

## Lezione 9

### **Moduli finitamente generati.**

Richiamiamo preliminarmente un importante enunciato dell'algebra lineare.

**Proposizione 9.1** Sia  $K$  un campo, e sia  $C = (c_{ij})_{i,j=1,\dots,n}$  una matrice  $n \times n$  a coefficienti in  $K$ . Allora

- a) la matrice  $C$  è invertibile se e solo se  $\det C \neq 0$ ;
- b) il sistema lineare omogeneo

$$\sum_{j=1}^n c_{ij} x_j = 0 \quad (i = 1, \dots, n)$$

di  $n$  equazioni in  $n$  incognite ha solo la soluzione banale se e solo se  $\det C \neq 0$ .

Vediamo come la Proposizione 9.1 cambia se si sostituisce al campo  $K$  un anello commutativo unitario  $A$ . Sia  $C = (c_{ij})_{i,j=1,\dots,n}$  una matrice  $n \times n$  a coefficienti in  $A$ .

**Proposizione 9.2** La matrice  $C$  è invertibile se e solo se  $\det C$  è invertibile.

Dimostrazione: Se  $C$  è invertibile, esiste  $C'$ , una matrice  $n \times n$  a coefficienti in  $A$ , tale che

$$CC' = I_n,$$

essendo  $I_n$  la matrice identità. Allora, per il Teorema di Binet,

$$1 = \det I_n = \det(CC') = \det C \det C'.$$

Segue che  $\det C$  è invertibile. Viceversa, supponiamo che  $\det C$  sia invertibile. Allora, detto, per ogni  $i, j = 1, \dots, n$ ,  $C_{ij}$  il complemento algebrico di  $c_{ij}$  in  $C$ , la matrice

$$C' = (C_{ji} (\det C)^{-1})_{i,j=1,\dots,n}$$

è la matrice inversa di  $C$ .

Prima di enunciare il prossimo risultato, è utile introdurre alcuni termini e simboli.

Per  $1 \leq t \leq n$ , si dice *minore di ordine  $t$*  il determinante di una sottomatrice  $t \times t$  di  $C$ . Se tale sottomatrice è formata dall'intersezione delle righe di indici  $i_1, \dots, i_t$  e delle colonne di indici  $j_1, \dots, j_t$ , indicheremo il minore con  $[i_1, \dots, i_t \mid j_1, \dots, j_t]$ . Denoteremo, inoltre, con  $M_t$  l'ideale di  $A$  generato dai minori di ordine  $t$  di  $C$ .

**Proposizione 9.3** Il sistema lineare omogeneo

$$(*) \quad \sum_{j=1}^n c_{ij}x_j = 0 \quad (i=1, \dots, n)$$

di  $n$  equazioni in  $n$  incognite ha solo la soluzione banale se e solo se  $\det C$  non è un divisore dello zero.

Dimostrazione: Se  $n=1$ , allora la tesi è ovvia. Supponiamo quindi che sia  $n > 1$ .

Supponiamo dapprima che  $\det C$  sia un divisore dello zero, e proviamo che il sistema (\*) ha una soluzione non banale. Si ha che  $\text{Ann}(M_n) = \text{Ann}(\det C) \neq (0)$ . Se  $\text{Ann}(M_1) \neq (0)$ , e  $b \in \text{Ann}(M_1), b \neq 0$ , allora  $bc_{ij} = 0$  per ogni  $i, j = 1, \dots, n$ , quindi  $(b, \dots, b)$  è una soluzione non banale di (\*). Supponiamo allora che  $\text{Ann}(M_1) = (0)$ . Sia  $t = \max\{i \mid \text{Ann}(M_i) = (0)\}$ . Allora  $1 \leq t \leq n-1$ . Sia  $b \in \text{Ann}(M_{t+1}), b \neq 0$ . Allora  $b \notin \text{Ann}(M_t)$ . Possiamo supporre, a meno di permutare righe e colonne, che  $b[1, \dots, t \mid 1, \dots, t] \neq 0$ . Sia  $D$  la sottomatrice di  $C$  formata dalle righe e dalle colonne di indici  $1, \dots, t+1$ . Per ogni  $j = 1, \dots, t+1$ , consideriamo il complemento algebrico  $d_j = D_{t+1, j}$ . Si ha

$$\sum_{j=1}^{t+1} c_{ij}d_j = \begin{cases} 0 & \text{se } 1 \leq i \leq t \\ [1, \dots, t, i \mid 1, \dots, t, t+1] & \text{se } t+1 \leq i \leq n \end{cases}$$

Segue che

$$b \sum_{j=1}^{t+1} c_{ij}d_j = 0 \quad \text{per ogni } 1 \leq i \leq n.$$

Quindi  $(bd_1, \dots, bd_{t+1}, 0, \dots, 0)$  è una soluzione di (\*). Poiché  $d_{t+1} = [1, \dots, t \mid 1, \dots, t]$ , si ha  $bd_{t+1} \neq 0$ , e dunque tale soluzione è non banale.

Viceversa, supponiamo che esista una soluzione  $Y = (y_1, \dots, y_n)$  non banale di (\*). Possiamo supporre che  $y_1 \neq 0$ . Detta  $C^*$  la matrice aggiunta di  $C$ , si ha  $(\det C)Y^t = C^*CY^t = 0$ , da cui, in particolare,  $y_1 \det C = 0$ . Ciò prova che  $\det C$  è un divisore dello zero.

**Proposizione 9.4** Sia  $M$  un  $A$ -modulo libero di rango  $m$ . Sia  $N$  un suo sottomodulo libero di rango  $n$ . Allora  $n \leq m$ .

Dimostrazione: Sia  $u_1, \dots, u_m$  una base di  $M$  e sia  $v_1, \dots, v_n$  una base di  $N$ . Esistono  $c_{ij} \in A$ ,  $i=1, \dots, m, j=1, \dots, n$ , tali che

$$v_j = \sum_{i=1}^m c_{ij}u_i \quad \text{per ogni } j=1, \dots, n.$$

Poiché  $v_1, \dots, v_n$  sono linearmente indipendenti su  $A$ , per ogni  $a_1, \dots, a_n \in A$ ,

$$\sum_{j=1}^n a_j v_j = 0 \Rightarrow a_j = 0 \quad \text{per ogni } j=1, \dots, n. \quad (1)$$

Ora:

$$\sum_{j=1}^n a_j v_j = \sum_{j=1}^n a_j \sum_{i=1}^m c_{ij} u_i = \sum_{i=1}^m \left( \sum_{j=1}^n a_j c_{ij} \right) u_i.$$

Quindi  $\sum_{j=1}^n a_j v_j = 0 \Leftrightarrow \sum_{j=1}^n a_j c_{ij} = 0$  per ogni  $i = 1, \dots, m$ . Pertanto la (1) equivale alla seguente condizione: il sistema lineare omogeneo

$$\sum_{j=1}^n c_{ij} x_j = 0 \quad (i = 1, \dots, m) \quad (2)$$

in  $m$  equazioni ed  $n$  incognite ha solo la soluzione banale. Supponiamo per assurdo che  $m < n$ . Riscriviamo (2) nella forma

$$\sum_{j=1}^m c_{ij} x_j = - \sum_{j=m+1}^n c_{ij} x_j \quad (i = 1, \dots, m) \quad (3)$$

Poniamo  $x_j = 0$ , per  $j = m+1, \dots, n$  ed otteniamo

$$\sum_{j=1}^m c_{ij} x_j = 0 \quad (i = 1, \dots, m), \quad (4)$$

un sistema lineare omogeneo di  $m$  equazioni in  $m$  incognite, che ha per ipotesi solo la soluzione banale. Allora, per la Proposizione 9.3, posto  $C = (c_{ij})_{i,j=1,\dots,m}$ , segue che  $d = \det C$  non è un divisore dello zero in  $A$ . Consideriamo  $A_d, M_d, N_d$ , le localizzazioni di  $A, M, N$  rispetto all'insieme moltiplicativo  $\{1, d, d^2, \dots\}$ . Essendo  $v_{m+1} \neq 0$ , esiste un indice  $i$  tale che  $c_{im+1} \neq 0$ . In (3) poniamo  $x_{m+1} = 1$  e  $x_j = 0$  per ogni  $j = m+2, \dots, n$ . Otteniamo così:

$$\sum_{j=1}^m c_{ij} x_j = -c_{im+1} \quad (i = 1, \dots, m) \quad (5)$$

A patto di identificare  $c_{ij}$  con  $\frac{c_{ij}}{1}$ , (5) è un sistema lineare (non omogeneo) di  $m$  equazioni in  $m$  incognite a coefficienti in  $A_d$ . Il determinante della matrice incompleta dei coefficienti è  $d$ , che è invertibile in  $A_d$ . Quindi, applicando la regola di Cramer, è facile concludere che (5) ha una soluzione  $(\frac{y_1}{d^{s_1}}, \dots, \frac{y_m}{d^{s_m}})$ , evidentemente non banale. Possiamo supporre che  $y_1 \neq 0$ . Sia  $s = \max_{j=1,\dots,m} s_j$ . Allora

$$d^s \sum_{j=1}^m c_{ij} \frac{y_j}{d^{s_j}} = -d^s c_{im+1} \quad (i = 1, \dots, m)$$

e quindi

$$\sum_{j=1}^m c_{ij} d^{s-s_j} y_j + c_{im+1} d^s + \sum_{j=m+2}^n c_{ij} 0 = 0 \quad (i=1, \dots, m)$$

ovvero  $(d^{s-s_1} y_1, \dots, d^{s-s_m} y_m, d^s, 0, \dots, 0)$  è una soluzione di (2). Essa non è banale, perché  $d^{s-s_1} y_1 \neq 0$ . Ciò costituisce la contraddizione cercata.

La Proposizione 9.4 ci fornisce la soluzione dell'Esercizio 4.5 b): se  $f: A^n \rightarrow A^m$  è un omomorfismo iniettivo, allora  $\text{Im } f$  è un sottomodulo libero di  $A^m$  di rango  $n$ , quindi  $n \leq m$ .

L'ipotesi, contenuta nella Proposizione 9.4, che  $N$  sia un sottomodulo *libero*, è una necessaria precisazione. Infatti, in generale, il sottomodulo di un modulo libero non è libero, come mostrano i seguenti

### Esempi 9.5

- Nell'anello  $\mathbf{Z}_6$ , l'ideale  $([2]_6)$  non è un sotto- $\mathbf{Z}_6$ -modulo libero di  $\mathbf{Z}_6$ . Infatti nessun elemento di questo ideale è libero.
- Nell'anello  $K[x, y]$ , l'ideale  $(x, y)$  non è un modulo libero su  $K[x, y]$ . Infatti nessun insieme avente un solo elemento di  $K[x, y]$  è un sistema di generatori, e nessun insieme avente più di un elemento è libero.

Nell'Esempio 9.5 a) l'anello non è integro, nell'Esempio 9.5 b) l'anello non è ad ideali principali. In realtà, quando valgono entrambe le proprietà, l'ipotesi che  $N$  sia un sottomodulo *libero* può essere rimossa dalla Proposizione 9.4.

**Proposizione 9.6** Sia  $A$  un PID, e sia  $M$  un  $A$ -modulo libero di rango  $m$ . Sia  $N$  un suo sottomodulo. Allora  $N$  è libero di rango  $n \leq m$ .

Dimostrazione: Sia  $u_1, \dots, u_m$  una base di  $M$ . Per ogni  $i = 1, \dots, m$  sia  $M_i = \sum_{k=1}^i A u_k$ , e definiamo

l'applicazione

$$\begin{aligned} \varphi_i: M_i &\rightarrow A \\ x &\mapsto a_i \end{aligned} \quad \text{se } x = \sum_{k=1}^i a_k u_k,$$

che è, evidentemente, un omomorfismo di moduli. Per ogni  $i = 1, \dots, m$ ,  $\varphi_i(M_i \cap N)$  è un ideale di  $A$ ; poiché  $A$  è un anello ad ideali principali, esiste  $c_i \in A$  tale che  $\varphi_i(M_i \cap N) = (c_i)$ . Sia, inoltre,  $y_i \in M_i \cap N$  tale che  $\varphi_i(y_i) = c_i$ . Sia  $J = \{i \mid c_i \neq 0\}$ . Proviamo che allora  $Y = \{y_i \mid i \in J\}$  è una base di  $N$ . Proviamo anzitutto che  $Y$  è un sistema di generatori, supponendo, per assurdo, che esista

$z \in N$  tale che  $z \notin \sum_{i \in J} A y_i$ . Si ha che  $z \in M_m \cap N = N$ . Sia  $\hat{i}$  il minimo indice per cui esiste

$z \in M_{\hat{i}} \cap N$  tale che  $z \notin \sum_{i \in J} A y_i$ . Allora  $z = \sum_{k=1}^{\hat{i}} a_k u_k$ , e  $\varphi_{\hat{i}}(z) = a_{\hat{i}} \neq 0$ . Inoltre

$\varphi_{\hat{i}}(z) \in (c_{\hat{i}}) = (\varphi_{\hat{i}}(y_{\hat{i}}))$ , con  $y_{\hat{i}} \in M_{\hat{i}} \cap N$ . Se  $\hat{i} \notin J$ , allora  $c_{\hat{i}} = 0$  e  $\varphi_{\hat{i}}(z) = 0$ , contraddizione.

Quindi  $\hat{i} \in J$ , e  $\varphi_{\hat{i}}(z) = \varphi_{\hat{i}}(d y_{\hat{i}})$  per qualche  $d \in A$ . Ora  $z - d y_{\hat{i}} \in M_{\hat{i}} \cap N$ , ma  $\varphi_{\hat{i}}(z - d y_{\hat{i}}) = 0$ .

Pertanto  $z - dy_i \in M_{\hat{i}-1} \cap N$ . Inoltre  $z - dy_i \notin \sum_{i \in J} Ay_i$ . Ciò contraddice la minimalità di  $\hat{i}$ . Abbiamo così provato che  $Y$  è un sistema di generatori di  $N$ . Per provare che è un insieme libero, supponiamo che

$$\sum_{i \in J} a_i y_i = 0 \quad (a_i \in A)$$

Sia  $j = \max\{i \in J\}$ . Allora  $0 = \varphi_j(\sum_{i \in J} a_i y_i) = \varphi_j(a_j y_j + \sum_{\substack{i \in J \\ i < j}} a_i y_i) = \varphi_j(a_j y_j) = a_j c_j$ . Essendo

$c_j \neq 0$ , ed essendo  $A$  integro, segue che  $a_j = 0$ . Per induzione finita discendente si prova che  $a_i = 0$  per ogni  $i \in J, i < j$ .

**Osservazione 9.7** Nella dimostrazione della Proposizione 9.6 abbiamo utilizzato la principalità dell'anello per provare che l'insieme  $Y$  è un sistema di generatori, l'integrità per provare che  $Y$  è un insieme libero.

L'enunciato della Proposizione 9.6 vale anche nel caso in cui il modulo  $M$  non sia finitamente generato: basta adattare la nostra dimostrazione, assumendo che una base sia indicata su un insieme bene ordinato.

Utilizzando la Proposizione 9.6, insieme ad ulteriori argomenti di algebra lineare, è possibile provare il

**Teorema 9.8** Sia  $A$  un PID. Sia  $M$  un  $A$ -modulo finitamente generato. Allora

$$M = M_1 \oplus \dots \oplus M_s,$$

ove, per ogni  $i = 1, \dots, s$ ,  $M_i$  è un sottomodulo generato da un elemento. Inoltre, questa decomposizione è unica a meno di isomorfismi.

**Nota** Il Teorema 9.8 è noto come *Teorema fondamentale di struttura per i moduli finitamente generati sui domini ad ideali principali*. Esso fornisce, in particolare, un teorema di struttura per i gruppi abeliani finiti (vedi Algebra 2, [Teorema 27.1](#)).

**Esercizio 9.9\*** Sia  $M$  un  $A$ -modulo e sia  $N$  un suo sottomodulo. Se  $M/N$  ed  $N$  sono finitamente generati, anche  $M$  è finitamente generato.