Lezione 11 Algebra 1

Federico De Sisti

2025-04-14

0.1 Boh

Obiettivo
Dare un teorema di struttura per i moduli finitamente generati su R PID

Lemma 1 (Esercizio)
R PID, $N \subseteq R^n$ sottomodulo. Supponiamo che esista un elemento $m \in N$ tale che $m = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ di lunghezza minimale in N
allora $l(m)$ è di lunghezza minima in N

Ricordiamo la definizione di lunghezza minimale:
$l(m) \in R/\approx, l(m) = [d]$ $l(m)$ è un elemento minimale nell'insieme
$\{l(m') \in R/\approx \mid m' \in N\}$

Dimostrazione
Sia $a = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in N \subseteq R$
Dimostriamo che $d \mid a_j \ \forall j \in \{1, \dots, n\}$
(se vero, allora $d \mid MCD(a_1, \dots, a_n)$ *quindi* $[d] \preceq l(a))$
Procediamo in due passi:

I. Step $d \mid a_1$ *a priori abbiamo* $d_1 = MCD(d, a_1)$ *la tesi diventa* $d_1 = d$
Per l'identità di Bezout, $\exists h, k \in R \ : \ d_1 = hd + ka_1$
Allora
$b := hm + ka \in N$ *(combinazione lineare di elementi in N)*
$b = \begin{pmatrix} hd+ka_1 \\ ka_2 \\ \vdots \\ ka_n \end{pmatrix} = \begin{pmatrix} d_1 \\ ka_2 \\ \vdots \\ ka_n \end{pmatrix} \in N$
Quindi: $b \in N$ *soddisfa*

$$l(b) \preceq [d_1] \preceq [d] = l(m).$$

Per la minimalità di m in $N \Rightarrow l(b) = l(m) \Rightarrow [d_1] = [d] \Rightarrow d \mid a_1$

II. step $d \mid a_j \quad \forall j \in \{1, \dots, n\}$
Dato che $d \mid a_1 \quad \exists h \in R$ *tale che* $a_1 = hd$

$$c := (1-h)m + a \in N$$

Osserviamo che

$$c = \begin{pmatrix} (1-h)d + a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = \begin{pmatrix} d \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

Quindi $c \in N$ *soddisfa*
$l(c) \preceq [d] = l(m)$
Per minimalità di m *in* N
$l(c) = [d]$
Allora $d \mid a_j \quad \forall j \in \{2, \dots, n\}$

□

Lemma 2 (Esercizio)
Sia R *PID* $N \subseteq R \oplus R^{n+1} = R \oplus R^n$ *sottomodulo di* R^n*, Supponiamo che esista un elemento di lunghezza minimale* $m = \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}$
Allora esiste un R*-sottomodulo* $N' \subseteq R^n$ *tale che* $N = (d) \oplus N'$

Dimostrazione
Consideriamo $N' = \{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in R^n \mid \begin{pmatrix} 0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} \in N \}$
Consideriamo la doppia inclusione:

- $(d) \oplus N' \subseteq N$
  infatti
  $$r_1 \begin{pmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + r_2 \begin{pmatrix} 0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} \in N.$$
  poiché combinazione di elementi in N

- *Viceversa, verifichiamo* $N \subseteq (d) \oplus N'$
  Sia $\begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} \in N$
  abbiamo dimostrato nel lemma precedente che $d \mid a_0 \Rightarrow a_0 = hf$
  $\Rightarrow \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} = h \begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix} \in (d) \oplus N$

□

Teorema 1 (Struttura dei sottomoduli di moduli liberi di rango finito)
R PID, $N \subseteq R^n$ sottomodulo
Allora esistono $d_1, \dots, d_n \in R$:

1. $d_1 = \min\{l(m') \mid m' \in N\}$
2. $d_j \mid d_{j+1} \quad \forall j \in \{1, \dots, n-1\}$
3. *esiste un isomorfismo di R-moduli, $\phi : R \to R^n$ tale che* $\phi(N) = (d_1) \oplus \dots \oplus (d_n)$

Dimostrazione
Per induzione su n

- *$n = 1$ allora $N \subseteq R$ è un ideale, quindi R $PID \Rightarrow N = (d_1)$*
- *$n > 1$ assumiamo l'enunciato per sottomoduli di R^n e dimostriamolo per sottomoduli di R^{n+1}*
  Sia $N \subseteq R^{n+1}$ R-sottomodulo
  e sia $m \in N$ un elemento di lunghezza minimale in N (sappiamo che esiste!)
  Esiste anche un isomorfismo di R-moduli $\phi_1 : R^{n+1} \to R^{n+1}$
  tale che $\phi(m) = \begin{pmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$
  Ora $\phi(m)$ è di lunghezza minima in $\phi(N)$
  Quindi esiste un complementare $N' \subseteq R^n$ tale che
  $\phi_1(N) \cong (d_1) \oplus N'$
  Per ipotesi induttiva a meno di un isomorfismo $\phi_2 : R^n \to R^n$ abbiamo $\phi_2(N) = (d_2) \oplus \dots \oplus (d_{n+1})$
  Abbiamo:
  $N \xrightarrow{\phi_1} (d_1) \oplus N' \xrightarrow{id \oplus \phi_2} (d) \oplus \phi_2(N') = (d_1) \oplus \dots \oplus (d_{n+1})$

□

Teorema 2 (Struttura dei moduli finitamente generati su PID)
R PID M R-modulo finitamente generato
Allora esistono $d_1, \dots d_n \in R$ tali che

- $d_j \mid d_{j+1} \quad j \in \{1, \dots, n-1\}$
- $M \cong R/(d_1) \oplus \dots \oplus R/(d_n)$

Dimostrazione
Siano $\{m_1, \dots, m_n\}$ generatori di M.

Allora consideriamo l'omomorfismo suriettivo di R-moduli

$$\begin{aligned} R^n &\to M \\ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} &\to \sum_{n}^{j=1} a_j m_j \end{aligned}.$$

Dal primo teorema di isomorfismo segue

$$M \cong R^n / ker(\phi).$$

Dato che $ker(\phi)$ è un R-sottomodulo di R^n esistono $d_1, \ldots, d_n \in R$ tali che

1. $d_j \mid d_{j+1} \quad \forall j \in \{1, \ldots, n-1\}$
2. $ker(\phi) \cong (d_1) \oplus \ldots \oplus (d_n)$

$\Rightarrow M \cong R^n/ker(\phi) \cong R/((d) \oplus \ldots \oplus (d_n)) \cong R/(d_1) \oplus \ldots \oplus R/(d_n)$ □

Osservazione:

1. Alcuni d_j possono essere nulli o anche ripetersi.
2. La scelta dei d_j è "unica" (esercizio)
3. Un gruppo abeliano G ha un'unica possibile struttura di $\mathbb{Z}$-modulo. Quindi i concetti di gruppo abeliano e di $\mathbb{Z}$-modulo sono equivalenti.

Corollario 1
G gruppo abeliano, Allora esistono $d_1, \ldots, d_n \in \mathbb{Z}$ tali che

1. $d_j \mid d_{j+1} \quad \forall j \in \{1, \ldots, n-1\}$
2. $G \cong \mathbb{Z}/(d_1) \oplus \ldots \oplus \mathbb{Z}/(d_n)$

Dimostrazione
Segue dal teorema con $R = \mathbb{Z}$ □

Osservazione
G gruppo abeliano

$$\begin{aligned} \mathbb{Z} \times G &\to G \\ (n, g) &\to g + \ldots + g(\text{n volte}) \end{aligned}.$$

1 Successioni esatte corte

Su R anello

Definizione 1
Una successione esatta corta di R-moduli è una coppia di omeomorfismi

$$M' \xrightarrow{i} M \xrightarrow{\pi} M''.$$

tali che

1. *i iniettiva*
2. *π suriettiva*
3. $\ker(\pi) = im(i)$

Esercizio
Dimostrare che

1. M finitamente generato $\Rightarrow M''$ finitamente generato.
2. M', M'' finitamente generati $\Rightarrow M$ finitamente generato.

Soluzione
1)$\{m_1, \dots, m_n\}$ generatori di M
Allora dato che π è suriettiva
$\{\pi(m_1), \dots, \pi(m_n)\}$ sono generatori di M''.
$\{m'_1, \dots, m'_h\}$ generatori di M'
$\{m''_1, \dots, m''_k\}$ generatori di M''
Considero $\{m_1, \dots, m_k\} \subseteq M$ tali che
$\pi(m_j) = m''_j \quad \forall j \in \{1, \dots, k\}$
Dimostriamo che

$$\{i(m'_1), \dots, i(m'_h), m_1, \dots, m_k\}.$$

sono generatori di M
Sia $m \in M$

$$\Rightarrow \pi(m) = \sum_{j=1}^{k} r_j m''_j \in M'' = \pi(\sum_{j=1}^{k} r_j m_j)$$

$$\Rightarrow m - \sum_{j=1}^{k} r_j m_j \in \ker(\pi) = im(i), \text{ che è generata da } \{i(m'_1), \dots, i(m'_n)\}$$