1 Teoria dei moduli

1.1 Moduli

Introduciamo ora il concetto di modulo, una generalizzazione del concetto di spazio vettoriale in cui gli scalari costituiscono un anello e non necessariamente un campo.

Definizione

Sia R un anello. Un gruppo abeliano $(M, \oplus)$ dotato di un'operazione $*\colon R \times M \to M$ si dice <u>R-modulo sinistro</u> se per ogni $r, r_1, r_2 \in R$ e $m, m_1, m_2 \in M$ si ha che:
(i) $(r_1 + r_2) * m = r_1 * m \oplus r_2 * m$ (distributività sinistra);
(ii) $r * (m_1 \oplus m_2) = r * m_1 \oplus r * m_2$ (distributività destra);
(iii) $r_1 * (r_2 * m) = (r_1 r_2) * m$ (associatività);
(iv) $1_R * m = m$.

Analogamente, un R-modulo destro è un gruppo abeliano $(M, \oplus)$ dotato di un'operazione $*\colon M \times R \to M$ per cui valgono proprietà analoghe ma con gli elementi di R scritti a destra. Se R è un anello commutativo, i concetti di R-modulo destro e sinistro coincidono.[1]

Esempio. Ogni spazio vettoriale V su un campo $\mathbb{K}$ può essere pensato come un $\mathbb{K}$-modulo, dove $*\colon \mathbb{K} \times V \to V$ è la moltiplicazione per scalari. Viceversa, essendo $\mathbb{K}$ commutativo, ogni $\mathbb{K}$-modulo è bilatero e può quindi essere pensato come uno spazio vettoriale su $\mathbb{K}$. $\square$

Esempio. Ogni gruppo abeliano G può essere visto come un modulo sull'anello degli interi. Si consideri l'operazione $*\colon \mathbb{Z} \times G \to G$ definita come $0 * g = 0_G$, $n * g = g + g + \ldots + g$ (somma di n termini) e $(-n) * g = -(n * g)$ per ogni $n > 0$ e $g \in G$. Si verifica facilmente che G dotato di tale operazione soddisfa le proprietà (i)-(iv) ed è quindi uno $\mathbb{Z}$-modulo. $\square$

Esempio. Sia R un anello e sia $I \lhd R$ un ideale sinistro. Allora, I è un R-modulo sinistro, dove $*\colon R \times I \to I$ è il prodotto dell'anello R, ed è ben definito in quanto per definizione di ideale sinistro $r * a = ra \in I$ per ogni $r \in R$ e $a \in I$. $\square$

Esempio. Sia R un anello e sia n un intero positivo. Si consideri il prodotto cartesiano $R^n = \{(r_1, \ldots, r_n) : r_1, \ldots, r_n \in R\}$ dotato della moltiplicazione componente per componente $*\colon R \times R^n \to R^n$ definita come $r * (r_1, \ldots, r_n) = (rr_1, \ldots, rr_n)$. Si verifica facilmente che R^n dotato di tale operazione soddisfa le proprietà (i)-(iv) ed è quindi un R-modulo sinistro. $\square$

L'esempio seguente è particolarmente importante nell'algebra lineare perché permette di dimostrare l'esistenza della forma canonica razionale e di Jordan di una matrice.[2]

Esempio. Sia V uno spazio vettoriale su un campo $\mathbb{K}$ e sia $\alpha \in \operatorname{End}_{\mathbb{K}}(V)$ un endomorfismo di V. Preso $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{K}[x]$, si consideri l'operazione $*_\alpha\colon \mathbb{K}[x] \times V \to V$ definita come $f *_\alpha v = f_\alpha(v)$, dove $f_\alpha = \sum_{i=0}^{n} a_i \alpha^i \in \operatorname{End}_{\mathbb{K}}(V)$.[3] Allora, si verifica facilmente che V dotato di tale operazione soddisfa le proprietà (i)-(iv) ed è quindi un $\mathbb{K}[x]$-modulo sinistro. $\square$

[1] Ogni modulo destro è isomorfo al corrispondente modulo sinistro, e si parla infatti di modulo bilatero.
[2] Riprenderemo questo argomento dopo il *Teorema di struttura per i gruppi abeliani finitamente generati*.
[3] Ricordiamo che l'insieme degli endomorfismi di un gruppo è un anello secondo le operazioni di somma puntuale e di composizione di funzioni. In questo caso, $a_i \alpha^i$ è l'endomorfismo che mappa $v \mapsto a_i \cdot \alpha^i(v)$, dove α^i indica la composizione $\underbrace{\alpha \circ \alpha \circ \ldots \circ \alpha}_{i \text{ volte}}$, inteso che $\alpha^0 = \mathrm{id}_V$.

Dimostriamo ora due proprietà dei moduli.

Proposizione 3.1.1

Sia R un anello e sia M un R-modulo sinistro. Allora,
(a) $0_R \cdot m = 0_M$ per ogni $m \in M$;
(b) $r \cdot 0_M = 0_M$ per ogni $r \in R$.

Dimostrazione. (a) Per la distributività sinistra $0_R \cdot m = (0_R + 0_R) \cdot m = 0_R \cdot m + 0_R \cdot m$. Dunque, sommando l'opposto $-0_R \cdot m$ ad entrambi i membri, otteniamo che $0_M = 0_R \cdot m$.
(b) Per la distributività destra $r \cdot 0_M = r \cdot (0_M + 0_M) = r \cdot 0_M + r \cdot 0_M$. Dunque, sommando l'opposto $-r \cdot 0_M$ ad entrambi i membri, otteniamo che $0_M = r \cdot 0_M$. ∎

Definizione

Sia R un anello e sia M un R-modulo sinistro. Un sottogruppo abeliano $A \subseteq M$ si dice R-sottomodulo di M se $r \cdot a \in A$ per ogni $r \in R$ e $a \in A$.

Un sottomodulo è quindi un sottogruppo abeliano $A \subseteq M$ per cui $(A, \cdot_{R\times A} \colon R \times A \to A)$ è di nuovo un R-modulo (sto quindi effettuando una restrizione dell'operazione $\cdot$).

Proposizione 3.1.2

Sia R un anello, M un R-modulo sinistro e sia $A \subseteq M$ un R-sottomodulo. Allora, $(M/A, \cdot \colon R \times M/A \to M/A)$ è un R-modulo sinistro, ove $r \cdot (m + A) = r \cdot m + A$ e $\overline{f}(r, m + A) = r \cdot m + A$.

Dimostrazione. Diagramma negli appunti cartacei. La dimostrazione è inesistente, ottimo. ∎

Proposizione 3.1.3

Sia R un anello, M un R-modulo sinistro, $A, B \subseteq M$ sono R-sottomoduli. Allora, $A + B = \{a + b : a \in A, b \in B\}$ è un R-sottomodulo di M.

Dimostrazione. Sappiamo già che $A+B \subseteq M$ è un sottogruppo abeliano. Siano $a+b \in A+B$ e $r \in R$. Allora, $r \cdot (a + b) = r \cdot a + r \cdot b \in A + B$ perché $r \cdot a \in A$ e $r \cdot b \in B$ per definizione di sottomodulo. ∎

Proposizione 3.1.4

Sia R un anello e M un R-modulo sinistro. Per $m \in M$ sappiamo che $R \cdot m = \{r \cdot m : r \in R\}$ è un R-sottomodulo di M. Siano $m_1, \dots, m_n \in M$. Allora, $\sum_{i=1}^{n} R \cdot m_i = R \cdot m_1 + \dots + R \cdot m_n = \{m \in M : \exists r_1, \dots, r_n \in R : m = \sum_{i=1}^{n} r_i \cdot m_i\}$ è un R-sottomodulo di M.

Dimostrazione. Usando distributività sx, $R \cdot m$ è un sottogruppo abeliano. Usando associatività, si conclude mostrando che $R \cdot m$ è un R-sottomodulo. Ora procediamo per induzione grazie alla *Proposizione 3.1.3.* ∎

Definizione

Sia R un anello e sia M un R-modulo sinistro. Definiamo numero minimo di generatori $d_R(M)$ il più piccolo $n \in \mathbb{N}$ per cui esistano $m_1, \dots, m_n \in M$ tali che $M = \sum_{i=1}^{n} R \cdot m_i$ Se tale $n \in \mathbb{N}$ non esiste, poniamo $d_R(M) = \infty$. Diciamo che M è finitamente generato se $d_R(M) < \infty$.

Lezione del 13/11/2019 (appunti grezzi)
Manca tutto un primo pezzo, Trenord ti voglio bene anche io
Esistono i corrispondenti dei 3 teoremi di isomorfismo per gli R-moduli.

Teorema 3.x.y: Primo teorema d'isomorfismo

Sia $\phi \colon M \to N$ un omomorfismo di R-moduli, dove R è un anello. Allora, l'omomorfismo indotto $\phi_\star \colon M/\ker(\phi) \to \operatorname{Im}(\phi)$ è un isomorfismo di R-moduli.

Dimostrazione. Dimostrazione mancante. ∎

Teorema 3.x.y: Secondo teorema d'isomorfismo

Sia R un anello, M un R-modulo, e siano $A, B \subseteq M$ degli R-sottomoduli. Allora, esiste un isomorfismo di R-moduli $\pi_\star \colon A/(A \cap B) \to (A + B)/B$.

Dimostrazione. Sia $\tau \colon M \to M/B$ la proiezione canonica, cioè $\tau(m) = m + B$, e sia la restrizione $\tau_A = \pi$. Allora, per il *Primo teorema d'isomorfismo* la mappa $\pi_{star} \colon A/\ker(\pi) \to \operatorname{Im}(\pi)$ è un isomorfismo. Poiché $\ker(\pi) = \ker(\tau) \cap A = B \cap A$ e $\operatorname{Im}(\pi) = \{a + B : a \in A\} = (A + B)/B$, abbiamo concluso. ∎

Teorema 3.x.y: Terzo teorema d'isomorfismo

Sia R un anello, M un R-modulo, $A \subseteq B \subseteq M$ degli R-sottomoduli. Allora, esiste un isomorfismo di R-moduli $\psi_\star \colon (M/A)/(B/A) \to M/B$.

Dimostrazione. Sia $\psi \colon M/A \to B/A$ la mappa definita come $\psi(m + A) = m + B$. Poiché ψ è un omomorfismo di R-moduli, per il *Primo teorema d'isomorfismo* la mappa indotta $\psi_\star \colon (M/A)/\ker(\psi) \to \operatorname{Im}(\psi)$ è un isomorfismo. Essendo $\operatorname{Im}(\psi) = \{m+B : m \in M\} = M/B$ e $\ker(\psi) = \{m+A : m \in M, m+B = B\} = \{m+A : m \in B\} = B/A$, abbiamo concluso. ∎

Proposizione

Sia R un anello, M un R-modulo sinistro e $B \subseteq M$ un R-sottomodulo di M. Allora $d_R(M) \leq d_R(B) + d_R(M/B)$ e $d_R(M/B) \leq d_R(M)$.

Dimostrazione. Se B o M/B non sono finitamente generati, cioè $d_R(B) = \infty$ o $d_R(M/B) = \infty$, la prima equazione è banalmente vera. Siano quindi $d_R(B) = k < \infty$ e $d_R(M/B) = n < \infty$. Allora, esistono $m_1, \dots, m_k \in B$ tali che $B = \sum_{i=1}^{k} R \cdot m_i$ ed esistono $t_1, \dots, t_n \in M$ tali che $M/B = \sum_{i=1}^{n} R \cdot (t_i + B)$. Dunque, per ogni $m \in M$ esistono $r_1, \dots, r_n \in R$ tali che $m + B = \sum_{i=1}^{n} r_i \cdot (t_i + B)$, cioè $m - \sum_{i=1}^{n} r_i \cdot t_i \in B$. Allora, esistono $s_1, \dots, s_k \in R$ tali che $m - \sum_{i=1}^{n} r_i \cdot t_i = \sum_{j=1}^{k} s_j \cdot m_j$, da cui $m = \sum_{i=1}^{n} r_i \cdot t_i + \sum_{j=1}^{k} s_j \cdot m_j$, cioè $d_R(M) \leq n + k$.

Per quanto riguarda la seconda disuguaglianza, possiamo assumere che $d_R(M) = n < \infty$, altrimenti è banalmente vera. Dunque, esistono $m_1, \dots, m_n \in M$ tali che $M = \sum_{i=1}^{n} R \cdot m_i$, quindi per ogni $m \in M$ esistono $r_1, \dots, r_n \in R$ tali che $m = \sum_{i=1^n} r_i \cdot m_i$, da cui $m + B = \sum_{i=1}^{n} r_i \cdot (m_i + B)$, e per l'arbitrarietà di M significa che $M/B = \sum_{i=1}^{n} R \cdot (m_i + B)$. Dunque, $d_R(M/B) \leq n$ come desiderato. ■

Proposizione

Sia R un anello commutativo. Allora, R è noetheriano se e solo se ogni sottomodulo di un R-modulo finitamente generato è finitamente generato.

Dimostrazione. Procediamo per induzione su $d = d_R(M)$. Se $d = 1$, esiste $m \in M$ tale che $M = R \cdot m$. Sia $\tau_m \colon R \to M$ la mappa definita come $\tau_m(r) = r \cdot m$. Osserviamo che $\tau_m(0) = 0$, $\tau_m(r_1 + r_2) = \tau_m(r_1) + \tau_m(r_2)$ e $\tau_m(r \cdot r_1) = r \cdot r_1 \cdot m = r \cdot \tau_m(r_1)$, quindi τ_m è un omomorfismo di R-moduli. Sia $B \subseteq M$ un R-sottomodulo e sia $I_B = \{r \in R : \tau_m(r) \in B\} \subseteq R$. Poiché I_B è un sottogruppo abeliano e presi $a \in I_B$ e $r \in R$ sappiamo che $r \cdot a \in I_B$ essendo B un sottomodulo, vale $I_B \lhd R$. Dunque, essendo R noetheriano per ipotesi, esistono $a_1, \dots, a_n \in I_B$ tale che $I_B = \langle a_1, \dots, a_n \rangle$. Poiché $B = \tau_m(I_B) = \operatorname{Im}(\tau_m|_{I_B})$, per la proposizione precedente concludiamo che $d_R(B) < \infty$. Supponiamo ora per induzione forte che tale affermazione valga per $k \leq d$, e mostriamo che vale per $d + 1$. Sia M un R-modulo sinistro con $d_R(M) = d + 1$. Allora, esistono $m_0, \dots, m_d \in M$ tali che $M = \sum_{k=0}^{d} R \cdot m_k$. Sia $B \subseteq M$ un sottomodulo e sia $M_\star = \sum_{k=1}^{d} R \cdot m_k$. Poiché $d_R(M_\star) \leq d$, $M/M_\star = R \cdot (m_0 + M_\star)$. Sia $\pi \colon M \to M/M_\star$ la proiezione canonica, dove $d_R(M/M_\star) \leq 1$. Per ipotesi induttiva, $d_R(B \cap M_\star) < \infty$, quindi $d_R(\pi(B)) < \infty$. Poiché $\pi(B) = (B + M_\star)/M_\star \subseteq M/M_\star$, per la proposizione precedente $d_R(B) \leq d_R(B \cap M_\star) + d_R(B/(B \cap M_\star))$. Ma per ipotesi induttiva sappiamo che $d_R(B \cap M_\star) < \infty$ e $B/(B \cap M_\star) \simeq \pi(B)$ per il *Secondo teorema d'isomorfismo*, quindi $d_R(B/(B \cap M_\star)) < \infty$ e $d_R(B) < \infty$, da cui la tesi.

Viceversa, sia $M = R$ con il prodotto di R (tale R-modulo è detto R-modulo regolare).[4] Poiché $B \subseteq R$ è un sottomodulo se e solo se $B \lhd R$ è un ideale, per ipotesi sappiamo che $d_R(B) < \infty$ pensando B come sottomodulo, cioè $d_R(B) < \infty$ pensando ora B come ideale, da cui R è noetheriano. ■

[4] Sto pensando $M = R$ come gruppo abeliano secondo il prodotto di R, essendo R commutativo.