Sia A un anello, M un A-mod. Se $M = M_1 \oplus M_2$

M_i ~~sotto~~moduli di M.

$$\begin{array}{ccc} M & \longrightarrow & M \\ \| & & \| \\ M_1 \oplus M_2 & \longrightarrow & M_1 \oplus M_2 \\ (x_1, x_2) & \xmapsto{p_1} & (x_1, 0) \\ (x_1, x_2) & \xmapsto{p_2} & (0, x_2) \end{array} \left.\right\} \begin{array}{l} p_1 \text{ morf. di } A\text{-mod.} \\ p_2 \text{ morf. di } A\text{-mod.} \end{array}$$

$$\left.\begin{array}{l} p_1 M = M_1 \\ p_2 M = M_2 \end{array}\right\} \begin{array}{l} p_1 \circ p_2 = 0 \in \mathrm{End}_A M \\ p_2 \cdot p_1 = 0 \in \text{''} \end{array}$$

$$p_1^2 = p_1, \quad p_2^2 = p_2$$

Def. Sia A un anello. Un elemento $e \in A$ è idempotente se

$$e^2 = e.$$

e.g. $0_A, 1_A$ sono idempotenti banale.

$\mathbb{Z}$ non ha alc. idempot. non-ban.

$\mathbb{Z}_6$ ha idempotenti $\overline{3}, \overline{4}$.

$\mathbb{Z}_9$ non ha alc. idempot. non-banal.

Quest. eser: per $n \in \mathbb{N}$,

$\mathbb{Z}_n$ contiene idempotenti non-banale

$\Longleftrightarrow n = ?$

e.g. $$E_i = \begin{array}{c} \begin{pmatrix} 0 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 0 \end{pmatrix} i \\ i \end{array} \in M_n(\mathbb{C})$$

Sono idempot. per $\forall\, 1 \leq i \leq n$.

$\forall\, i \neq j$, $E_i \cdot E_j = 0 = E_j E_i$, $\sum_{i=1}^{n} E_i = I_n$

eser: $X \in M_n(\mathbb{C})$, $X^2 = X \Longleftrightarrow$

X è coniugata a $\sum_{i=1}^{r} E_i$, dove

$r =$ rango di X.

Def.: A un anello,

$\{e_1, \dots, e_n\}$ un sottoins. di A

idempotenti:

per $1 \leq i, j \leq n$, e_i, e_j sono <u>ortogonale</u>

se vale $e_i \cdot e_j = 0 = e_j e_i$.

$\{e_1, \dots, e_n\}$ è <u>completo</u> se

$$\sum_{i=1}^{n} e_i = 1_A .$$

e.g. Sia $e \in A$ un elem. idempotente.

$\Rightarrow$ $1_A - e$ è anche idempotente,

$\Rightarrow$ $\{e, 1_A - e\}$ ins. di idempotenti.

completo e ortogonale.

$$e(1_A - e) = e - e^2 = 0$$

e.g.: $M = M_1 \oplus M_2$, $p_1, p_2 \in \mathrm{End}_A M$

$\{p_1, p_2\}$ insieme idempotente ortogonale e completo:

perché: $p_1 + p_2 = id_M$.

<u>Prop</u>: Sia A un anello, M un A-modulo. allora M è decomponibile come somma diretta di un numero finito di sottomoduli $\iff$ $\exists$ un sottoinsieme finito idempotente di $\mathrm{End}_A M$ che è ortogonal e completo.

<u>Cor</u>: Un A-mod. M è decomponib. $\iff$ $\exists$ un idempotente $e \in \mathrm{End}_A M$.

In tale caso:

$$M = eM \oplus (1-e)M.$$

Dim: (Cor). "$\Rightarrow$" ✓

"$\Leftarrow$": $e \in End_A M$ idempt. non-ban.

$$\forall x \in M, \quad x = (e + 1 - e)x$$
$$= \underset{\underset{eM}{\cap}}{ex} + \underset{\underset{(1-e)M}{\cap}}{\underbrace{(1-e)x}}$$

$$\Rightarrow \quad M = eM + (1-e)M$$

Sia $y \in eM \cap (1-e)M$

$y = ex$ per q.c. $x \in M$

$y = (1-e)x'$, .. $x' \in M$

$$y = ex = e^2x = e(ex) = e\cdot y$$
$$= \underbrace{e\cdot(1-e)}_{0}x' = 0_M$$

$$\Rightarrow M = eM \oplus (1-e)M.$$

//

Eser: dimostrare la prop.

Sia $\{M_i\}_{i \in I}$ una famiglia di sottomod. di un A-mod. M;

$\{M_i\}_{i \in I}$ sono sottomod. <u>indipendente</u>

se $\forall\, i \in I$,

$$M_i \cap \sum_{\substack{\forall j \in I \\ j \neq i}} M_j = \{0\}.$$

* $\{M_i\}_{i \in I}$ è indipendente $\Longleftrightarrow$

$$\sum_{i \in I} M_i = \bigoplus_{\forall i \in I} M_i .$$

Prop: Sia $\{M_i\}_{i \in I}$ una famiglia di sottomod. di M. allora

$$\sum_{\forall i \in I} M_i = \bigoplus_{\forall i \in I} M_i \Longleftrightarrow \text{Per } \forall i \in I.$$

$\exists\, e_i : \sum_{\forall j \in I} M_j \to M_i \subset \sum_{\forall j \in I} M_j$

che è idempotente

e $\{e_i\}_{i \in I}$ ins. ortogonali

Def: Un elem. idempotente $e \in A$ è <u>primitivo</u> se non è una somma di due idempotenti ortogonali non-banale.

e.g. $1 \in \mathbb{Z}$ è primitivo
$\bar{1} \in \mathbb{Z}_6$ Non è primitivo $\bar{1} = \bar{3} + \bar{4}$.
$E_i \in M_n(\mathbb{C})$ è primitivo

Prop: Un A-mod M è decomponibile come una somma diretta di un numero finito di sottomoduli indecomponibile

$\Longleftrightarrow$ $\exists$ un ins. di elem. idempotenti $\{e_i\}_{i=1}^{n}$ in $End_A M$, che è ortogonale, completo e primitivo.

In tale caso:
$M = \bigoplus_{i=1}^{n} e_i M$, dove $e_i M$ è indecomponibile.

e.g. $\left.\begin{array}{l} \mathrm{End}_{\mathbb{Z}}\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z} \\ f \longmapsto f(1) \end{array}\right\}$ isomorf. di anello.

$\Rightarrow$ $\mathrm{End}_{\mathbb{Z}}\mathbb{Z}$ non ha alc. elem. idempotente non-banale

$\Rightarrow$ $\mathbb{Z}$ non si spezz. come $\mathbb{Z}$-mod.

e.g.: p primo. $\mathbb{Z}_{p^r}$, $r \in \mathbb{N}$.

$\left.\begin{array}{l} \mathrm{End}_{\mathbb{Z}}\mathbb{Z}_{p^r} \xrightarrow{\varphi} \mathbb{Z}_{p^r} \\ f \longmapsto f(\bar{1}) \end{array}\right\}$ morf. di anello

$$\mathrm{End}_{\mathbb{Z}}\mathbb{Z}_{p^r} \xleftarrow{\psi} \mathbb{Z}_{p^r}$$

$$\psi(\bar{a}) \longleftarrow\!\shortmid\ \bar{a} \qquad \forall \bar{a} \in \mathbb{Z}_{p^r}$$

ben-def. $\left\{\begin{array}{l} \mathbb{Z}_{p^r} \to \mathbb{Z}_{p^r} \\ \bar{1} \longmapsto \bar{a} \end{array}\right.$

$\varphi \circ \psi = id$, $\psi \circ \varphi = id$ $\Rightarrow$ φ isomorf.

Se $\overline{a} \in \mathbb{Z}_{p^r}$ è idempotente, $0 < a < p^r$
$a \in \mathbb{N}$:

$$\overline{a}^2 = \overline{a} \Rightarrow \underbrace{\overline{a}(\overline{a} - \overline{1})}_{\overline{a(a-1)}} = \overline{0} \in \mathbb{Z}_{p^r}$$

$\Rightarrow p^r \mid a(a-1)$

a e $a-1$ sono coprimi

$\Rightarrow p^r \mid a$ opp. $p^r \mid (a-1)$

$\Rightarrow$ contrad. $\Rightarrow$

$\mathbb{Z}_{p^r}$ non ha alc. elem. idempotente non-banale.

$\Rightarrow \mathbb{Z}_{p^r}$ non si spezz. come somma diretta dei sottomoduli.