \quad M = T \oplus A^{s-t}$$

Caso particolare del teorema di struttura: $A = \mathbb{Z}$,

M gruppo abeliano.

COROLLARIO. Ogni gruppo abeliano finitamente generato (in particolare: finito) è somma diretta di sottogruppi ciclici.

Rileggiamo la dim. del teor. di struttura su un

ESEMPIO. Dato il gruppo abeliano

$$G = \langle m_1, m_2, m_3 \mid m_1 + 2m_2 + 3m_3 = 4m_1 + 5m_2 + 6m_3 = 7m_1 + 8m_2 + 9m_3 = 0 \rangle$$

trovare una scomposizione di G come somma diretta di sottogruppi ciclici

Sol. $\sigma : \mathbb{Z}^3 \to G$ è definita da

$$\sigma(e_1) = m_1$$
$$\sigma(e_2) = m_2$$
$$\sigma(e_3) = m_3$$

Poiché $\sigma(e_1) + 2\sigma(e_2) + 3\sigma(e_3) = 0$ ecc. sugli altri generatori risulta

$$\ker\sigma = \langle g_1, g_2, g_3 \rangle \quad \text{ove} \quad \begin{aligned} g_1 &= e_1 + 2e_2 + 3e_3 \\ g_2 &= 4e_1 + 5e_2 + 6e_3 \\ g_3 &= 7e_1 + 8e_2 + 9e_3 \end{aligned}$$

che si riscrive in forma compatta:

$$\begin{pmatrix} g_1 \\ g_2 \\ g_3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \\ e_3 \end{pmatrix} \qquad N = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$$

Per trovare la forma normale di Smith si possono fare operazioni elementari su righe e colonne (somme di multipli di una R o C ad altre, cambio del segno S di una R o C..) che corrispondono a prodotti per matrici a determinante invertibile!

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \xrightarrow{R} \begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \xrightarrow{C} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix} \longrightarrow$$

$$\xrightarrow{R} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & -6 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{S} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \Delta$$

$\Delta = XNY$ ove X è la matrice delle operazioni sulle righe,
Y " " " " " sulle colonne;

quindi

$$X = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ -7 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ -4 & 1 & 0 \\ 1 & -2 & 1 \end{pmatrix}$$

$$Y = \begin{pmatrix} 1 & -2 & -3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Da $(g_1, g_2, g_3)^T = X^{-1} \Delta Y^{-1} (e_1, e_2, e_3)^T$

ricavo $\underbrace{X(g_1, g_2, g_3)^T}_{(g_1', g_2', g_3')^T} = \Delta \cdot \big[\underbrace{Y^{-1}(e_1, e_2, e_3)^T}_{(v_1, v_2, v_3)^T}\big]$

Poiché $d_1 = 1$, $d_2 = 3$, $d_3 = 0$ si vede che

$$g_1' = v_1, \quad g_2' = 3v_2, \quad g_3' = 0v_3$$

cioè la base di $\ker\sigma$ correlata alla base $\{v_1, v_2, v_3\}$ di $\mathbb{Z}^3$ è $\{v_1, 3v_2\}$.

Poiché

$$Y^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

la nuova base scelta per $\mathbb{Z}^3$ ha la forma

$$\begin{aligned} v_1 &= e_1 + 2e_2 + 3e_3 \\ v_2 &= \quad\;\; - e_2 - 2e_3 \\ v_3 &= \qquad\qquad\;\; e_3 \end{aligned}$$

Per il teor. di struttura

$$G \simeq \frac{\mathbb{Z}^3}{\ker \bar\sigma} = \langle [\ker\bar\sigma + v_1] \rangle \oplus \langle [\ker\bar\sigma + v_2] \rangle \oplus \langle [\ker\bar\sigma + v_3] \rangle$$

$\mathrm{Ann} = (1) = \mathbb{Z}$ $\qquad$ $\mathrm{Ann} = (3)$ $\qquad$ $\mathrm{Ann} = (0)$

quindi

$$G \simeq \frac{\mathbb{Z}}{(3)} \oplus \mathbb{Z} \simeq \mathbb{Z}_3 \oplus \mathbb{Z}.$$

Quindi

$$G = \langle \sigma(v_2) \rangle \oplus \langle \sigma(v_3) \rangle = \langle -m_2 - 2m_3 \rangle \oplus \langle m_3 \rangle =$$
$$= \langle m_2 + 2m_3 \rangle \oplus \langle m_3 \rangle$$

e risulta

$m_2 + 2m_3$ elemento di ordine 3 che genera il sottogruppo di TORSIONE di G, cioè il sottogruppo formato da tutti gli elementi di periodo finito di G;

m_3 elemento di ordine ∞ che genera la componente libera di G.

6. Mod. fin. gen. su un P.I.D.: DECOMPOSIZIONE PRIMARIA

Problema: La scomposizione di M fornita dal teor. di struttura si può raffinare? Cioè: un modulo ciclico H si può scomporre come somma diretta di moduli ciclici più piccoli? La risposta dipenderà da $\mathrm{Ann}\, H$.

LEMMA 27. Sia A un P.I.D. e M un A-modulo. Se $m \in M$ e $\mathrm{Ann}(m) = (ab)$ con $\mathrm{M.C.D}(a,b) = 1$, allora
$$\langle m \rangle = \langle am \rangle \oplus \langle bm \rangle$$
e $\mathrm{Ann}(am) = (b)$, $\mathrm{Ann}(bm) = (a)$.

DIM. Poiché $(a,b) = 1$, $\exists x, y \in A$ t.c. $ax + by = 1 \Rightarrow$

$\Rightarrow m = axm + bym \in \langle am \rangle + \langle bm \rangle$

Quindi $\langle m \rangle = \langle am \rangle + \langle bm \rangle$

Provo che $\langle am \rangle \cap \langle bm \rangle = (0)$:

considero un elemento comune: $cam = dbm \Rightarrow$

$\Rightarrow (ca - db)m = 0$ cioè $ca - db \in \mathrm{Ann}(m) = (ab)$

$\Rightarrow ca - db = kab \Rightarrow (c - kb)a = db$

Dunque $a \mid db$ ma $a \nmid b \Rightarrow a \mid d$, cioè $d = ha$

$\Rightarrow cam = dbm = habm = 0.$

Infine

$r(am) = 0 \iff ra \in \mathrm{Ann}\, m = (ab) \iff r \in (b)$

quindi $\mathrm{Ann}(am) = (b)$.

Similmente $\mathrm{Ann}(bm) = (a)$.

c.v.d.

Ricordo che un P.I.D. è un dominio a fattorizzazione unica, cioè ogni suo elemento non nullo e non invertibile si può scrivere in modo "unico" come prodotto di elem. "irriducibili"

TEOR. 28. Siano A un P.I.D., M un A-modulo e $m \in M$.
Se $Ann(m) = (d)$ e

$$d = p_1^{r_1} p_2^{r_2} \cdot \ldots \cdot p_s^{r_s} \quad (\text{con } p_i \text{ irriducibili distinti e } r_i \neq 0)$$

allora

$$\langle m \rangle = \langle d_1 m \rangle \oplus \langle d_2 m \rangle \oplus \ldots \oplus \langle d_s m \rangle$$

ove $d_i = \dfrac{d}{p_i^{r_i}}$ e $Ann(d_i m) = \left(p_i^{r_i}\right) \quad \forall i = 1, \ldots, s$.

DIM. Posto $a = p_1^{r_1}$ e $b = p_2^{r_2} \cdot \ldots \cdot p_s^{r_s} = d_1$ si ha $(a, b) = 1$

$\Rightarrow$ per il lemma 27: $\langle m \rangle = \langle am \rangle \oplus \langle bm \rangle = \langle am \rangle \oplus \langle d_1 m \rangle$

con $Ann(am) = (b)$

e $Ann(bm) = Ann(d_1 m) = (a) = \left(p_1^{r_1}\right)$

Iterando il procedimento su $\langle am \rangle$ si ha

$$a' = p_2^{r_2}, \quad b' = p_3^{r_3} \cdot \ldots \cdot p_s^{r_s} = \frac{d}{aa'} \quad ; \quad (a', b') = 1$$

$\Rightarrow$ per il lemma 27: $\langle am \rangle = \langle a'am \rangle \oplus \langle b'am \rangle =$
$= \langle a'am \rangle \oplus \langle d_2 m \rangle$

con $Ann(a'am) = (b')$

e $Ann(d_2 m) = (a') = \left(p_2^{r_2}\right)$.

Si itera nuovamente su $\langle a'am \rangle$ scomponendo ulteriormente il suo annullatore e così via finché si esaurisce l'ultimo fattore irriducibile.

c.v.d.

ESEMPIO. Essendo $42 = 2 \cdot 3 \cdot 7$, lo $\mathbb{Z}$-modulo $\mathbb{Z}_{42}$ si può scrivere – per il lemma 27 – come $\langle [2] \rangle \oplus \langle [21] \rangle$ oppure $\langle [3] \rangle \oplus \langle [14] \rangle$ oppure $\langle [6] \rangle \oplus \langle [7] \rangle$, mentre per il teor. 28 si scrive come

$$\langle [6] \rangle \oplus \langle [14] \rangle \oplus \langle [21] \rangle$$

e gli annullatori dei 3 sottogruppi sono rispettivamente (7), (3), (2).

DEF. 29 Si dice PRIMARIO un modulo ciclico $M = \langle m \rangle$ tale che

$$Ann(m) = (p^r) \quad \text{con } p \text{ irriducibile in } A \text{ e } r \geq 1.$$

Tali moduli, insieme a quelli liberi, giocano un ruolo fondamentale per rispondere al problema del possibile raffinamento della scomposizione.

DEF. 30 Un A-modulo M è detto INDECOMPONIBILE se $M \neq (0)$ e se $M = M_1 \oplus M_2$ implica $M_1 = (0)$ oppure $M_2 = (0)$.

Moduli liberi di rango 1 e moduli ciclici primari sono indecomponibili per il seguente:

TEOR. 31 Sia A un P.I.D. e $M = \langle m \rangle$ un A-modulo ciclico tale che

$$Ann(m) = (0) \text{ oppure } Ann(m) = p^r \text{ con } p \text{ irriduc. in } A \text{ e } r \geq 1.$$

Due sottomoduli <u>non nulli</u> di M hanno sempre intersezione $\neq (0)$.

DIM. 1) Sia $\boxed{Ann(m) = (0)} \Rightarrow M \simeq A \Rightarrow$ i suoi sottomoduli sono gli ideali. Per ogni coppia di ideali I, J di A risulta:
$\forall x \in I \setminus (0), \ \forall y \in J \setminus (0) \Rightarrow xy \neq 0$ e $xy \in I \cap J$.

2) Sia $\boxed{Ann(m) = (p^r)}$. Mostro che $p^{r-1} m$ appartiene a ogni sottomodulo N di $\langle m \rangle$.
Sia $am \in N \setminus (0)$: allora $a \notin (p^r)$ e quindi si scompone come

$$a = p^s \cdot q \quad \text{con } q \notin (p) \text{ e } 0 \leq s \leq r-1.$$

Si ha $(p^r, q) = 1$ e quindi $\exists\, x, y \in A$ t.c. $1 = xq + yp^r$

$\Rightarrow m = xqm + yp^r m = xqm \Rightarrow$

$\Rightarrow p^s m = p^s xq m = x(p^s q) m = x(am) \in N$.

Poiché $s \leq r-1$ si ha: $p^{r-1} m \in N$ e $p^{r-1} m \neq 0$, cioè $p^{r-1} m$ <u>è un elem. non nullo contenuto in ogni sottomodulo N di M.</u>

C.V.D.