1

Capitolo T25
teoria dei moduli

Contenuti delle sezioni

18 pagine

T250.01 Questo capitolo riprende la nozione di modulo su anello per presentare con una certa ampiezza le loro prime proprietà.

In particolare sono esaminate le proprietà che sono utilizzate per lo studio delle trasformazioni lineari degli spazi vettoriali e quindi per giungere ad alcuni risultati baslari per l'algebra lineare.

T25 a. moduli su anelli, sottomoduli e somme dirette

T25a.01 Consideriamo l'anello.u $\boldsymbol{R}=\langle R,+,-,0,\cdot,1\rangle$; si dice **modulo a sinistra** su $\boldsymbol{R}$ una struttura della forma $\boldsymbol{M}=\langle M,\boldsymbol{R},\boldsymbol{+},\boldsymbol{-},\boldsymbol{0},{}_{\perp}\rangle$ dove $\langle M,\boldsymbol{+},\boldsymbol{-},\boldsymbol{0}\rangle$ è un gruppo abeliano, mentre com ${}_{\perp}$ abbiamo denotata [T16a01] una cosiddetta **legge di composizione esterna** per la quale chiediamo che sia del genere ${}_{\perp}\in\lceil R\times M\longmapsto M\rceil$ e che valgano le proprietà

$$\forall a,b\in R,\quad \forall \boldsymbol{v},\boldsymbol{w}\in M\ :\ a{}_{\perp}(\boldsymbol{v}\boldsymbol{+}\boldsymbol{w})=(a{}_{\perp}\boldsymbol{v})\boldsymbol{+}(a{}_{\perp}\boldsymbol{w})\ ,\qquad (a+b){}_{\perp}\boldsymbol{v}=(a{}_{\perp}\boldsymbol{v})\boldsymbol{+}(b{}_{\perp}\boldsymbol{v})\ ,$$
$$(a\cdot b){}_{\perp}\boldsymbol{v}=a{}_{\perp}(b{}_{\perp}\boldsymbol{v})\ ,\qquad 1{}_{\perp}\boldsymbol{v}=\boldsymbol{v}\ .$$

Denotiamo con $\mathsf{Mdl}_{\boldsymbol{R}}$ la classe dei moduli a sinistra sull'anello $\boldsymbol{R}$ e con $\mathsf{Mdl}_{\mathsf{RngU}}$ la classe dei moduli a sinistra sugli anelli.u .

Discutendo di un modulo su anello $\boldsymbol{R}$, usualmente gli elementi di R vengono chiamati scalari e la legge di composizione esterna viene detta **moltiplicazione per uno scalare**.

T25a.02 Dualmente-LR si dice **modulo a destra** su $\boldsymbol{R}$ una struttura della forma $\boldsymbol{M}=\langle M,\boldsymbol{R},\boldsymbol{+},\boldsymbol{-},\boldsymbol{0},{}_{\perp}\rangle$ dove $\langle M,\boldsymbol{+},\boldsymbol{-},\boldsymbol{0}\rangle$ è un gruppo abeliano, mentre ${}_{\perp}$ denota una legge di composizione esterna per la quale si chiedono il genere ${}_{\perp}\in\lceil M\times R\longmapsto M\rceil$ e le proprietà

$$\forall a,b\in R,\quad \forall \boldsymbol{v},\boldsymbol{w}\in M\ :\ (\boldsymbol{v}\boldsymbol{+}\boldsymbol{w}){}_{\perp}a=(\boldsymbol{v}{}_{\perp}a)\boldsymbol{+}(\boldsymbol{w}{}_{\perp}a)\ ,\qquad \boldsymbol{v}{}_{\perp}(a+b)=(\boldsymbol{v}{}_{\perp}a)\boldsymbol{+}(\boldsymbol{v}{}_{\perp}b)\ ,$$
$$\boldsymbol{v}{}_{\perp}(a\cdot b)=(\boldsymbol{v}{}_{\perp}a){}_{\perp}b\ ,\qquad \boldsymbol{v}{}_{\perp}1=\boldsymbol{v}\ .$$

Denotiamo con $\mathsf{Mdlrt}_{\boldsymbol{R}}$ la classe dei moduli a destra sull'anello $\boldsymbol{R}$ e con $\mathsf{Mdlrt}_{\mathsf{RngU}}$ la classe dei moduli a destra su un qualsiasi anello.u . Le notazioni duali-LR sono $\mathsf{Mdlrt}_{\boldsymbol{R}}$ e $\mathsf{Mdlrt}_{\mathsf{RngU}}$

La distinzione tra moduli a sinistra e moduli a destra ha interesse solo per gli anelli noncommutativi. Se RBi è un anello commutativo tutte le proprietà di un modulo a sinistra si trasformano in proprietà di un modulo a destra mediante semplici trasformazioni formali come la trasformazione dell'espressione $(r\cdot s){}_{\perp}\mathsf{v}$ nella $\mathsf{v}{}_{\perp}(s\cdot r)$.

T25a.03 Conviene distinguere vari tipi di moduli su anelli.u in relazione ai tipi degli anelli.u utilizzati: infatti con diversi tipi di anelli.u si hanno moduli con proprietà anche molto diverse e di conseguenza finalizzati a utilizzi differenti.
Naturalmente quando si utilizzano anelli.u dotati di proprietà più incisive si hanno moduli con proprietà più stringenti che possono costituire strumenti più efficaci e talora con applicazioni più complete.

In particolare gli spazi vettoriali in quanto moduli su un campo, si possono considerare strutture di una specie più ricca e più specifica dei più generici moduli su anello.u, in quanto un campo può considerarsi un arricchimento di un anello.u commutativo; in effetti gli spazi vettoriali sono strutture particolarmente efficaci e ampiamente utilizzate.

Tra i moduli su anello si distinguono innanzi tutto i moduli su anelli commutativi e dotati di unità, in quanto godono di proprietà che ne fanno degli strumenti più efficaci.
Prevedibilmente denotiamo la loro collezione con $\mathsf{Mdl}_{\mathsf{RngUAb}}$.

Tra questi ultimi si distinguono i moduli su domini di integrità; la loro collezione la denotiamo con Mdl_{Intdmn}.
Anche queste specie di strutture sono comunque meno utilizzabili e molto meno utilizzate degli spazi vettoriali.

T25a.04 Per un primo esempio di modulo su anello.u consideriamo un intero positivo d, l'anello.u $\boldsymbol{R}$ e l'insieme delle sequenze di lunghezza d di elementi del supporto R, $R^d = \lceil (\mathrm{d}\,] \longmapsto R \rceil$.
Se $\boldsymbol{v} = \langle v_1, ..., v_d \rangle$ e $\boldsymbol{w} = \langle w_1, ..., w_d \rangle$ sono due elementi di tale insieme, consideriamo la **somma termine a termine** di $\boldsymbol{v}$ e $\boldsymbol{w}$ $\boldsymbol{v}\mathbf{+}\boldsymbol{w} := \langle v_1 + w_1, ..., v_d + w_d \rangle$, il passaggio alla sequenza opposta di $\boldsymbol{v}$ $-\boldsymbol{v} := \langle -v_1, ..., -v_d \rangle$ e il **vettore nullo** $0^{seq_d} := \langle 0, ..., 0 \rangle \in R^d$ che contrassegnamo anche con $\mathbf{0}$.

Come si è già notato parlando di prodotti diretti di gruppi, $\langle R^d, \mathbf{+}, \mathbf{-}, \mathbf{0} \rangle$ costituisce un gruppo abeliano.

Considerando anche il prodotto esterno definito ponendo $\forall a \in R \ : \ a \mathbin{\perp} \boldsymbol{v} := \langle a \cdot v_1, ..., a \cdot v_d \rangle$. si verifica che $\langle R^d, \boldsymbol{R}, \mathbf{+}, \mathbf{-}, \mathbf{0}, \mathbin{\perp} \rangle$ costituisce un modulo a sinistra.
Esso si chiama **modulo delle sequenze su** R **di dimensione** d e si denota con $\mathbf{Mdl}_{\boldsymbol{R},d}$.

Ricordiamo che se al posto di un anello.u si ha un campo $\boldsymbol{F}$ si ottiene lo spazio vettoriale chiamato **spazio vettoriale delle sequenze sul campo di dimensione** d.

T25a.05 Una rilevante generalizzazione della precedente costruzione si ottiene considerando un insieme qualsiasi X e basandosi sull'anello delle funzioni $\lceil X \longmapsto F \rceil$.
Munendo tale insieme dell'operazione binaria di somma di funzioni, dell'operazione di passaggio alla funzione opposta e dell'operazione nullaria $0^{fun_X} := \lceil x \in X \mapsto 0 \rceil$, cioè della funzione che assume il valore costante 0 per ogni elemento di X, si ottiene un gruppo abeliano.

Sopra questo terreno $\lceil X \longmapsto F \rceil$ possiamo definire anche il prodotto esterno

$$\mathbin{\perp} := {}^{.act f_X} := \left\lceil a \in F \ , \ f \in \lceil X \longmapsto F \rceil \quad \mapsto \quad \lceil x \in X \mapsto a \cdot f(x) \rceil \right\rceil .$$

Si verifica che $\left\langle \lceil X \longmapsto F \rceil, \boldsymbol{F}, \mathbf{+}, \mathbf{-}, \mathbf{0}, \mathbin{\perp} \right\rangle$ è un modulo su $\boldsymbol{R}$, detto **modulo delle funzioni** da X nell'anello.u $\boldsymbol{F}$.

Troveremo utile prendere in considerazione, come varianti dei moduli di sequenze finite, i moduli costruiti sull'anello delle matrici di un profilo $d \times e$, con d ed e interi positivi qualsiasi, le cui entrate sono elementi di un anello $\boldsymbol{R}$.
Per un tale anello di matrici la somma è la somma entrata per entrata e il prodotto è il prodotto righe per colonne che si serve delle due operazioni binarie di $\boldsymbol{R}$.

T25a.06 Un gruppo abeliano $\boldsymbol{G} = \langle G, \mathbf{+}, \mathbf{-}, \mathbf{0} \rangle$ può essere arricchito e promosso a modulo sull'anello.u degli interi, cioè diventare elemento di $\mathbf{Mdl}_{\mathbb{Z}}$, in un modo unico.
Per ogni $x \in G$ e per ogni $n \in \mathbb{P}$ si definisce $n \mathbin{\perp} x$ come la somma di n repliche dell'elemento x; inoltre si pone $0 \mathbin{\perp} x := \mathbf{0}$ e $(-n) \mathbin{\perp} x := \mathbf{-}(n \mathbin{\perp} x)$.

Da ogni anello.u commutativo $\boldsymbol{R} = \langle R, +, -, 0, \cdot, 1 \rangle$ si ottiene un modulo sullo stesso $\boldsymbol{R}$ avente R come primo e secondo terreno e come moltiplicazione per lo scalare $s \in R$ del vettore $v \in R$ il semplic3e prodotto $s \cdot v$. Questo modulo lo chiamiamo **modulo anello-anello** su $\boldsymbol{R}$ e lo denotiamo con $\mathbf{MdlRR}(\boldsymbol{R})$. Formalmente

$$\mathbf{MdlRR}_{\boldsymbol{R}} := \langle R, \boldsymbol{R}, +, -, 0, \cdot \rangle .$$

Più in generale, dato un anello.u commutativo $\boldsymbol{R} = \langle R, +, -, 0, \cdot, 1 \rangle$ ed un $I \subseteq R$ che costituisce il terreno di un suo ideale (bilatero), si definisce **modulo anello-ideale** su $\boldsymbol{R}$ associato a I il modulo su $\boldsymbol{R}$ avente I come primo terreno e come moltiplicazione per lo scalare $s \in R$ del vettore $\mathbf{v} \in I$ il semplice prodotto $s \cdot \mathbf{v}$. In formula

$$\mathbf{MdlRRI}_{\boldsymbol{R},I} := \langle S, \boldsymbol{R}, +, -, 0, \cdot \rangle .$$

Per questi moduli su anelli commutativi risulta particolarmente evidente la sostanziale equivalenza di modulo a sinistra e modulo a destra. Per porre in rilievo questa equivalenza queste strutture sono anche chiamate **moduli bilateri**.

T25a.07 Consideriamo ancor più in generale un anello.u noncommutativo $\boldsymbol{R}$. Se esso è dotato di un ideale sinistro I si definisce come **modulo anello-ideale sinistro** su $\boldsymbol{R}$ ed I il modulo

$$\big\langle I, \boldsymbol{R}, +, -, 0, \cdot \big\rangle \ .$$

Dualmente-LR, se $\boldsymbol{R}$ possiede un ideale destro J si dice **modulo anello-ideale destro** su $\boldsymbol{R}$ e J il modulo

$$\big\langle J, \boldsymbol{R}, +, -, 0, \cdot \big\rangle \ .$$

T25a.08 Introduciamo la nozione di sottostruttura per i moduli su anello.
Si dice **sottomodulo di un modulo a sinistra** $\boldsymbol{M} = \big\langle M, \boldsymbol{R}, \mathbf{+}, \mathbf{-}, \mathbf{0}, {}^{\perp} \big\rangle$ ogni

$$\big\langle S, \boldsymbol{F}, \mathbf{+}|_{S\times S}, \mathbf{-}|_{S\times S}, \mathbf{0}, {}^{\perp}|_{\boldsymbol{F}\times S} \big\rangle \in \mathbf{Vsp}_F \ , \text{ ove } S \subseteq V \ .$$

In parole povere un sottomodulo di un modulo $\boldsymbol{M}$ è un suo sottoinsieme che, munito delle restrizioni delle operazioni definite per il modulo, costituisce esso stesso un modulo (a sinistra).

Questo equivale a chiedere che S sia chiuso rispetto alle operazioni $\mathbf{+}$ e $\mathbf{-}$, che contenga $\mathbf{0}$ e che sia stabile rispetto alla moltiplicazione per qualsiasi elemento dell'anello.

Questo sottomodulo si denota con $\boldsymbol{M}|_S$.

Equivalentemente si trova che S è sottomodulo di $\boldsymbol{V}$ sse $\forall a, b \in \boldsymbol{F}$ e $\forall \mathbf{v}, \mathbf{w} \in \boldsymbol{V}$: $a {}^{\perp}\mathbf{v} + b {}^{\perp}\mathbf{w} \in S$.

Similmente si tratta la nozione di **sottomodulo a destra**.

T25a.09 Denotiamo con $\boldsymbol{SbMdl}(\boldsymbol{M})$ l'insieme dei sottomoduli del modulo $\boldsymbol{M}$. In questo insieme si trovano, in particolare, il **sottomodulo zero** avente come terreno $\{\mathbf{0}\}$ e l'intero $\boldsymbol{M}$ (con il ruolo di sottomodulo improprio); i sottomoduli rimanenti si dicono **sottomoduli propri nonnulli**.

Per enunciare che $\boldsymbol{N}$ è, risp., sottomodulo e sottomodulo proprio del modulo $\boldsymbol{M}$ scriviamo $\boldsymbol{N} \leq_{Mdl} \boldsymbol{M}$ e $\boldsymbol{N} <_{Mdl} \boldsymbol{M}$.

Per un qualsiasi $\boldsymbol{M} \in \mathbf{Mdl}$ e per ogni suo vettore $\mathbf{v}$ nonnullo l'insieme di vettori $\{a \in R :| \ a {}^{\perp}\mathbf{v}\}$ sottende un sottomodulo che in breve può denotarsi con $R {}^{\perp}\mathbf{v}$ o, quando i può sottintendere $\boldsymbol{R}$, con $\boldsymbol{span}(\mathbf{v})$.
Questo sottospazio si chiama anche **raggio del vettore** $\boldsymbol{V}$, (*array*).

T25a.10 **(1) Prop.**: Un sottoinsieme S del terreno M di un modulo $\boldsymbol{M}$ sull'anello.u $\boldsymbol{R}$ è terreno di un sottomodulo di $\boldsymbol{M}$ sse

$$\forall r_1, r_2 \in R \ , \ \mathbf{v}_1, \mathbf{v}_2 \in M \ : \ r_1 \mathbf{v}_1 + r_2 \mathbf{v}_2 \in S \ \blacksquare$$

(2) Prop.: Consideriamo un anello.u commutativo $\boldsymbol{R}$ e il modulo $\mathbf{MdlRR}(\boldsymbol{R})$. I suoi sottomoduli sono ottenuti precisamente dagli ideali (bilateri) di $\boldsymbol{R}$ $\blacksquare$

T25a.11 $\boldsymbol{SbMdl}(\boldsymbol{M})$, come ogni collezione di sottostrutture di una data struttura, è ordinato parzialmente dall'inclusione.

(1) Prop.: Se S e T sono terreni di sottomoduli di $\boldsymbol{M}$, lo è anche $S \cap T$; più precisamente questo è il più esteso dei sottomoduli contenuti sia in S che in T $\blacksquare$

T25a.12 Viceversa, come nel caso degli spazi vettoriali, per un modulo generico e per due suoi sottoinsiemi qualsiasi S e T può accadere che il sottoinsieme $S \cup T$ non sia sottomodulo di $\boldsymbol{V}$.

(1) Prop.: $S \cup T$ è sottomodulo di $\boldsymbol{V}$ sse $S \subseteq T$ oppure $T \subseteq S$ ∎

T25a.13 Si dice **somma diretta dei sottomoduli** S e T del modulo $\boldsymbol{M}$ sull'anello $\boldsymbol{R}$ l'insieme

$$S \mathbf{+}^{be} T := \{\mathsf{v} \in S,\ \mathsf{w} \in T :|\ \mathsf{v}\mathbf{+}\mathsf{w}\} .$$

Evidentemente la comutatività della somma degli anelli implica che $S \mathbf{+}^{be} T = T \mathbf{+}_{\mathsf{B}} S$. **(1) Prop.**: $S \mathbf{+}^{be} T$ è un sottomodulo di $\boldsymbol{M}$ e, più precisamente, è il più ridotto sottomodulo il cui terreno contiene $S \cup T$.

Abbiamo quindi che $\boldsymbol{Sbvsp}(\boldsymbol{M})$ è un insieme ordinato, reticolato dall'inclusione e che $\langle \boldsymbol{SbMdl}(\boldsymbol{M}), \cap, \mathbf{+}^{be} \rangle$ è un reticolo dotato di minimo ($\{\mathbf{0}\}$) e di massimo (M). Esso si dice **reticolo dei sottomoduli del modulo** $\boldsymbol{M}$.

Va segnalato che per l'operatore binario somma diretta di solito viene usato, non il segno $\mathbf{+}^{be}$, ma il segno $\oplus$. Così faremo qui di seguito, ossia poniamo $\oplus := \mathbf{+}^{be}$.

T25a.14 Più in generale si può cercare la decomposizione di un modulo su un anello.u $\boldsymbol{R}$ come somma diretta di una famiglia qualsiasi, finita o infinita, di moduli su $\boldsymbol{R}$.

Qui ci limitiamo a presentare la decomposizione fornita da una sequenza finita di moduli nonnulli $\langle \boldsymbol{S}_1, \boldsymbol{S}_2, ..., \boldsymbol{S}_n \rangle$, con $n = 2, 3, ...$

Scriviamo

$$\boldsymbol{M} = \boldsymbol{S}_1 \oplus \boldsymbol{S}_2 \oplus ... \oplus \boldsymbol{S}_n$$

sse ogni $\mathsf{v} \in M$ si può esprimere in un solo modo come

$$\mathsf{v} = \mathsf{s}_1 \mathbf{+} \mathsf{s}_2 \mathbf{+} \cdots \mathbf{+} \mathsf{s}_n \quad \text{ove} \quad \forall i = 1, 2, ..., n : \mathsf{s}_i \in S_i .$$

L'unicità della decomposizione si esplicita affermando che se si trova un'espressione

$$\mathsf{v} = \mathsf{t}_1 \mathbf{+} \mathsf{t}_2 \mathbf{+} \cdots \mathbf{+} \mathsf{t}_n \quad \text{ove} \quad \forall i = 1, 2, ..., n : \mathsf{t}_i \in S_i ,$$

allora deve essere $\forall i = 1, 2..., n : \mathsf{t}_i = \mathsf{s}_1$.

Gli $\boldsymbol{S}_i$ sono sottomoduli di $\boldsymbol{M}$ e sono detti **sommandi diretti per il modulo** $\boldsymbol{M}$.

(1) Prop.: Due diversi sommandi diretti possono avere in comune solo il vettore nullo di $\boldsymbol{M}$.

Dim.: In caso contrario cadrebbe l'unicità della decomposizione diretta ∎

Abbiamo quindi la seguente caratterizzazione della decomposizione diretta mediante una sequenza finita di sottomoduli.

(2) Prop.: Un modulo $\boldsymbol{M}$ sull'anello.u $\boldsymbol{R}$ è decomponibile come somma diretta di una sequenza di n sottomoduli nonnulli $\langle \boldsymbol{S}_1, \boldsymbol{S}_2, ..., \boldsymbol{S}_n \rangle$ sse

(a) $M = S_1 \dot{+}^{be} S_2 \dot{+}^{be} \cdots \dot{+}^{be} S_n$;

(b) $\forall i = 1, 2..., n : S_i \cap \bigoplus_{j \in (\mathrm{n}\,]\setminus\{i\}} S_j = \{\mathbf{0}\}$.

T25a.15 Consideriamo i moduli $\boldsymbol{S}$ e $\boldsymbol{T}$ tali che $S \cap T = \{\mathbf{0}\}$ e la loro somma diretta $\boldsymbol{V} := \boldsymbol{S} \mathbf{+}_{\mathsf{B}} \boldsymbol{T}$. $\boldsymbol{T}$ è chiamato **sottomodulo complemento** di $\boldsymbol{S}$ in $\boldsymbol{V}$. Per simmetria anche $\boldsymbol{S}$ ha il ruolo di sottomodulo complemento di $\boldsymbol{T}$ in $\boldsymbol{V}$. La complementarietà tra sottomoduli è evidentemente una relazione simmetrica e antiriflessiva.

Mentre ogni sottospazio proprio di uno spazio vettoriale possiede un sottospazio complementare (in genere più di uno), vi sono moduli su anelli.u che non sono campi per i quali questo non accade.

(1) Prop.: Consideriamo il modulo $\mathsf{MdlRR}(\mathbb{Z})$ sull'anello.u $\mathbb{Z}_{Fld}$; nessuno dei suoi sottomoduli possiede complementare.

Dim.: La collezione dei sottomoduli propri nonnulli di $\mathsf{MdlRR}(\mathbb{Z})$ [a06] è ottenuta precisamente dagli ideali propri (bilateri) di $\mathbb{Z}_{Fld}$ aventi la forma $n\,\mathbb{Z}$ per $n = 2, 3, ...$
Ciascun duetto di questi insiemi di interi ha come intersezione un altro ideale proprio nonnullo di $\mathbb{Z}_{Fld}$: $n\,\mathbb{Z} \cap k\,\mathbb{Z} = \mathrm{mcm}(n,k)\,\mathbb{Z}$. La a15(1) implica che $\mathsf{MdlRR}(\mathbb{Z})$ non è decomponibile in due o più sottomoduli e quindi l'enunciato ∎

T25a.16 Se E è un sottoinsieme di M, si scrive $\boldsymbol{span_R}(E)$ per denotare l'insieme delle combinazioni lineari dei vettori di E. In formula:

$$\boldsymbol{span_R}(E) \;:=\; \{h \in \mathbb{P}\ ,\ a_1, ...a_h \in R\ ,\ \mathsf{v}_1, ..., \mathsf{v}_h \in R :|\ a_1\,\mathsf{v}_1 + \cdots + a_h\,\mathsf{v}_h\}\ .$$

Un tale sottoinsieme di M costituisce un sottomodulo di $\boldsymbol{M}$.

Se $\boldsymbol{N}$ è sottomodulo di $\boldsymbol{M}$ e G è sottoinsieme di N; si dice che G genera o sottende (o anche "spanna") $\boldsymbol{N}$ mediante $\boldsymbol{R}$ sse $N = \boldsymbol{span_R}(E)$, cioè sse ogni $\mathsf{v} \in N$ si può individuare con una espressione della forma $\mathsf{v} = r_1\,\mathbf{g}_1 + \cdots + r_d\,\mathbf{g}_d$ per qualche intero positivo d, per qualche sequenza $\langle r_1, ...,_d \rangle$ di scalari e per qualche sequenza $\langle \mathbf{g}_1, ..., \mathbf{g}_d \rangle$ di vettori di E.
Quando $\boldsymbol{R}$ si può sottintendere si dice anche che E è **sottoinsieme generatore di un sottomodulo** o **spanning set di un sottomodulo** di $\boldsymbol{N}$.

Un modulo $\boldsymbol{M}$ su $\boldsymbol{R}$ si dice **modulo finitamente generato** sse contiene un insieme finito di vettori G che lo genera.

Un sottomodulo di un $\boldsymbol{M}$ che può essere generato da un solo vettore, cioè che si può espriere mediante un suo vettore $\mathbf{g}$ con la formula $R\,\mathbf{g}$, viene chiamato **sottomodulo ciclico generato da un vettore $\mathbf{g}$**.

Ricordiamo che uno spazio vettoriale è finitamente generato sse possiede una base finita, cioè sse ha dimensione finita.
Vi sono invece moduli per i quali le due proprietà precedenti non sono equivalenti. Vediamo a questo proposito un esempio di modulo finitamente generato che presenta sottomoduli non finitamente generati.

Sia $\boldsymbol{P}$ l'anello.u dei polinomi sopra un campo $\boldsymbol{F}$ in una successione infinita di variabili $\langle x_1, x_2, ..., x_n, ... \rangle$.
Per trattare questo anello.u conviene denotare sinteticamente la successione delle variabili con una scrittura di stile vettoriale come $\boldsymbol{x}$ e denotare il suddetto insieme di polinomi con $\boldsymbol{F[x]}$.
Il modulo anello-anello ottenuto come $\mathsf{MdlRR}(\boldsymbol{F[x]})$ è finitamente generato in quanto si può ottenere come $\boldsymbol{span_P}(1_{\boldsymbol{F}})$, dove con $1_{\boldsymbol{F}}$ denotiamo l'elemento unità di $\boldsymbol{F}$ e il polinomio che si riduce a tale termine costante e che costituisce l'unità di $\boldsymbol{R}$, due entità tanto collegate da potersi trattare come coincidenti.

Adottiamo la notazione $\boldsymbol{F_{>0}[x]}$ per esprimere l'insieme dei polinomi nelle variabili componenti di $\boldsymbol{x}$ con il termine costante nullo. Questo insieme è terreno di un sottomodulo di $\mathsf{MdlRR}(\boldsymbol{F[x]})$ per il quale scriviamo $\boldsymbol{S} := \mathsf{MdlRR}\Big(\boldsymbol{F_{>0}[x]}\Big)$; infatti $p(\boldsymbol{x}) \in \boldsymbol{F[x]}$ e $q(\boldsymbol{x}) \in \boldsymbol{F_{>0}[x]}$ implicano $p(\boldsymbol{x})\,q(\boldsymbol{x}) \in \boldsymbol{F_{>0}[x]}$. Il sottomodulo $\boldsymbol{S}$ è generato dal suo sottoinsieme dei polinomi forniti dalle semplici variabili $x_1, x_2, ...$

Dimostriamo ora che $\boldsymbol{S}$ non è finitamente generato. Procedendo per assurdo supponiamo che esista un insieme di polinomi $\{p_1(\boldsymbol{x}), ..., p_m(\boldsymbol{x})\}$ in grado di generare finitamente $\boldsymbol{S}$.
In tal caso per ogni $k \in \mathbb{P}$ esiste una m-upla di polinomi $\langle b_{k,1}(\boldsymbol{x}), ..., b_{k,m}(\boldsymbol{x}) \rangle$ tale che

$$x_k = \sum_{i=1}^{m} b_{k,i}\,p_i(\boldsymbol{x})\ . \tag{1}$$

Si osserva che ciascuno degli addendi a secondo membro ha termine costante nullo.

Denotiamo con V l'insieme finito delle variabili x_h che compaiono nei precedenti polinomi p_i. Se per l'uguaglianza precedente scegliamo $x_k \notin V$, possiamo scrivere

$$b_{k,i} \;=\; x_k\, q_i(\boldsymbol{x}) + r_i(\boldsymbol{x}) \;, \tag{2}$$

dove $q_i(\boldsymbol{x})$ è un opportuno polinomio in $\boldsymbol{F[x]}$, mentre $r_i(\boldsymbol{x})$ non coinvolge la variabile x_k.
Le espressioni (1) e (2) implicano

$$x_k = x_k \sum_{i=1}^{n} q_i(\boldsymbol{x})\, p_i(\boldsymbol{x}) + \sum_{i=1}^{n} r_i(\boldsymbol{x})\, p_i(\boldsymbol{x}) \;.$$

La seconda sommatoria non coinvolge la variabile x_k e quindi vale 0; deve quindi essere $\displaystyle\sum_{i=1}^{n} q_i(\boldsymbol{x})\, p_i(\boldsymbol{x}) = 1$, ma questo non può verificarsi in quanto i $p_i(\boldsymbol{x})$ hanno il termine costante nullo. Dunque $\boldsymbol{S}$ non è finitamente generabile ∎

T25 b. moduli: indipendenza lineare, basi, morfismi

T25b.01 Introduciamo ora per i moduli le nozioni di insiemi di vettori linearmente indipendenti e insiemi di vettori linearmente dipendenti: vedremo che per questi argomenti i moduli per alcuni aspetti sono vicini agli spazi vettoriali, mentre per altri sono ben diversi.

Un insieme di vettori I di $\boldsymbol{M}$ si dice **insieme di vettori linearmente indipendenti** sse per ogni $\{\mathsf{v}_1, ..., \mathsf{v}_h\} \subseteq I$ e per ogni scelta di scalari loro associati c_1, ..., c_h si ha:

$$a_1 \,\mathsf{v}_1 \boldsymbol{+} \cdots \boldsymbol{+} a_h \,\mathsf{v}_h = \mathbf{0} \implies a_1 = \cdots = a_h = 0 \ .$$

Se non vi sono ambiguità un insieme di vettori linearmente indipendenti viene chiamato semplicemente **insieme indipendente**.
Un insieme di vettori che non è linearmente indipendente viene detto **insieme di vettori linearmente dipendenti** o, concisamente, **insieme dipendente**.

T25b.02 Dalla definizione segue che ogni sottoinsieme di un insieme di vettori linearmente indipendenti è a sua volta un insieme di vettori linearmente indipendenti. Quindi tra gli insiemi indipendenti hanno maggiore interesse quelli più estesi.
Viceversa tra gli insiemi dipendenti hanno maggiore interesse quelli meno estesi.

Mentre in uno spazio vettoriale ogni insieme costituito da un solo vettore è un insieme indipendente, questo può non accadere in un modulo.

Consideriamo il modulo su $\mathbb{Z}_{n;Rng}$ avente come supporto $\mathbb{Z}_n$, insieme delle classi di resti modulo n, per qualche $n \in \mathbb{P}$ e per il quale la moltiplicazione per uno scalare è definita ponendo

$$\forall z \in \mathbb{Z} \ , \ a \in \mathbb{Z}_n \ : \ z \mathbin{\perp} a = z \cdot_n a \ .$$

Dato che per ogni $a \in \mathbb{Z}_n \ n \cdot_n a = 0_n$ nessun insieme costituito da un solo elemento di questo modulo è linearmente indipendente.

T25b.03 Mentre in uno spazio vettoriale un insieme di vettori è linearmente dipendente sse ogni suo elemento si può esprimere come combinazione lineare dei vettori rimanenti, in alcuni moduli si trovano insiemi di vettori linearmente dipendenti contenenti elementi non esprimibili come combinazioni lineari dei rimanenti.

Per questa situazione consideriamo il modulo sull'anello.u $\mathbb{Z}_{Rng}$ avente come terreno $\mathbb{Z} \times \mathbb{Z}$ per il quale la moltiplicazione per uno scalare è definita ponendo

$$\forall z \in \mathbb{Z} \ , \ \langle a, b\rangle \in \mathbb{Z} \times \mathbb{Z} \ : \ z \mathbin{\perp} \langle a, b\rangle \ := \big\langle z\, a, z\, b\big\rangle \ .$$

Per ogni duetto di interi coprimi $\{p, q\}$ i due vettori del modulo $\big\langle p, 0\big\rangle$ e $\big\langle q, 0\big\rangle$ sono linearmente dipendenti in quanto $q\big\langle p, 0\big\rangle - p\big\langle q, 0\big\rangle = \langle 0, 0\rangle$. accade inoltre che nessuna delle due coppie è una combinazione lineare, cioè un multiplo, dell'altra.

Questa incapacità di esprimere un vettore di un insieme dipendente mediante combinazione lineare dei restanti è strettamente collegata alla incapacità di trovare nell'anello degli scalari il reciproco di qualche elemento. Per esempio se si hanno le relazioni

$$r_1 \mathbin{\perp} \mathsf{v}_1 + r_2 \mathbin{\perp} \mathsf{v}_2 + \cdots + r_n \mathbin{\perp} \mathsf{v}_n = \mathbf{0} \quad \text{e} \quad r_1 \neq 0 \ ,$$

si deduce che

$$r_1 \mathbin{\perp} \mathsf{v}_1 = -r_2 \mathbin{\perp} \mathsf{v}_2 - \cdots - r_n \mathbin{\perp} \mathsf{v}_n \ ,$$

ma può accadere che non si possa disporre del reciproco di r_1 per riuscire a esprimere v_1 come combinazione lineare di v_2, ... , v_n .

T25b.04 Ogni insieme $B \subseteq M$ è detto **base del modulo** $\boldsymbol{M}$ sse

$$B \text{ è linearmente indipendente e } \boldsymbol{span}_{\boldsymbol{R}}(B) = \boldsymbol{M} .$$

(1) Prop.: Se $\mathfrak{B}$ è una base del modulo $\boldsymbol{M}$ sull'anello $\boldsymbol{R}$, allora:

(a) $\mathfrak{B}$ è un insieme generatore minimale;
(b) $\mathfrak{B}$ è un sottoinsieme linearmente indipendente massimale ∎

Ricordiamo che per gli spazi vettoriali le due condizioni precedenti sono equivalenti e che un sottoinsieme di vettori che le soddisfa è una base dello spazio; vi sono invece moduli per i quali le condizioni non bastano a garantire si tratti di una base.

Il modulo su $\mathbb{Z}_{Rng}$ il cui terreno è $\mathbb{Z}_n$ di b02 non possiede alcun insieme indipendente e quindi non possiede una base; l'intero modulo è generatore di se stesso e quindi abbiamo che un insieme spanning minimale che non è una base.

Si dice **modulo finitodimensionale** un modulo ridotto al vettore zero oppure un modulo che possieda una base finita.

Si dice **modulo infinitodimensionale** un modulo che possiede una base infinita.

T25b.05 Introduciamo ora i morfismi per le strutture di modulo su anello.u, cioè le funzioni da modulo a modulo che nel caso degli spazi vettoriali sono le trasformazioni lineari.

Consideriamo due moduli sullo stesso anello.u $\boldsymbol{R}$:

$$\boldsymbol{M} = \langle M, \boldsymbol{R}, \boldsymbol{+}_V, \boldsymbol{-}_M, \mathbf{0}_{\boldsymbol{M}}, {}^{\perp}{}_M \rangle \text{ e } \boldsymbol{N} = \langle W, \boldsymbol{F}, \boldsymbol{+}_W, \boldsymbol{-}_N, \mathbf{0}_N, {}^{\perp}{}_{\boldsymbol{N}} \rangle .$$

Si dice **omomorfismo di modulo** di MBi in $\boldsymbol{N}$ una funzione $\tau \in \lceil M \longmapsto N \rceil$ tale che

$$\forall a, b \in \boldsymbol{R} \ , \ \mathsf{u}, \mathsf{v} \in \boldsymbol{M} \ : \ \tau(a {}^{\perp}{}_M \mathsf{u} \ \boldsymbol{+}_M \ b {}^{\perp}{}_M \mathsf{v}) \ = \ a {}^{\perp}{}_N \tau(\mathsf{u}) \ \boldsymbol{+}_N \ b {}^{\perp}{}_N \tau(\mathsf{v}) .$$

Denotiamo con $\mathsf{Hom}(\boldsymbol{M}, \boldsymbol{N})$ l'insieme degli omomorfismi di modulo da $\boldsymbol{M}$ ad $\boldsymbol{N}$.

Si dice **omomorfismo di modulo nullo** di $\boldsymbol{M}$ ad $\boldsymbol{N}$ la funzione $\mathbf{0}_N{}^{\mathrm{cnst}} = \lceil \mathsf{v} \in M \mapsto \mathbf{0}_{\boldsymbol{N}} \rceil$.

T25b.06 Vi sono alcuni casi particolari di omomorfismi di modulo di rilevante importanza.

Si dice **endomorfismo di modulo** entro $\boldsymbol{M}$ un omomorfismo di modulo da $\boldsymbol{M}$ in $\boldsymbol{M}$; Denotiamo con $\mathsf{Endom}(\boldsymbol{M})$ o con $\lceil MBi \longrightarrow_{Mdl} \boldsymbol{M} \rceil$ l'insieme degli endomorfismi di modulo entro $\boldsymbol{M}$.

Si dice **monomorfismo di modulo** di MBi in $\boldsymbol{N}$ un omomorfismo di modulo iniettivo da $\boldsymbol{M}$ in $\boldsymbol{N}$. Denotiamo con $\mathsf{Monom}(\boldsymbol{M}, \boldsymbol{N})$ o con $\lceil MBi \longhookrightarrow_{Mdl} \boldsymbol{N} \rceil$ l'insieme dei monomorfismi di modulo da $\boldsymbol{M}$ in $\boldsymbol{N}$.

Si dice **epimorfismo di modulo** di MBi su $\boldsymbol{N}$ un omomorfismo di modulo suriettivo di $\boldsymbol{M}$ in $\boldsymbol{N}$. Denotiamo con $\mathsf{Epim}(\boldsymbol{M}, \boldsymbol{N})$ o con $\lceil MBi \longrightarrow\!\!\!\!\triangleright_{Mdl} \boldsymbol{N} \rceil$ l'insieme degli epimorfismi di modulo da $\boldsymbol{M}$ in $\boldsymbol{N}$.

Si dice **isomorfismo di modulo** di MBi ed $\boldsymbol{N}$ un omomorfismo di modulo biiettivo di $\boldsymbol{M}$ in $\boldsymbol{N}$. Denotiamo con $\mathsf{Isom}(\boldsymbol{M}, \boldsymbol{N})$ o con $\lceil MBi \triangleleft\!\!\longrightarrow\!\!\!\!\triangleright_{Mdl} \boldsymbol{N} \rceil$ l'insieme degli isomomorfismi di modulo di $\boldsymbol{M}$ ed $\boldsymbol{N}$.

Si dice **automorfismo di modulo** entro $\boldsymbol{M}$ un endomorfismo di modulo biiettivo tra $\boldsymbol{M}$ e se stesso; Denotiamo con $\mathsf{Autom}(\boldsymbol{M})$ o con $\lceil \boldsymbol{M} \triangleleft\!\!\longrightarrow\!\!\!\!\triangleright_{Mdl} \boldsymbol{M} \rceil$ l'insieme degli automorfismi di modulo entro $\boldsymbol{M}$.

T25b.07 Consideriamo l'omomorfismo di modulo $H \in \mathsf{Hom}(\boldsymbol{M}, \boldsymbol{N})$.

Si dice **nucleo** o **kernel** di tale omomorfismo l'insieme dei vettori di $\boldsymbol{M}$ che H manda nel vettore nullo $\mathbf{0}_{\boldsymbol{N}}$; tale sottoinsieme di M si denota con $\boldsymbol{ker}(H)$.

Si dice **immagine dell'omomorfismo** H l'insieme dei vettori di $\boldsymbol{N}$ che costituiscono il codominio di H; tale sottoinsieme di N si denota con $\mathrm{img}(H)$.

(1) Prop.: Per ogni omomorfismo di modulo $H \in \mathsf{Hom}(\boldsymbol{M}, \boldsymbol{N})$ $\boldsymbol{ker}(H)$ è il terreno di un sottomodulo di $\boldsymbol{M}$ e $\mathrm{img}(H)$ è il terreno di un sottomodulo di $\boldsymbol{N}$ ∎

Questa proprietà rende lecito, quando questo non conduce ad ambiguità, servirsi di $\boldsymbol{ker}(H)$ e di $\mathrm{img}(H)$ per denotare anche i sottomoduli dei quali tali sottoinsiemi, risp., son i terreni.

T25b.08 La disponibilità di una base da parte di un modulo costituisce un notevole vantaggio.

Un modulo si dice **modulo libero** sse possiede una base. Se $\mathfrak{B}$ è una base per il modulo $\boldsymbol{M}$ sull'anello.u $\boldsymbol{R}$ si dice che $\boldsymbol{M}$ è libero su $\mathfrak{B}$.

Presentiamo ora un modulo libero che non possiede alcun sottomodulo libero, esempio che mostra che anche i moduli liberi presentano differenze marcate dagli spazi vettoriali.

Consideriamo il modulo $\mathsf{MdlRR}(\mathbb{Z} \times \mathbb{Z})$ e il suo sottoinsieme $\{\langle 1, 1\rangle\}$.

Questo è un insieme linearmente indipendente, in quanto:

$$\forall h, k \in \mathbb{Z} \ : \ \langle h, k\rangle \perp \langle 1, 1\rangle = \langle 0, 0\rangle \implies \langle h, k\rangle = \langle 0, 0\rangle \ .$$

Inoltre $\langle 1, 1\rangle$ genera l'intero $\mathbb{Z} \times \mathbb{Z}$, in quanto $\forall h, k \in \mathbb{Z} \ : \ \langle h, k\rangle = \langle h, k\rangle \perp \langle 1, 1\rangle$.

Quindi $\{\langle 1, 1\rangle\}$ è una base per questo modulo.

Chiaramente $\mathbb{Z} \times \{0\}$ è sottomodulo di $\mathsf{MdlRR}(\mathbb{Z} \times \mathbb{Z})$; esso non possiede base, in quanto per ogni $h \in \mathbb{Z}_{nz}$ si ha $\langle 0, 1\rangle \langle h, 0\rangle = \langle 0, 0\rangle$ e quindi $\{\langle h, 0\rangle\}$ non è un insieme di vettori linearmente indipendenti.

T25b.09 Se cerchiamo di assegnare una dimensione a un modulo, come si fa per gli spazi vettoriali a partire dala cardinale delle sue basi, si possono incontare gravi difficoltà. In effetti presentiamo un modulo sopra un anello.u noncommutativo che per ogni intero $n \in \mathbb{P}$ presenta una base avente cardinale n.

Sia $\boldsymbol{V}$ uno spazio vettoriale sopra un campo $\boldsymbol{F} = \langle F, +, -, 0, \cdot, {}^{-1}, 1\rangle$, spazio avente dimensione $\aleph_0$ e sia $\mathfrak{B} = \langle \mathbf{b}_1, \mathbf{b}_2, ...\rangle$ una sua base illimitatamente generabile.

Denotiamo con $\boldsymbol{R}_V$ l'anello nonabeliano costituito dagli operatori lineari su $\boldsymbol{V}$, cioè sia

$$\boldsymbol{R}_V \ := \langle \mathsf{Lintr}(\boldsymbol{V}), +^{ce}, -^{ce}, \lceil \mathbf{v} \in \boldsymbol{V} \mapsto \mathbf{0}_V \rceil \rangle \ .$$

Introduciamo infine il modulo $\boldsymbol{M}_V = \mathsf{MdlRR}(\boldsymbol{R}_V)$.

Osserviamo che $\mathsf{Id}_{\boldsymbol{R}_V}$ è una base per $\boldsymbol{M}_V$ e dimostriamo l'enunciato che segue.

(1) Prop.: Per ogni $n \in \P)Mb$ si può costruire una base di $\boldsymbol{M}_V = \mathsf{MdlRR}(\mathsf{Lintr}(\boldsymbol{V}))$ avente cardinale n.

Dim.: Ripartiamo $\mathfrak{B}$ negli n sottoinsiemi

$$\mathfrak{B}_s \ := \ \{k \in \mathbb{N} :| \ \mathbf{b}_{k\,n+s}\} \quad \text{per} \quad s = 0, 1, 2, ..., n-1 \ ,$$

consideriamo gli n proiettori sui primi n vettori della base $P_s \ := \ \boldsymbol{Prj}_{\mathbf{b}_s}$ e introduciamo gli n operatori di $\mathsf{Lintr}(\boldsymbol{V})$ relativi a $s = 0, 1, ..., n-1$ ponendo

$$Q_s(\mathbf{b}_{k\,n+t}) \ := \ P_s \quad \text{sse} \quad t = s \ , \ \mathbf{0}_{\boldsymbol{V}} \quad \text{sse} \quad t \neq s \ .$$

L'insieme $\mathsf{Q} := \langle P_0, P_1, P_2, ..., P_{n-1}\rangle$ è una sequenza di vettori di $\boldsymbol{M}_V$ linearmente indipendenti: infatti per ogni n-upla di scalari $\langle \alpha_0, \alpha_1, ..., \alpha_{n-1}\rangle$ tali che

$$\alpha_0\, Q_0 + \alpha_1\, Q_1 + \cdots + \alpha_{n-1}\, Q_{n-1} = \mathbf{0} \ ,$$

applicando i due membri a $\mathbf{b}_{k\,n+t}$ si ottiene

$$\mathbf{0} = \alpha_t\, Q_t(\mathbf{b}_k\, n + t) = \alpha_t(\mathbf{b}_k)\ ;$$

quindi $\forall t = 0, 1, 2, ..., n-1\ :\ `\alpha_t = \mathbf{0}$.

Inoltre Q è generatore dell'intero $\boldsymbol{M}_V$: infatti per ogni trasformazione $\boldsymbol{L} \in \mathsf{Lintr}(\boldsymbol{V})$, per ogni $s = 0, 1, 2, ..., n-1$ e per ogni $k \in \mathbb{N}$ definiamo

$$L_s(\mathbf{b}_k) := \boldsymbol{L}(\mathbf{b}_{k\,n+s})\ ;$$

allora

$$(L_0\, Q_0 + L_1\, Q_1 + \cdots + L_{n-1}\, Q_{n-1})(\mathbf{b}_{k\,n+t}) := L_t\, Q_t(\mathbf{b}_{k\,n+s}) = L_t(\mathbf{b}_k) = \boldsymbol{L}(\mathbf{b}_{k\,n+t})\ ;$$

quindi

$$\boldsymbol{L} = L_0\, Q_0 + L_1\, Q_1 + \cdots + L_{n-1}\, Q_{n-1}\ ,$$

uguaglianza che dimostra che

$$\boldsymbol{L} \in \boldsymbol{span}\{Q_0, Q_1, ..., Q_{n-1}\}\ .$$

In conclusione Q è una base per $\boldsymbol{M}_v$ e il modulo in esame possiede basi di ogni cardinale finito ∎

T25b.10 Una misura per l'estensione dei moduli che generalizza quella di dimensione per gli spazi vettoriali si può invece definire per tutti i moduli liberi sopra un anello.u $\boldsymbol{R}$ commutativo, grazie all'enunciato che segue e che dimostreremo in :c.

(1) Teorema Due basi qualsiasi di un modulo sopra un anello.u commutativo hanno lo stesso cardinale.

Diciamo **rango di un modulo libero** $\boldsymbol{M}$ sopra un anello.u commutativo il cardinale comune delle sue basi. Tale numero cardinale si denota con $\mathrm{rnk}(\boldsymbol{M})$.

T25b.11 Prendiamo in considerazione un anello $\boldsymbol{R}$, un insieme qualsiasi E, l'insieme delle funzioni da E in R aventi supporto finito che denotiamo con ${R^E}_\varphi$ e il modulo su $\boldsymbol{R}$ avente come insieme dei vettori ${R^E}_\varphi$ e come operazioni di combinazione lineare le combinazioni lineari delle funzioni di $\lceil\, E \longmapsto R\, \rceil$. Questo modulo lo denotiamo con $\mathsf{Mdlfun}\phi(E, \boldsymbol{R})$.

Introduciamo inoltre l'insieme di funzioni

$$\mathfrak{B}_{E,\boldsymbol{R}}\ :=\ \{e \in E\ :|\ \lceil\, x \in E \nmapsto \delta_K(e, x)\, \rceil\}\,;$$

evidentemente si tratta di un insieme avente cardinale $|E|$.

(1) Prop.: $\mathsf{Mdlfun}_\phi(E, \boldsymbol{R})$ è un modulo libero che ha come base $\mathfrak{B}_{E,\boldsymbol{R}}$ ∎

T25b.12 Sia $\boldsymbol{M}$ un modulo libero su $\boldsymbol{R}$ e sia B una sua base. $\boldsymbol{M}$ è isomorfo a $\mathsf{Mdlfun}_\phi(B, \boldsymbol{R})$.

Dim.: Essendo B una base di $\boldsymbol{M}$, ogni $\mathbf{v} \in M$ si può esprimere in un unico modo come $\mathbf{v} = a_1\, \mathbf{b}_1 + \cdots + r_n\, \mathbf{b}_n$ per qualche intero positivo n e a meno dell'ordine dei vettori $\mathbf{b}_1, ..., \mathbf{b}_n \in B$.

Al vettore $\mathbf{v}$ associamo la funzione di $\lceil\, B \longmapsto R\, \rceil$

$$\beta(\mathbf{v})\ :=\ \lceil\, b \in B \nmapsto \begin{cases} r_i & \text{sse } b = \mathbf{b}_i \text{ per qualche } i \text{ della combinazione} \\ 0 & \text{sse altrimenti} \end{cases}$$

Per estensione lineare di β si ottiene una applicazione τ dell'intero modulo $\boldsymbol{M}$ in ${R^B}_\phi$.

La τ è chiaramente un omomorfismo di modulo di $\boldsymbol{M}$ in ${R^B}_\phi$. Si tratta di un omomorfismo iniettivo, dato che $\tau(\mathbf{v}) = \lceil\, b \nmapsto \mathbf{0}\, \rceil$ implica che le coordinate di $\mathbf{v}$ rispetto ai vari vettori della base valgono $\mathbf{0}$, cioè che $\mathbf{v} = \lceil\, b \in B \nmapsto \mathbf{0}\, \rceil$.

Inoltre τ è suriettivo, in quanto per ogni $f \in {R^B}_\phi$ si può individuare l'elemento di M $\mathbf{v} := \sum_{b \in B} f(b)\, b$, espressione che si riduce a una combinazione lineare finita in forza del fatto che la f ha supporto finito.
Infine la τ è tale che $\forall b \in B \ : \ (\tau(\mathbf{v}))(b) = f(b)$, cioè $\forall \mathbf{v} \in \boldsymbol{M} \ : \ `\tau(\mathbf{v}) = f$.
Dunque $\tau \in \lceil\!\lceil\, \boldsymbol{M} \lhd\!\!\rightarrow\!\!\rhd_{Mdl} {R^B}_\phi \,\rceil\!\rceil$ ∎

T25b.13 **Prop.** Due moduli liberi sullo stesso anello sono isomorfi sse hanno lo stesso rango.

Dim.: Consideriamo l'anello $\boldsymbol{R}$ e i due moduli su di esso $\boldsymbol{M}$ ed $\boldsymbol{N}$.

"$\Longrightarrow$" Se i due moduli sono isomorfi e τ è un isomorfismo che li collega, tale applicazione pone in biiezione una base di $\boldsymbol{M}$ con una base di $\boldsymbol{N}$ e di conseguenza $\mathrm{rnk}(\boldsymbol{M}) = \mathrm{rnk}(\boldsymbol{N}$.

"$\Longleftarrow$" Sia $\mathrm{rnk}(\boldsymbol{M}) = \mathrm{rnk}(\boldsymbol{N})$; denotiamo con $\mathfrak{B}$ una base di $\boldsymbol{M}$ e con $\mathfrak{C}$ una base di $\boldsymbol{N}$. Essendo $|\mathfrak{B}| = |\mathfrak{C}|$ esiste una biiezione $\beta \in \lceil\!\lceil\, \mathfrak{B} \lhd\!\!\rightarrow\!\!\rhd \mathfrak{C} \,\rceil\!\rceil$. Estendendo per linearità questa funzione si ottiene un isomorfismo tra i due moduli ∎

T25b.14 Munendo l'insieme degli omomorfismi $\mathsf{Hom}(\boldsymbol{M}, \boldsymbol{N})$ della somma ${\boldsymbol{+}_N}^{\mathrm{fun}}$ e della differenza ${\boldsymbol{-}_N}^{\mathrm{fun}}$ tra funzioni a valori in N e del prodotto ${\perp_N}^{\mathrm{fun}}$ per elementi dell'anello, si ottiene un altro modulo su $\boldsymbol{R}$:

$$\left\langle \mathsf{Hom}(\boldsymbol{M}, \boldsymbol{N}), \boldsymbol{R}, {\boldsymbol{+}_N}^{\mathrm{fun}}, {\boldsymbol{-}_N}^{\mathrm{fun}}, {\mathbf{0}_N}^{\mathrm{cnst}}, {\perp_N}^{\mathrm{fun}} \right\rangle .$$

Questa struttura viene chiamata **modulo degli omomorfismi** di $\boldsymbol{M}$ in $\boldsymbol{N}$.

Si trova facilmente che se $\boldsymbol{X}$ è un terzo modulo sull'anello $\boldsymbol{R}$, la composizione di $H \in \mathsf{Epim}(\boldsymbol{M}, \boldsymbol{N})$ e di $K \in \mathsf{Hom}(\boldsymbol{N}, \boldsymbol{X})$ è $H \circ_{lr} K \in \mathsf{Hom}(\boldsymbol{M}, \boldsymbol{X})$.
Inoltre, se $H \in \mathsf{Isom}(\boldsymbol{M}, \boldsymbol{N})$, allora $H^{-\mathbf{1}} \in \mathsf{Isom}(\boldsymbol{N}, \boldsymbol{M})$.

T25 c. moduli quozienti, moduli noetheriani e teorema della base di Hilbert

T25c.01 Riprendiamo la nozione di somma diretta considerandola come costruzione di nuovi moduli a partire da moduli noti.

Per $k \in \{2,3,4,...\}$ consideriamo k moduli sull'anello.u $\boldsymbol{R}$ $\boldsymbol{M}_i = \langle M_i, \boldsymbol{R}, \boldsymbol{+}_i, \boldsymbol{-}_i, \mathbf{0}_i, \perp_i \rangle$ per $i = 1, ..., k$ e poniamo attenzione al loro prodotto cartesiano $M_1 \times \cdots \times M_k$.

Presi $\mathsf{v}_i, \mathsf{w}_i \in \boldsymbol{M}_i$ per $i = 1, ..., k$ ed $a \in \boldsymbol{R}$ si definiscono:

$\langle \mathsf{v}_1, ..., \mathsf{v}_k \rangle \boldsymbol{+} \langle \mathsf{w}_1, ..., \mathsf{w}_k \rangle := \langle \mathsf{v}_1 \ \boldsymbol{+}_1 \ \mathsf{w}_1, ..., \mathsf{v}_k \ \boldsymbol{+}_k \ \mathsf{w}_k \rangle$;

$\langle \mathsf{v}_1, ..., \mathsf{v}_k \rangle \boldsymbol{-} \langle \mathsf{w}_1, ..., \mathsf{w}_k \rangle := \langle \mathsf{v}_1 \ \boldsymbol{-}_1 \ \mathsf{w}_1, ..., \mathsf{v}_k \ \boldsymbol{-}_k \ \mathsf{w}_k \rangle$;

$a \perp \langle \mathsf{v}_1, ..., \mathsf{v}_k \rangle := \langle a \perp_1 \mathsf{v}_1, ..., a \perp_k \mathsf{v}_k \rangle$;

$\mathbf{0} := \langle \mathbf{0}_1, ..., \mathbf{0}_k \rangle$.

Si dice **somma diretta dei moduli** $\boldsymbol{M}_1$, ... , $\boldsymbol{M}_k$:

$$\boldsymbol{M}_1 \oplus \boldsymbol{M}_2 \oplus \cdots \oplus \boldsymbol{M}_k := \left\langle \boldsymbol{M}_1 \times \boldsymbol{M}_2 \times \cdots \times \boldsymbol{M}_k, \boldsymbol{R}, \boldsymbol{+}, \boldsymbol{-}, \langle \mathbf{0}_1, \mathbf{0}_2, ..., \mathbf{0}_k \rangle, \perp \right\rangle .$$

T25c.02 Consideriamo il sottomodulo supportato dal sottoinsieme S di M e la relazione binaria entro M

$$\mathsf{v} =_S \mathsf{w} \iff \mathsf{v} - \mathsf{w} \in S \quad \text{ove} \quad \mathsf{v}, \mathsf{w} \in M .$$

(1) Prop.: La $=_S$ è una relazione di uguaglianza modulo S di elementi di un modulo /;;equivalenza.

Dim.: Evidente che la relazione è riflessiva e simmetrica. Inoltre se per $\mathsf{x} \in M$ si ha $\mathsf{w} - \mathsf{x} \in S$, allora $\mathsf{v} - \mathsf{x} = (\mathsf{v} - \mathsf{w}) - (\mathsf{x} - \mathsf{w}) \in S$, cioè la relazione è transitiva ∎

Le classi di equivalenza della $=_S$ sono i sottoinsiemi di M della forma $C := \mathsf{v} + S = \{\mathsf{s} \in S :| \ \mathsf{v} + \mathsf{s}\}$.

Per **modulo quoziente** di $\boldsymbol{M}$ su S si intende il modulo costituito dalle classi $\mathsf{v} + S$ per $\mathsf{v} \in M$ il cui insieme è munito della somma $\boldsymbol{+}^{be}$ definita da $(\mathsf{v} + S) \boldsymbol{+}^{be} (\mathsf{w} \boldsymbol{+} S) := (\mathsf{v} \boldsymbol{+} \mathsf{w}) \boldsymbol{+}^{be} S$ e della moltiplicazione per gli scalari definita da $r \perp^{be} (\mathsf{v} \boldsymbol{+} S) := r \perp \mathsf{v} \boldsymbol{+}^{be} S$ per ogni $r \in R$, $\mathsf{v}, \mathsf{w} \in M$.

Questo modulo viene denotato da $\boldsymbol{M}/S$.

T25c.03 È naturale chiedersi se ogni modulo libero presenta tutti i moduli quoziente liberi, ma questa speranza è negata dal seguente controesempio.

Consideriamo il modulo **MdlRR**$(\mathbb{Z})$, modulo libero avente come base semplicemente $\{1\}$. Per ogni $n \in \{2,3,4,...\}$ si ha che $n\,\mathbb{Z}$ sostiene un suo sottomodulo.
Grazie alla biiezione $\lceil k \in \mathbb{Z} : \ k + n\,\mathbb{Z} \mapsto [k]_n \rceil$ si ha isomorfismo tra gli anelli $\mathbb{Z}/n\,\mathbb{Z}$ e $\mathbb{Z}_n$ e quindi isomorfismo tra i moduli **MdlRR**$(\mathbb{Z}/n\,\mathbb{Z})$ e **MdlRR**$(\mathbb{Z}_n)$.
Ma abbiamo visto che quest'ultimo non è libero e quindi non è libero neppure il modulo quoziente **MdlRR**$(\mathbb{Z}/n\,\mathbb{Z})$.

T25c.04 Un modulo $\boldsymbol{M}$ sull'anello $\boldsymbol{R}$ si dice soddisfare la condizione della catena ascendente sui sottomoduli sse ogni catena di suoi sottomoduli ascendente $\langle S_1 \subset S_2 \subset S_3 \subset ... \rangle$ è finita, ossia sse ogni catena di suoi moduli ascendente in senso lato $\langle S_1 \subseteq S_2 \subseteq S_3 \subseteq ... \rangle$ presenta un indice k per il quale sia $S_k = S + k + 1 = s_{k+2}...$.

T25c.05 **Teorema** Consideriamo un modulo $\boldsymbol{M}$ sopra l'anello.u $\boldsymbol{R}$.
Ogni sottomodulo di $\boldsymbol{M}$ è finitamente generato $\iff$ $\boldsymbol{M}$ ha tutte le catene di sottomoduli finite.

Dim.: "$\Longrightarrow$"

"$\Longleftarrow$" ∎

I moduli che posseggono una delle due precedenti proprietà si dicono **moduli noetheriani** (in onore di Emmy Noether).

Denotiamo con $\mathsf{MdlNoet}_{\boldsymbol{R}}$ l'insieme dei moduli noetheriani sull'anello.u $\boldsymbol{R}$.

T25c.06 Le considerazioni precedenti valgono in particolare per i moduli $\mathsf{MdlRR}(\boldsymbol{R})$ e di conseguenza si possono trasferire agli anelli.u.

Un anello $\boldsymbol{R}$ si dice soddisfare la **condizione della catena ascendente sugli ideali** sse ogni catena di suoi ideali ascendente $\langle I_1 \subset I_2 \subset I_3 \subset ... \rangle$ è finita,

Ogni ideale di $\boldsymbol{R}$ inteso come sottomodulo è finitamente generato $\Longleftrightarrow$ $\boldsymbol{R}$ ha tutte le catene di ideali finite. ∎Gli anelli che posseggono una delle due precedenti proprietà si dicono **anelli noetheriani**.
Denotiamo con $\mathsf{RngNoet}_{\boldsymbol{R}}$ l'insieme degli anelli noetheriani.

T25c.07 Se l'anello $\boldsymbol{R}$ è noetheriano, allora ciascuno dei moduli su $\boldsymbol{R}$ finitamente generati è noetheriano.

Dim.: ∎

T25c.08 A questo punto è naturale chiedersi quali sono gli anelli noetheriani. Si trova senza difficoltà che un anello commutativo è un campo sse non presenta ideali propri diversi da quello nullo.
Si conclude che a ogni campo è associato un anello noetheriano ottenuto come suo impoverimento.

Inoltre anche ogni dominio a ideali principali è un anello noetheriano.
Altri anelli noetheriani sono individuabili sulla base dell'enunciato che segue.

T25c.09 **Teorema** (**teorema della base di Hilbert**)
Se un anello $\boldsymbol{R}$ è noetheriano, allora è noetheriano anche i corrispondente 'anello di polinomi $\boldsymbol{R}[x]$.

Dim.: ∎

T25 d. moduli su domini con ideale principale

T25d.01 Prendiamo ora in considerazione i moduli il cui anello è più particolarmente un dominio con ideale principale cioè un dominio di integrità (anello commutativo privo di divisori dello zero) in cui tutti gli ideali si possono generare a partire da un unico elemento (ossia hanno una forma del tipo $\langle a \rangle$) .
Ricordiamo che usiamo **PID**, come acronimo di principal ideal domain; ossia del termine **dominio dotato di ideale principale**; inoltre denotiamo con $\boldsymbol{DomPid}$ l'insieme dei domini dotati di ideale principale e con MdlPid la collezione dei moduli sopra un $\boldsymbol{R} \in \boldsymbol{DomPid}$.
Qui ci proponiamo di individuare proprietà godute da questi moduli privilegiati e non garantite per tutti gli altri tutti i moduli.

T25d.02 **Teorema** Consideriamo un $\boldsymbol{R} \in \boldsymbol{DomPid}$ e un modulo $\boldsymbol{M}$ su questo $\boldsymbol{R}$ e libero. Ogni suo sottomodulo $\boldsymbol{S}$ è libero e per il suo rango si ha $\mathrm{rnk}(\boldsymbol{S}) \leq \mathrm{rnk}(\boldsymbol{M})$ ∎

Dim.: Il teorema è valido per tutti i moduli sopra un Pid $\boldsymbol{R}$ e liberi, ma qui ci limitiamo ai moduli di rango finito.
Procederemo per induzione e, dato che ogni modulo libero di rango $n \in \mathbb{N}$ è isomorfo ad $\boldsymbol{R}^{\times n}$, possiamo limitarci a considerare questi i moduli per i diversi n.
Per $n = 1$ dobbiamo esaminare $\boldsymbol{M} = \mathsf{MdlRR}(\boldsymbol{R})$; ogni sottomodulo $\boldsymbol{S}$ di $\boldsymbol{M}$ è un ideale di $\boldsymbol{R}$; quindi $\boldsymbol{S} =< a >$, ossia è ideale principale.
Essendo $\boldsymbol{R} \in \boldsymbol{DomPid}$, $\forall r \in R \setminus \{o\} \,:\, r\,a \neq 0$: quindi la mappa $\tau \;:=\; \lceil\, r \in R \mapsto r\,a \,\rceil \in \lceil\, R \longleftrightarrow\!\triangleright S \,\rceil$ è un isomorfismo tra $\boldsymbol{R}$ ed $\boldsymbol{S}$ e quindi $\boldsymbol{S}$ è libero..

Per l'induzione assumiamo che l'enunciato valga per $\boldsymbol{S}_k = \boldsymbol{R}^{\times k}$ per $k = 1, 2, ..., n-1$ e proponiamoci di dimostrarlo per $\boldsymbol{S}_n := \boldsymbol{R}^{\times n}$.
Consideriamo i due insiemi di coppie di n-uple

$$\boldsymbol{S'} \;:=\; \left\{ \langle s_1, ..., s_{n-1}, s_n \rangle \in \boldsymbol{S}_n \,:|\, \langle s_1, ..., s_{n-1}, 0 \rangle \right\} \quad \text{e}$$
$$\boldsymbol{S''} \;:=\; \left\{ \langle s_1, ..., s_{n-1}, s_n \rangle \in S_n \,:|\, \langle 0, ..., 0, s_n \rangle \right\} .$$

Evidentemente essi sono sottomoduli di $\boldsymbol{S}_n$ e $\boldsymbol{S}_n = \boldsymbol{S'} \oplus \boldsymbol{S''}$.
Inoltre chiaramente $\boldsymbol{S'}$ è isomorfo a

$$\{ \langle s_1, ..., s_{n-1}, 0 \rangle \,:|\, \langle s_1, ..., s_{n-1}, s_n \rangle \in S \}$$

mentre $\boldsymbol{S''}$ è isomorfo a

$$\left\{ \langle 0, ..., 0, s_n \rangle \,:|\, \langle s_1, ..., s_{n-1}, s_n \rangle \in S \right\} <_M dl\boldsymbol{R} \,.$$

Per l'ipotesi induttiva $\boldsymbol{S'}$ e $\boldsymbol{S''}$ sono moduli liberi. Se $\boldsymbol{S'}$ è generato da un $\{v_1, ..., v_h\}$ con $h \leq n-1$ ed $\boldsymbol{S''}$ è generato da un w, allora $\boldsymbol{S}$ è generato da $\{v_1, ..., v_h, w\}$ con $h + 1 \leq n$ ∎

T25d.03 Un elemento v di un modulo $\boldsymbol{M}$ con terreno M tale che per qualche $m \in M \setminus \{0\} \;:\; m\,\mathsf{v} = 0$ si chiama **elemento di torsione** di $\boldsymbol{R}$.
Un modulo che non presenta elementi di torsione si dice **modulo libero da torsione**, mentre un modulo che presenta tutti gli elementi di torsione si dice **modulo di torsione**.

Denotiamo con M_{trsn} il sottoinsieme di $\boldsymbol{M}$ costituito dell'insieme dei suoi elementi di torsione. Si trova facilmente che tale sottoinsieme sostiene un sottomodulo di $\boldsymbol{M}$ che denotiamo con $\boldsymbol{M}_{\mathsf{trsn}}$.

Si verifica poi che $\boldsymbol{M}/\boldsymbol{M}_{\mathsf{trsn}}$ è un modulo libero da torsione.
Inoltre si mostra che ogni modulo libero su un Pid è libero da torsione.

T25d.04 Vediamo un enunciato che si avvicina alla proposizione inversa.

Ogni modulo $\boldsymbol{M}$ libero da torsione, finitamente generato sopra un Pid $\boldsymbol{R}$ è un modulo libero.

Dim.: Dato che $\boldsymbol{M}$ è finitamente generato si può scrivere $\boldsymbol{M} = \langle v_1, v_2, ..., v_n \rangle$ dove $G = \{v_1, v_2, ..., v_n\}$ è un opportuno insieme di vettori di M. Denotiamo con $\{w_1, ..., w_k\}$ un insieme massimale di questi vettori linearmente indipendente e in seguito a una opportuna ridefinizione degli indici possiamo scrivere $G = \{w_1, w_2, ..., w_n\}$.
Dunque si possono trovare per ogni $j = k+1, ..., n$ $k+1$ scalari $a_j, r_{j,1}, ..., r_{j,k}$ tali che $r_{j,1}\, w_1 + \cdots + r_{j,k}\, w_k + a_j w_j = \mathbf{0}$.
Introduciamo il prodotto $a := a_{k+1}\, a_{k+2} \cdot \cdots a_n \in R$ e i vettori $a\, w_h$ per $h = k+1, k+2, ..., n$; chiaramente per ciascuno di tali h si ha $a\, w_h \in \boldsymbol{span}(G)$. Quindi il modulo $a \cdot M = \{\mathbf{v} \in M :| \ a \cdot \mathbf{v}\}$ è sottomodulo di $\boldsymbol{span}(G)$; ma questo è un modulo libero con base G e quindi, grazie a d02, $a \cdot M$ è anche un modulo libero.
La mappa $\lceil\, \mathbf{v} \in M \ \mapsto \ a \cdot \mathbf{v} \,\rceil$ è un epimorfismo e inoltre è iniettivo in quanto M è libero da torsione. Quindi $\boldsymbol{M}$ è isomorfo ad $a \cdot M$ e come questo è un modulo libero ∎

T25d.05 Ci proponiamo ora di dimostrare che ogni modulo $\boldsymbol{M}$ sopra un Pid è decomponibile come somma diretta del suo sottomodulo dei vettori di torsione $\boldsymbol{M}_{\mathsf{trsn}}$ [d03] e di un modulo libero da torsione che denoteremo con $\boldsymbol{M}_{free}$.

Dato che il modulo quoziente $\boldsymbol{M}/\boldsymbol{M}_{\mathsf{trsn}}$ è libero da torsione e finitamente generato quando lo è $\boldsymbol{M}$, grazie a d04 si ottiene che esso è anche un modulo libero.

Consideriamo il proiettore

$$\pi \ := \ \left\lceil\, \mathbf{v} \in M \ \mapsto \ \mathbf{v}^{be} M_{\mathsf{trsn}} \,\right\rceil \ \in \ \lceil\, M \longmapsto M/M_{\mathsf{trsn}} \,\rceil \ .$$

Cerchiamo ora di dimostrare che, analogamente a quanto accade per gli spazi vettoriali, anche i nostri moduli si possono esprimere come somma diretta del nucleo e dell'immagine della suddetta proiezione.

T25d.06 **Teorema** Ogni modulo $\boldsymbol{M}$ finitamente generato sopra un Pid si può decomporre come

$$\boldsymbol{M} = \boldsymbol{M}_{\mathsf{trsn}} \oplus \boldsymbol{M}_{free} \ ,$$

dove $\boldsymbol{M}_{free}$ è un modulo libero.

Dim.:

T25d.07 Ci proponiamo ora di decomporre ogni modulo di torsione sopra un Pid e finitamente generato come somma diretta di sottomoduli ciclici.

Per un generico modulo $\boldsymbol{M}$ sopra un anello **annichilatore di un vettore v** del modulo il sottoinsieme di R

$$annh(\mathbf{v}) \ := \ \{r \in R \,\rceil\!\rceil\, r \cdot \mathbf{v} = \mathbf{0}\}$$

e diciamo **annichilatore** del modulo $\boldsymbol{M}$ il sottoinsieme di R

$$annh(\boldsymbol{M}) \ := \ \{r \in R \,\rceil\!\rceil\, r \cdot M = \{\mathbf{0}\}\}$$

Si mostra facilmente che tutti gli $annh(\mathbf{v})$ e tutti gli $annh(\boldsymbol{M})$ sono ideali di $\boldsymbol{M}$. Questi sono detti **ideali d'ordine-G** di $\boldsymbol{M}$. Si osserva inoltre che $\mathbf{v} \in M$ è un elemento di torsione di $\boldsymbol{M}$ sse $annh(\mathbf{v}) \neq \{0\}$.

Consideriamo ora $\boldsymbol{M}$ modulo di torsione sopra un Pid che inoltre sia finitamente generato. Scriviamo dunque $\boldsymbol{M} = \langle u_1, u_2, ..., u_n \rangle >$ e $g := \{u_1, u_2, ..., u_n\}$.
Per ogni $i = 1, 2, ..., n$ esiste $a_i \in annh(u_1)$ diverso da $\mathbf{0}$ e definiamo $a := a_1 \cdot a_2 \cdot \cdots \cdot a_n$.

Chiaramente $a \neq 0$ e $\forall \mathbf{v} \in M \ : \ a \cdot \mathbf{v} = \mathbf{0}$, ossia $a \in annh(\boldsymbol{M}$. In particolare si ha che $annh(\boldsymbol{M}) \neq \{\mathbf{0}\}$

T25d.08 Ogni generatore di un ideale principale $annh(\mathbf{v})$ lo chiamiamo **ordine-G di un ideale v**.
Ogni generatore di un ideale principale $annh(\boldsymbol{M})$ diverso da $\{\mathbf{0}\}$ lo diciamo ordine-G di $\boldsymbol{M}$.

Si osserva che se g_1 e g_2 sono ordini-G di $\boldsymbol{M}$ si ha un collegamento della forma $g_2 = u\, g_1$ con u unità-I di $\boldsymbol{R}$. Analoga relazione si ha tra due ordini-G di ogni $\mathbf{v} \in \boldsymbol{M}$.

Dunque ogni ordine-G di $\boldsymbol{M}$ o di un vettore di tale modulo è univocamente determinato a meno di un fattore unità-I e due elementi g_1 e g_2 presentano due fattorizzazioni come prodotto di elementi primi di $\boldsymbol{R}$ che differiscono solo per un fattore dato da una unità-I.

Un $\boldsymbol{M} \in$ **Mdl** si dice **modulo primario** sse il suo annichilatore ha la forma $annh(\boldsymbol{M}) = p^e$, dove p è un suo elemento primo ed $e \in \mathbb{P}$; in altre parole un modulo è primario sse presenta come ordine-G una potenza positiva di un elemento primo.

Si osserva che un modulo sopra un Pid di torsione e finitamente generato è primario sse ogni suo elemento ha come ordine-G una potenza di un unico elemento primo. JR

T25d.09 Ora ci proponiamo di decomporre un modulo di torsione come somma diretta di sottomoduli primari e successivamente di decomporre un modulo primario come somma diretta di sottomoduli ciclici.

Teorema (**teorema di decomposizione in sottomoduli primari**)
Consideriamo un modulo $\boldsymbol{M}$ nonnullo sopra un Pid RBi, di torsione e finitamente generato avendo come ordine-G $p := {p_1}^{e_1}\, {p_2}^{e_2} \cdots {p_n}^{e_n}$, dove p_1, p_2,...,p_n sono elementi primi distinti.
Tale modulo è esprimibile come

$$\boldsymbol{M} \ = \ M_{p_1} \oplus M_{p_2} \oplus \cdots \oplus M_{p_n} \quad \text{dove} \quad \forall i = 1, 2..., n \ : \ M_{p_i} = \{\mathbf{v} \in M \,\rceil\, {p_i}^{e_i}\, \mathbf{v} = \mathbf{0}\} \ ,$$

somma diretta di sottomoduli primari aventi ordini-G ${p_1}^{e_1}$,...,${p_n}^{e_n}$.

Dim.:

T25d.10 **Teorema** Consideriamo il modulo $\boldsymbol{M}$ sopra un Pid $\boldsymbol{R}$ nonnullo, di torsione e finitamente generato con ordine-G p^e.
$\boldsymbol{M}$ si può esprimere come somma diretta di sottomoduli ciclici

$$\boldsymbol{M} \ = \ C_1 \oplus C_2 \oplus \cdots \oplus C_k \ ,$$

dove per ogni $i = 1, 2..., k$ C_i è sottomodulo ciclico avente ordine-G ${p_i}^{e_i}$ e con gli esponenti che soddisfano la

$$e = e_1 \geq e_2 \geq \cdots \geq e_k \quad \text{ovvero} \quad p^{e_n} \preceq_{:} p^{e_{n-1}} \preceq_{:} \cdots \preceq_{:} p^{e_1} \ .$$

dim

∎

T25d.11 La decomposizione del teorema precedente non è unica, ma ci proponiamo di dimostrare che gli ordini-G sono unici a meno di una moltiplicazione per una unità-G.
Per questo bisogna premettere alcuni risultati.

(1) Prop.: Sia $\boldsymbol{R}$ un Pid e sia $\langle \mathbf{v} \rangle$ un modulo su $\boldsymbol{R}$ ciclico con $annh(\mathbf{v}) = \langle a \rangle >$. La mappa $\lceil r \in R \mapsto r\, \mathbf{v} \rceil \in \lceil R \longmapsto\!\triangleright \langle \mathbf{v} \rangle \rceil$ ha come nucleo $\langle a \rangle$ e quindi $\langle \mathbf{v} \rangle$ è isomorfo a $\boldsymbol{R}/\langle a \rangle$.
Inoltre se a è un elemento primo, allora $\langle a \rangle$ è ideale massimale in $\boldsymbol{R}$ e quindi $\boldsymbol{R}/\langle a \rangle$ costituisce un campo. ∎

(2) Prop.: Sia p un elemento primo e $\boldsymbol{M}$ un modulo su $\boldsymbol{R}$ tale che $p\,M = \{\mathbf{0}\}$.
Allora $\boldsymbol{M}$ è uno spazio vettoriale sopra $\boldsymbol{R}/\langle p\rangle$ con la moltiplicazione per uno scalare definita da

$$\forall \mathbf{v} \in M \;:\; \big(r + \langle p\rangle\big)\cdot \mathbf{v} \;:=\; r\cdot \mathbf{v}\ .$$

(3) Prop.: Sia p un elemento primo di $\boldsymbol{R}$ e sia S un sottomodulo di un modulo $\boldsymbol{M}$ su $\boldsymbol{R}$.
Allora l'insieme $S^{(p)} \;:=\; \{v \in S \,\big[\!\big]\, p\,\mathbf{v} = \mathbf{0}\}$ è un sottomodulo di $\boldsymbol{M}$.
Inoltre se si ha la decomposizione $\boldsymbol{M} = S \oplus T$, allora $\boldsymbol{M}^{(p)} = S^{(p)} \oplus T^{(p)}$.

T25**d.12** Sia $\boldsymbol{R}$ un Pid e sia $\boldsymbol{M}$ un modulo su $\boldsymbol{R}$ nonnullo, di torsione, primario, finitamente generato avente come ordine-G p^e. Sia inoltre $\boldsymbol{M} = \boldsymbol{C}_1 \oplus \cdots \oplus \boldsymbol{C}_k$, dove per $i = 1, ..., k$ $\boldsymbol{C}_i$ è un sottomodulo ciclico nonnullo avente ordine-G p_i^e e scegliamo gli indici in modo che sia $e_1 \geq e_2 \geq \cdots \geq e_k$.

Allora se si trova $\boldsymbol{M} = \boldsymbol{D}_1 \oplus \cdots \oplus \boldsymbol{D}_h$ dove per ogni $j = 1, ..., h$ D_j è un sottomodulo, nonnullo, ciclico avente ordine-G p^{f_j}, e $f_1 \geq f_2 \geq \cdots \geq f_h$, deve essere $h = k$, $e_1 = f_1$, ... , $e_k = f_k$ ∎

T25**d.13** **Teorema** (**decomposizione ciclica per moduli finitamente generati sopra un Pid**)
Sia $\boldsymbol{M}$ un modulo nonnullo sopra un Pid $\boldsymbol{R}$, finitamente generato. Allora

$$\boldsymbol{M} = \boldsymbol{M}_{\mathsf{trsn}} \oplus \boldsymbol{M}_{free}\ ,$$

dove $\boldsymbol{M}_{\mathsf{trsn}}$ è il sottomodulo sostenuto dall'insieme degli elementi di torsione di $\boldsymbol{M}$ ed $\boldsymbol{M}_{free}$ è un modulo libero il cui rango è determinato unicamente da $\boldsymbol{M}$.

Se $\boldsymbol{M}_{\mathsf{trsn}}$ ha ordine-G $p = {p_1}^{e_1} \cdots {p_k}^{e_k}$ con i P_i elementi primi di $\boldsymbol{R}$ distinti, allora si ha

$$\boldsymbol{M}_{\mathsf{trsn}} = \boldsymbol{M}_{p_1} \oplus \cdots \oplus \boldsymbol{M}_{p_k}\ ,\quad \text{dove}\quad \forall i = 1, ..., k \;:\; \boldsymbol{M}_{p_i} \;:=\; \{\mathbf{v} \in M \,\big[\!\big]\, {p_i}^{e_i}\ \mathbf{v} = \mathbf{0}\}\ ,$$

ciascuno di questi sottomoduli essendo primario e avente ordine-G pari a ${p_i}^{e_i}$.

Inoltre $\boldsymbol{M}_{p_i}$ si può decomporre come somma diretta di sottomoduli ciclici,

$$\boldsymbol{M}p_i \;=\; \boldsymbol{C}_{i,1} \oplus \cdots \oplus \boldsymbol{C}_{i,h_i}\ ,$$

aventi, risp., ordini-G ${p_i}^{e_{i,j}}$ con $e_i = e_{i,1} \geq e_{i,2} \geq \cdots \geq e_{i,h_i}$.

Gli ordini-G $p_{i\,i,j}^{e}$ sono detti **divisori elementari** di $\boldsymbol{M}$ e sono determinati univocamente dal modulo $\boldsymbol{M}$ a meno di un fattore consistente in una unità-I.

Questo conduce alla decomposizione della forma

$$\boldsymbol{M} \;=\; \Big(\boldsymbol{C}_{1,1} \oplus \cdots \oplus \boldsymbol{C}_{1,h_1}\Big) \;\oplus \cdots \oplus \Big(\boldsymbol{C}_{k,1} \oplus \cdots \oplus \boldsymbol{C}_{k,h_k}\Big)\ .$$