UNIVERSITÀ CATTOLICA DEL SACRO CUORE

Facoltà di Scienze Matematiche, Fisiche e Naturali

APPROFONDIMENTI DI ALGEBRA

M. Chiara Tamburini

Anno Accademico 2013/2014

Indice

Prefazione

Il corso di *Approfondimenti di Algebra*, rivolto a studenti del terzo anno della triennale in matematica, consta di 20 ore di lezione e 20 di esercitazioni. Esso presuppone *Algebra* 1, *Algebra* 2 e *Algebra lineare* per i cui contenuti, in parte riassunti nel primo capitolo, rimando a [8].

La trattazione è incentrata sul teorema di struttura dei moduli finitamente generati su un dominio a ideali principali. Si tratta di un risultato centrale in algebra, che unifica concetti apparentemente scollegati e che, come tale, ha parecchie applicazioni. Due di queste vengono sviluppate, e offrono ampio materiale per le esercitazioni: la struttura dei gruppi abeliani finitamente generati e le forme canoniche delle matrici.

I temi considerati e la loro impostazione derivano da un bellissimo libro di B.Hartley e T.O.Hawkes [4], ai quali va la mia affettuosa riconoscenza. Sono grata anche ai colleghi Marco Degiovanni e Clara Franchi per gli utili suggerimenti ed osservazioni.

Brescia, novembre 2005 M. C. Tamburini

Capitolo I

Moduli su un anello

Sia R un anello con unità $1_R \neq 0_R$.

1 Definizione e prime proprietà

(1.1) Definizione *Un gruppo abeliano $(M, +, 0_M)$ è un R-modulo sinistro se è definito un prodotto $(r, m) \mapsto rm$ da $R \times M$ a M per cui valgono le seguenti proprietà .*
Per ogni $r,\ r_1,\ r_2 \in R$ e per ogni $m,\ m_1,\ m_2 \in M$:
1) $r(m_1 + m_2) = rm_1 + rm_2$;
2) $(r_1 + r_2)m = r_1m + r_2m$;
3) $r_1(r_2m) = (r_1r_2)m$;
4) $1_Rm = m$.

Analogamente, M è un *R-modulo destro* se è definito un prodotto $M \times R \to M$ per cui valgono le analoghe proprietà . Qui considereremo sempre R-moduli sinistri, chiamandoli per brevitá R-moduli.
Se R è un corpo, un R-modulo si dice anche uno *spazio vettoriale* su R.
Chiaramente ogni R-modulo é un R_0-modulo per ogni sottoanello R_0 di R.

(1.2) Lemma *Sia $f : S \to R$ un omomorfismo di anelli. Ogni R-modulo M risulta un S-modulo rispetto*

$$sm := f(s)m, \quad \forall s \in S,\ m \in M.$$

La dimostrazione é lasciata per esercizio.

(1.3) Esempio *Il gruppo abeliano $(R, +, 0_R)$ è un R-modulo sinistro rispetto al prodotto di anello $(r_1, r_2) \mapsto r_1r_2$. Si chiama l'$R$-modulo* regolare sinistro *e si indica con ${}_RR$.*

(1.4) Esempio *Sia $\mathbb{Z}$ l'anello degli interi. Ogni gruppo abeliano $(M,+,0_M)$ è uno $\mathbb{Z}$-modulo sinistro rispetto al prodotto $(z,m)\mapsto zm$, dove:*

$$zm := \begin{cases} \underbrace{m+\cdots+m}_{z \text{ volte}} & \text{se} \quad z>0 \\ 0_M & \text{se} \quad z=0 \\ -(-zm) & \text{se} \quad z<0. \end{cases}$$

Ricordiamo che R^* indica l'insieme degli elementi di R che hanno inverso moltiplicativo. Dagli assiomi di modulo si deducono le seguenti utili regole di calcolo.

(1.5) Lemma *Sia M un R-modulo. Per ogni $r\in R$, $m\in M$:*

1) $0_R\, m = 0_M$*;*

2) $r\, 0_M = 0_M$*;*

3) $(-r)\, m = r\,(-m) = -(rm)$*;*

4) *se $\nu\in R^*$ e $\nu\, m = 0_M$, allora $m = 0_M$.*

Dimostrazione.

1) $0_R\, m = (0_R + 0_R)\; m = 0_R\, m + 0_R\, m$.

Sommando al primo e all'ultimo termine $-\,(0_R\, m)\in M$ si ha $0_M = 0_R\, m$.

2) $r\, 0_M = r\;(0_M + 0_M) = r\, 0_M + r\, 0_M$.

Sommando al primo e all'ultimo termine $-\,(r\, 0_M)\in M$ si ha $0_M = r0_M$.

3) $(-r)m + rm = (-r+r)m = 0_R m = 0_M$.

Quindi $(-r)\, m$ è l'opposto di rm.

$r(-m) + rm = r(-m+m) = r0_M = 0_M$.

Quindi $r(-m)$ è lopposto di rm:

4) Moltiplicando per ν^{-1} si ha: $\nu^{-1}(\nu m) = \nu^{-1}0_M$, da cui $\left(\nu^{-1}\nu\right) m = 0_M$.

Si conclude $1_R m = m = 0_M$. ■

(1.6) Definizione *Un sottoinsieme N di un R-modulo M si dice un* sottomodulo *(o anche un* sottospazio *quando R è un corpo) se soddisfa i seguenti assiomi:*

1) $0_M\in N$*;*

2) *per ogni $n_1, n_2\in N$, l'elemento (n_1+n_2) appartiene a N;*

3) *per ogni $r\in R$, $n\in N$, l'elemento (rn) appartiene a N.*

Per ogni $n\in N$, anche $-1_R n = -n\in N$. Quindi un sottomodulo è un sottogruppo N di $(M,+,0_M)$ tale che $RN\subseteq N$. Indichiamo che N è sottomodulo di M mediante $N\leq M$.

Notiamo che i sottomoduli del modulo regolare ${}_RR$ sono gli ideali sinistri dell'anello R. In particolare, se R è un corpo, gli unici sottomoduli di ${}_RR$ sono $\{0_R\}$ e R.

(1.7) Lemma *Siano N_1 e N_2 due sottomoduli di un R-modulo M. Allora:*
1) *il massimo sottomodulo di M contenuto in entrambi è $N_1 \cap N_2$;*
2) *il minimo sottomodulo di M che li contiene entrambi è*

$$N_1 + N_2 := \{n_1 + n_2 \mid n_1 \in N_1,\ n_2 \in N_2\}.$$

Dimostrazione. Per definizione di sottomodulo $0_M \in N_1$ e $0_M \in N_2$.
Quindi $0_M \in N_1 \cap N_2$. Inoltre $0_M = 0_M + 0_M \in N_1 + N_2$.
1) Basta dimostrare che $N_1 \cap N_2$ è sottomodulo. Siano $m_1, m_2, m \in N_1 \cap N_2$, $r \in R$.
Da $m_1,\ m_2,\ m \in N_1$ segue $(m_1 + m_2) \in N_1$ e $rm \in N_1$ per definizione di sottomodulo.
Idem per N_2. Si conclude che $(m_1 + m_2) \in N_1 \cap N_2$, $rm \in N_1 \cap N_2$.
2) Siano $(n_1 + n_2), (\overline{n}_1 + \overline{n}_2) \in N_1 + N_2$, $r \in R$.
Da $n_1, \overline{n}_1 \in N_1$ e $n_2, \overline{n}_2 \in N_2$, segue:
$(n_1 + n_2) + (\overline{n}_1 + \overline{n}_2) = (n_1 + \overline{n}_1) + (n_2 + \overline{n}_2) \in N_1 + N_2$,
$r(n_1 + n_2) = (rn_1) + (rn_2) \in N_1 + N_2$.
Abbiamo così verificato che $N_1 + N_2$ è un sottomodulo.
Resta da vedere che è il minimo sottomodulo che contiene sia N_1, sia N_2.
Per ogni $n_1 \in N_1$ si ha $n_1 = n_1 + 0_M \in N_1 + N_2$. Quindi $N_1 \leq N_1 + N_2$.
In modo analogo $N_2 \leq N_1 + N_2$. Concludiamo $N_1 \cup N_2 \subseteq N_1 + N_2$.
Infine sia X un sottomodulo di N che contiene $N_1 \cup N_2$.
Per ogni $n_1 + n_2 \in N_1 + N_2$ si ha: $n_1 \in N_1 \leq X$, $n_2 \in N_2 \leq X$.
Pertanto $(n_1 + n_2) \in X$, ossia $N_1 + N_2 \leq X$. ■

Più in generale, valgono i seguenti fatti. Sia $\{N_i \mid i \in I\}$ una famiglia non vuota di sottomoduli N_i di un R-modulo M. Si definisca $\sum_{i\in I} N_i$ come l'insieme di tutte le somme finite $n_{i_1} + \cdots + n_{i_m}$ di elementi n_{i_j} appartenenti ai sottomoduli della famiglia.
• l'intersezione insiemistica $\cap_{i\in I} N_i$ è un sottomodulo di M;
• $\sum_{i\in I} N_i$ è il minimo sottomodulo di M che contiene $\cup_{i\in I} N_i$.

2 Sottomoduli generati da un sottoinsieme

Dato un elemento m di un R-modulo M, definiamo

$$< m >:= \{rm \mid r \in R\} = Rm.$$

In virtù del successivo Lemma, $< m >$ è il minimo sottomodulo di M a cui appartiene m. Si dice quindi che $< m >$ è il *sottomodulo generato da* m. Più in generale, si ha:

(2.1) Lemma *Dato un sottoinsieme* $S = \{m_1, \ldots, m_n\}$ *di un* R*-modulo* M*, sia* $< S >$ *l'insieme delle combinazioni lineari, a coefficienti in* R*, degli elementi di* S*, ossia:*

$$< S >:= \left\{ \sum_1^n r_i m_i \mid r_i \in R \right\} = Rm_1 + \cdots + Rm_n.$$

1) $< S >$ *è un sottomodulo di* M*;*

2) $S \subseteq < S >$*;*

3) *per ogni sottomodulo* N *di* M *tale che* $S \subseteq N$*, si ha* $< S > \leq N$*.*

Dimostrazione.

1) $0_M = 0_R m_1 + \cdots + 0_R m_n \in < S >$.

Per ogni $(r_1 m_1 + \cdots + r_n m_n)$, $(\overline{r}_1 m_1 + \cdots + \overline{r}_n m_n) \in < S >$ e per ogni $r \in R$, si ha:

$(r_1 m_1 + \cdots + r_n m_n) + (\overline{r}_1 m_1 + \cdots + \overline{r}_n m_n) = (r_1 + \overline{r_1})\, m_1 + \cdots + (r_n + \overline{r_n}) \in < S >$,

$r\,(r_1 m_1 + \cdots + r_n m_n) = (rr_1)m_1 + \cdots + (rr_n)m_n \in < S >$.

2) $m_1 = 1_R m_1 + \cdots + 0_R m_n \in < S >$. Così per gli altri elementi di S.

3) Da $S \subseteq N$, sottomodulo, segue $r_1 m_1 + \cdots + r_n m_n \in N$ per ogni $r_1, \ldots, r_n \in R$. ■

Pertanto $< S >$ è il minimo sottomodulo di M che contiene S. Ciò giustifica la seguente:

(2.2) Definizione $< S >$ *si dice il* sottomodulo di M generato da S.

Poichè il minimo sottomodulo di M che contiene $\emptyset$ è quello nullo, si pone $< \emptyset >:= \{0_M\}$. Più in generale, se S è un qualunque insieme non vuoto, il sottomodulo $< S >$ è definito come l'insieme delle combinazioni lineari finite, a coefficienti in R, degli elementi di S.

(2.3) Definizione S *è un* insieme di generatori *per* M*, o* genera M*, se* $\langle S \rangle = M$*.*

3 Moduli quoziente e omomorfismi

Siano M un R-modulo e N un suo sottomodulo. In particolare N è un sottogruppo del gruppo $(M, +, 0_M)$. Possiamo quindi considerare la relazione di congruenza modulo N, definita ponendo, per ogni $m, \overline{m} \in M$:

$$m \equiv \overline{m} \pmod{N} \iff (m - \overline{m}) \in N.$$

Come visto nel Teorema 4.2 del Capitolo 2 di [9], la congruenza modulo N è una relazione di equivalenza in M. Per ogni $m \in M$, la classe di equivalenza di m è l'insieme

$$N + m := \{n + m \mid n \in N\}$$

detto il *laterale destro* di N individuato da m. Ne segue che, per ogni $m, \overline{m} \in M$:

$$N + m = N + \overline{m} \quad \Leftrightarrow \quad (m - \overline{m}) \in N. \tag{3.1}$$

Della relazione (3.1), per comodità del lettore, diamo anche una dimostrazione diretta. Sia $N + m = N + \overline{m}$. Da $m = 0_M + m \in N + m$, segue $m \in N + \overline{m}$. Quindi $m = n + \overline{m}$, per un opportuno $n \in N$. Si conclude $(m - \overline{m}) = n \in N$. Viceversa, sia $(m - \overline{m}) \in N$. Posto $(m - \overline{m}) = n$ si ha $m = n + \overline{m}$. Ne segue che $N + m \subseteq N + \overline{m}$. Infatti, per ogni $n_1 \in N$, si ha $n_1 + m = n_1 + (n + \overline{m}) = (n_1 + n) + \overline{m} \in N + \overline{m}$. Analogamente, da $\overline{m} = (-n) + m$ segue $N + \overline{m} \subseteq N + m$. Pertanto $N + m = N + \overline{m}$.

(3.2) Teorema *L'insieme $\frac{M}{N}$ dei laterali di N in M è un R-modulo rispetto alle operazioni definite ponendo, per ogni $m_1, m_2, m \in M$ e per ogni $r \in R$:*

$$(N + m_1) + (N + m_2) := N + (m_1 + m_2), \quad r(N + m) := N + rm.$$

Dimostrazione.
N è un sottogruppo normale di $(M, +, 0_M)$, essendo tale gruppo abeliano. Pertanto, rispetto alla somma, $\frac{M}{N}$ è un gruppo (abeliano) per il Teorema 5.7 del Capitolo 2 di [8]. Resta da vedere che è un R-modulo. A tale scopo verifichiamo innanzitutto che il prodotto $R \times \frac{M}{N} \to \frac{M}{N}$ è ben definito. Ossia che, per ogni $r \in R$, $m, \overline{m} \in M$,

$$N + m = N + \overline{m} \implies N + rm = N + r\overline{m}.$$

Infatti da $(m - \overline{m}) \in N$ segue $r(m - \overline{m}) \in N$, per definizione di sottomodulo. Ne segue $(rm - r\overline{m}) \in N$, da cui $N + rm = N + r\overline{m}$.
Infine, per ogni $r,\ r_1,\ r_2 \in R$ e per ogni $N + m,\ N + m_1,\ N + m_2 \in \frac{M}{N}$ si ha:
1) $r\left((N + m_1) + (N + m_2)\right) = r\left(N + m_1 + m_2\right) = N + r(m_1 + m_2) =$
$N + rm_1 + rm_2 = (N + rm_1) + (N + rm_2) = r(N + m_1) + r(N + m_2)$;
2) $(r_1 + r_2)(N + m) = N + (r_1 + r_2)m = N + r_1m + r_2m = (N + r_1m) + (N + r_2m) =$
$r_1(N + m) + r_2(N + m)$;
3) $r_1(r_2(N + m)) = r_1(N + r_2m) = N + r_1(r_2m) = N + (r_1r_2)m = (r_1r_2)(N + m)$;
4) $1_R(N + m) = N + 1_Rm = N + m$. ∎

(3.3) Definizione *Il modulo $\frac{M}{N}$, descritto nel Teorema* 3.2*, è detto il* modulo quoziente *di M rispetto a N.*

Siano M e M' degli R-moduli, con rispettivi prodotti

$$* : \ R \times M \to M, \quad \circ : \ R \times M' \to M'.$$

Si noti che, anche nel caso $M = M'$, puó essere $* \neq \circ$.

(3.4) Definizione *Un* R-omomorfismo *da* M *a* M' *è una applicazione* $\Phi : M \to M'$ *tale che, per ogni* $m_1, m_2, m \in M$ *e per ogni* $r \in R$*:*
1*)* $\Phi(m_1 + m_2) = \Phi(m_1) + \Phi(m_2)$,
2*)* $\Phi(r * m) = r \circ \Phi(m)$.

Se non vi é ambiguitá si omettono i simboli $*$ e $\circ$. Quando R è un corpo, un R-omomorfismo si dice anche una *applicazione lineare*.
Un esempio importante di omomorfismo fra moduli è fornito dal seguente:

(3.5) Lemma *Sia* M *un* R*-modulo. Fissato* $r \in R$*, sia* $\mu_r : M \to M$ *l'applicazione tale che* $m \mapsto rm$*, per ogni* $m \in M$*. Se* R *è commutativo la* μ_r *è un* R*-omomorfismo.*

Dimostrazione. Per ogni $m_1, m_2, m \in M$, e per ogni $s \in R$:
$\mu_r (m_1 + m_2) = r (m_1 + m_2) = rm_1 + rm_2 = \mu_r (m_1) + \mu_r (m_2)$.
$\mu_r (sm) = r(sm) = (rs)m = (sr)m = s(rm) = s\mu_r(m)$. ■

I prodotti e, quando esistono, gli inversi di R-omomorfismi sono R-omomorfismi. Infatti:

(3.6) Lemma *Siano* $\Phi : M \to M'$ *e* $\Psi : M' \to M''$ *degli* R*-omomorfismi.*
1) *L'applicazione prodotto* $\Psi\Phi : M \to M''$ *è un* R*-omomorfismo;*
2) *se* Φ *è bijettiva, la sua inversa* $\Phi^{-1} : M' \to M$ *è un* R*-omomorfismo.*

Dimostrazione.
1) Per ogni $m_1, m_2 \in M$:
$\Psi\Phi(m_1 + m_2) = \Psi (\Phi(m_1 + m_2)) = \Psi (\Phi(m_1) + \Phi(m_2)) = \Psi\Phi(m_1) + \Psi\Phi(m_2)$.
Per ogni $r \in R$ e ogni $m \in M$: $\Psi\Phi(rm) = \Psi (\Phi(rm)) = \Psi (r\Phi(m)) = r\Psi (\Phi(m))$.
2) Per ogni $m'_1, m'_2 \in M'$, dette m_1, m_2 le rispettive preimmagini in M si ha:
$m'_1 + m'_2 = \Phi(m_1) + \Phi(m_2) = \Phi(m_1 + m_2)$. Ne segue:
$\Phi^{-1}(m'_1 + m'_2) = m_1 + m_2 = \Phi^{-1}(m'_1) + \Phi^{-1}(m'_2)$.
Per ogni $r \in R$ e ogni $m' \in M'$, detta m la sua preimmagine in M, si ha:
$rm' = r\Phi(m) = \Phi(rm)$. Ne segue: $\Phi^{-1}(rm') = rm = r\Phi^{-1}(m')$. ■

(3.7) Definizione *Sia* $\Phi : M \to M'$ *un* R*-omomorfismo. Poniamo:*

• Im $\Phi := \{\Phi(m) \mid m \in M\}$;

• Ker $\Phi := \{m \in M \mid \Phi(m) = 0_{M'}\}$.

(3.8) Lemma *Sia $\Phi : M \to M'$ un R-omomorfismo. Per ogni sottomodulo N di M e per ogni sottomodulo N' di M' valgono i seguenti fatti:*

1) *l'immagine $\Phi(N) := \{\Phi(n) \mid n \in N\}$ è un sottomodulo di M';*

2) *se $N = \langle n_1, \ldots, n_k \rangle$, allora $\Phi(N) = \langle \Phi(n_1), \ldots, \Phi(n_k) \rangle$;*

3) *la preimmagine $\Phi^{-1}(N') := \{m \in M \mid \Phi(m) \in N'\}$ è un sottomodulo di M.*

In particolare:

• *M sottomodulo di M implica* Im $\Phi := \Phi(M)$ *sottomodulo di M';*

• *$\{0_{M'}\}$ sottomodulo di M' implica* Ker $\Phi := \Phi^{-1}\{0_{M'}\}$ *sottomodulo di M.*

Dimostrazione.

Φ è un omomorfismo di gruppi additivi, per l'assioma 1) della Definizione 3.4. Quindi, per il Lemma 7.6 del Capitolo II di [9] si ha $\Phi(0_M) = 0_{M'}$. Così , da $0_M \in N$ segue $0_{M'} \in \Phi(N)$ e da $0_{M'} \in N'$ segue $0_M \in \Phi^{-1}(N')$. Inoltre, per lo stesso Lemma, $\Phi(-m) = -\Phi(m)$, per ogni $m \in M$.

1) Per ogni $\Phi(n_1)$, $\Phi(n_2)$, $\Phi(n)$, dove $n_1, n_2, n \in N$, e per ogni $r \in R$ si ha:
$\Phi(n_1) - \Phi(n_2) = \Phi(n_1 - n_2) \in \Phi(N)$, dato che $(n_1 - n_2) \in N$, in quanto sottomodulo,
$r\Phi(n) = \Phi(rn) \in \Phi(N)$ dato che $rn \in N$ in quanto sottomodulo.

2) Per ogni $\Phi(n) \in \Phi(N)$, dove $n \in N$, si ha $n = \sum_{i=1}^{k} r_i n_i$
per opportuni coefficienti $r_i \in R$. Pertanto: $\Phi(n) = \Phi\left(\sum_{i=1}^{k} r_i n_i\right) = \sum_{i=1}^{k} r_i \Phi(n_i)$.

3) Siano $m_1, m_2, m \in \Phi^{-1}(N')$, $r \in R$. Da $\Phi(m_1), \Phi(m_2), \Phi(m) \in N'$ segue:
$\Phi(m_1 - m_2) = \Phi(m_1) - \Phi(m_2) \in N'$, da cui $(m_1 - m_2) \in \Phi^{-1}(N')$,
$\Phi(rm) = r\Phi(m) \in N'$ da cui $rm \in \Phi^{-1}(N')$. ■

(3.9) Definizione *Sia $\Phi : M \to M'$ un R-omomorfismo.*

• Φ *è un* monomorfismo *se è una applicazione iniettiva* ($\Leftrightarrow$ Ker $\Phi = \{0_M\}$);

• Φ *è un* epimorfismo *se è una applicazione suriettiva, ossia se* Im $\Phi = M'$;

• Φ *è un* isomorfismo *se è monomorfismo e epimorfismo.*

(3.10) Definizione *Come sopra, siano M e M' due R-moduli. Diciamo che:*

• *M' è* immagine epimorfa *di M se esiste un R-epimorfismo da M a M';*

• *M' è* isomorfo *a M, in simboli $M \simeq M'$, se esiste un R-isomorfismo da M a M'.*

La relazione di isomorfismo fra moduli è riflessiva, simmetrica e transitiva. Dal punto di vista dell'algebra astratta, moduli isomorfi sono identificati.
Illustriamo ora la stretta connessione fra moduli quoziente e omomorfismi.

(3.11) Lemma *Siano M un R-modulo, N un suo sottomodulo e $\frac{M}{N}$ il modulo quoziente. L'applicazione $\pi : M \to \frac{M}{N}$ tale che $m \mapsto N + m$ è un R-epimorfismo e Ker $\pi = N$.*

Dimostrazione.
Per ogni $m_1, m_2, m \in M$, $r \in R$ si ha:
$\pi(m_1 + m_2) = N + m_1 + m_2 = (N + m_1) + (N + m_2) = \pi(m_1) + \pi(m_2)$,
$\pi(rm) = N + (rm) = r(N + m) = r\pi(m)$.
Ogni laterale $N + m$ ha come preimmagini gli elementi di $N + m$ (fra cui m).
Ker $\pi = \{m \in M \mid N + m = N + 0_M\} = \{m \mid m - 0_M \in N\} = N$. ■

Quindi ogni modulo quoziente di M è immagine epimorfa di M. Viceversa ogni immagine epimorfa di M è isomorfa a un suo modulo quoziente, in virtù del seguente:

(3.12) Teorema *Sia $\Phi : M \to M'$ un R-omomorfismo. Allora l'applicazione:*

$$\overline{\Phi} : \frac{M}{\text{Ker } \Phi} \to \text{Im } \Phi \quad \text{tale che} \quad \text{Ker } \Phi + m \mapsto \Phi(m) \tag{3.13}$$

è un R-isomorfismo. In particolare $\frac{M}{\text{Ker } \Phi} \simeq \text{Im } \Phi$.

Dimostrazione.
$\overline{\Phi}$ è ben definita. Infatti, con ovvie notazioni:

$$\text{Ker } \Phi + m = \text{Ker } \Phi + \overline{m} \implies (m - \overline{m}) \in \text{Ker } \Phi \implies \Phi(m - \overline{m}) = 0 \implies \Phi(m) = \Phi(\overline{m}).$$

Poichè valgono anche le implicazioni inverse, $\overline{\Phi}$ è iniettiva. Chiaramente è suriettiva.
Infine è un R-omomorfismo:
$\overline{\Phi}((\text{Ker } \Phi + m_1) + (\text{Ker } \Phi + m_2)) = \overline{\Phi}(\text{Ker } \Phi + m_1 + m_2) = \Phi(m_1 + m_2) =$
$\Phi(m_1) + \Phi(m_2) = \overline{\Phi}(\text{Ker } \Phi + m_1) + \overline{\Phi}(\text{Ker } \Phi + m_2)$,
$\overline{\Phi}(r(\text{Ker } \Phi + m)) = \overline{\Phi}(\text{Ker } \Phi + rm) = \Phi(rm) = r\Phi(m) = r\overline{\Phi}(\text{Ker } \Phi + m)$. ■

4 Somme dirette

(4.1) Definizione *Dati un R-modulo M e due sottomoduli M_1 e M_2, diciamo che M è* somma diretta interna *di M_1 e M_2, e scriviamo $M = M_1 \dot{+} M_2$, se:*

1) $M = M_1 + M_2$;
2) $M_1 \cap M_2 = \{0_M\}$.

(4.2) Lemma *$M = M_1 \dot{+} M_2$ se e solo se ogni $m \in M$ si scrive in modo unico nella forma $m = m_1 + m_2$ con $m_1 \in M_1$, $m_2 \in M_2$.*

Dimostrazione. Sia $M = M_1 \dot{+} M_2$. Per l'assioma 1) ogni m si scrive nella forma richiesta. Quanto all'unicità , sia $m_1 + m_2 = m_1' + m_2'$ con $m_1, m_1' \in M_1$, $m_2, m_2' \in M_2$. Ne segue $m_1 - m_1' = m_2' - m_2 \in M_1 \cap M_2$. Per l'assioma 2) $m_1 - m_1' = 0_M$, da cui $m_1 = m_1'$, $m_2 = m_2'$.
Viceversa. Se ogni $m \in M$ si scrive nella forma indicata si ha $M = M_1 + M_2$. Infine sia $i \in M_1 \cap M_2$. Da $0_M = 0_M + 0_M = i + (-i)$ segue $i = 0_M$, per l' unicità della scrittura di 0_M nella forma indicata. ■

Siano ora M_1 e M_2 due R-moduli. Il lettore verifichi, per esercizio, che

$$M_1 \oplus M_2 := \left\{ \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \mid m_1 \in M_1, m_2 \in M_2 \right\} \tag{4.3}$$

è un R-modulo rispetto alle seguenti operazioni:

$$\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} + \begin{pmatrix} \overline{m}_1 \\ \overline{m}_2 \end{pmatrix} := \begin{pmatrix} m_1 + \overline{m}_1 \\ m_2 + \overline{m}_2 \end{pmatrix}, \quad r \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} := \begin{pmatrix} rm_1 \\ rm_2 \end{pmatrix}, \tag{4.4}$$

dove $m_1, \overline{m}_1 \in M_1$, $m_2, \overline{m}_2 \in M_2$, $r \in R$.

(4.5) Definizione *Il modulo $M_1 \oplus M_2$ si dice la* somma diretta esterna *di M_1 e M_2.*

Si noti che gli elementi di $M_1 \oplus M_2$ sono quelli del *prodotto cartesiano* $M_1 \times M_2$ e che le operazioni sono definite *componente per componente.* Il lettore verifichi che le proiezioni

$$\pi_1 : M_1 \oplus M_2 \to M_1, \quad \pi_2 : M_1 \oplus M_2 \to M_2$$

definite rispettivamente mediante:

$$\begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \mapsto m_1 \quad , \quad \begin{pmatrix} m_1 \\ m_2 \end{pmatrix} \mapsto m_2$$

sono R-epimorfismi. Verifichi inoltre che

$$\text{Ker } \pi_2 = \left\{ \begin{pmatrix} m_1 \\ 0_{M_2} \end{pmatrix} \mid m_1 \in M_1 \right\}, \quad \text{Ker } \pi_1 = \left\{ \begin{pmatrix} 0_{M_1} \\ m_2 \end{pmatrix} \mid m_2 \in M_2 \right\} .$$

Ne deduca:

$$M_1 \oplus M_2 = \text{Ker } \pi_2 \dot{+} \text{ Ker } \pi_1, \qquad \text{Ker } \pi_2 \simeq M_1, \ \text{Ker } \pi_1 \simeq M_2.$$

Dati $n > 2$ moduli $M_1, \cdots, M_n$ su R, la loro somma diretta esterna $M_1 \oplus \cdots \oplus M_n$ è definita induttivamente come il modulo $(M_1 \oplus \cdots \oplus M_{n-1}) \oplus M_n$.
Considerando il caso particolare in cui ogni $M_i = {}_RR$, si ha:

(4.6) Definizione $({}_RR)^0 := \{0\}$ *e, per* $n > 1$*:*

$$({}_RR)^1 := {}_RR,\ ({}_RR)^2 := {}_RR \oplus {}_RR,\ \ldots,\ ({}_RR)^n := \underbrace{{}_RR \oplus \cdots \oplus_R R}_{n \text{ volte}}.$$

In virtù di (4.3) di (4.4), per ogni $n > 1$ il modulo $({}_RR)^n$ ha come elementi i *vettori colonna* a n componenti in R e le operazioni di modulo risultano le seguenti:

$$\text{(4.7)} \qquad \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \ldots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \ldots \\ x_n + y_n \end{pmatrix}, \quad r \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix} = \begin{pmatrix} rx_1 \\ \ldots \\ rx_n \end{pmatrix}.$$

5 Moduli liberi

(5.1) Definizione *Un sottoinsieme* S *di un* R*-modulo* M *si dice* indipendente *se* $S = \emptyset$ *oppure se, posto* $S = \{m_1, \ldots, m_n\}$*, si ha che:*

$$\sum_{i=1}^{n} r_i m_i = 0_M \ (\text{con } r_i \in R) \quad \Rightarrow \quad r_i = 0_R, \quad 1 \leq i \leq n.$$

In caso contrario si dice che S è *dipendente.*
Ad esempio $\{0_M\}$ è dipendente: infatti $1_R 0_M = 0_M$.

(5.2) Lemma *Sia* S *indipendente. Ogni suo sottoinsieme* T *è indipendente.*
In particolare $0_M \notin S$*.*

Dimostrazione.
Se $T = \emptyset$ oppure $T = S$ l'asserto è vero. Supponiamo quindi $T = \{m_1, \ldots, m_k\}$, $S = \{m_1, \ldots, m_n\}$, $1 \leq k < n$. Se, per assurdo, T fosse dipendente, esisterebbero dei coefficienti non tutti nulli $r_1, \ldots, r_k \in R$ tali che $\sum_{i=1}^{k} r_i m_i = 0_M$. Posto $r_{k+1} = 0_R, \ldots, r_n = 0_R$, ne seguirebbe $\sum_{i=1}^{n} r_i m_i = 0_M$, in contrasto con l' indipendenza di S. ■

(5.3) Lemma *Sia* $S = \{v_1, \ldots, v_n\}$ *un sottoinsieme di un* R*-modulo* M*.*
L'applicazione $\eta : ({}_RR)^n \to M$ *tale che:*

$$\text{(5.4)} \qquad \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^{n} x_i v_i$$

è un R-omomorfismo. Inoltre

- *η è suriettiva se e solo se S genera M come R-modulo (Definizione 2.3);*
- *η è iniettiva se e solo se S è indipendente.*

Dimostrazione. Verifichiamo che η è un R-omomorfismo.

$$\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \cdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \cdots \\ x_n + y_n \end{pmatrix} \mapsto \sum_{i=1}^{n} (x_i + y_i)v_i = \sum_{i=1}^{n} x_i v_i + \sum_{i=1}^{n} y_i v_i$$

$$r \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} = \begin{pmatrix} rx_1 \\ \cdots \\ rx_n \end{pmatrix} \mapsto \sum_{i=1}^{n} (rx_i)v_i = r \sum_{i=1}^{n} x_i v_i.$$

Il resto è ovvio. ■

(5.5) Definizione *Un sottoinsieme $\mathcal{B}$ di un R-modulo M è una* base *di M se genera M come R-modulo e se è indipendente.*

(5.6) Osservazione *Chiaramente un sottoinsieme $\{v_1, \cdots, v_n\}$ di un R-modulo M è una base se e solo se l'applicazione $\eta : ({}_R R)^n \to M$, definita da (5.4), è bijettiva. Equivalentemente $\{v_1, \cdots, v_n\}$ è una base di M se ogni $m \in M$ si scrive in modo unico nella forma $x_1 v_1 + \cdots + x_n v_n$ con $x_i \in R$.*

Un'altra caratterizzazione delle basi è data dal seguente:

(5.7) Lemma *Sia $\mathcal{B} = \{v_1, \cdots, v_n\}$ una base di un R-modulo M. Per ogni R-modulo N e ogni applicazione (di insiemi!) $\varphi : \mathcal{B} \to N$, esiste un unico R-omomorfismo $\Phi : M \to N$ che estende φ.*

Dimostrazione. Φ è l'estensione, per linearità , di φ a M. Ossia:
$\Phi(x_1 v_1 + \cdots + x_n v_n) := x_1 \varphi(v_1) + \cdots + x_n \varphi(v_n)$. ■

(5.8) Definizione *Un R-modulo L si dice* libero *se ha una base.*

Per ogni $n \geq 0$ il modulo $({}_R R)^n$ è libero. Infatti:
$R^0 = \{0_R\}$ ha come base l'insieme $\emptyset$.
$R^1 = {}_R R$ ha come base il singoletto $\{1_R\}$.
Per $n \geq 2$, è immediato verificare che $({}_R R)^n$ ha come base l'insieme:

$$\left\{ e_1 := \begin{pmatrix} 1_R \\ \cdots \\ 0_R \end{pmatrix}, \ \ldots, \ e_n := \begin{pmatrix} 0_R \\ \cdots \\ 1_R \end{pmatrix} \right\} \quad (\textit{base canonica}). \tag{5.9}$$

Se L è un R-modulo libero con base $\{v_1, \cdots, v_n\}$, l'applicazione $\eta : ({}_RR)^n \to L$, definita da (5.4), è un R-isomorfismo. Quindi:

$$({}_RR)^n \simeq L.$$

Ne segue, ad esempio, che $\mathbb{Z}_2$ non è libero come $\mathbb{Z}$-modulo. Infatti $|\mathbb{Z}_2| = 2$. D'altra parte, $\left|({}_{\mathbb{Z}}\mathbb{Z})^0\right| = 1$ e, per $n > 0$, $({}_{\mathbb{Z}}\mathbb{Z})^n$ è infinito. Tuttavia $\mathbb{Z}_2$ è libero come $\mathbb{Z}_2$-modulo. Un isomorfismo fra R-moduli porta basi in basi. Infatti:

(5.10) Lemma *Dati due R-moduli L, L', sia $\Phi : L \to L'$ un R-isomorfismo.*
Se $\mathcal{B} = \{v_1, \ldots, v_n\}$ è una base di L, allora $\mathcal{B}' = \{\Phi(v_1), \ldots, \Phi(v_n)\}$ è una base di L'.
In particolare se L è libero, anche L' è libero.

Dimostrazione. Da $\langle \mathcal{B} \rangle = L$ segue $\langle \mathcal{B}' \rangle = L'$ per il punto 2) del Lemma 3.8. Quanto alla indipendenza di $\mathcal{B}'$, sia $\sum_{i=1}^n x_i \Phi(v_i) = 0_{L'}$. Segue $\Phi\left(\sum_{i=1}^n x_i v_i\right) = 0_{L'}$ da cui $\sum_{i=1}^n x_i v_i \in \mathrm{Ker}(\Phi) = \{0_L\}$. Si conclude $x_i = 0_R$ per $i \leq n$, essendo $\mathcal{B}$ indipendente. ∎

Una somma diretta di moduli liberi è un modulolibero. Infatti:

(5.11) Lemma *Sia $L = L_1 \dot{+} L_2$. Se $\mathcal{B}_1$ è una base di L_1 e $\mathcal{B}_2$ è una base di L_2, allora $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$ e $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ è una base di L.*

Dimostrazione.
$\mathcal{B}_1 \cap \mathcal{B}_2 \subseteq L_1 \cap L_2 = \{0_L\}$. Poichè $0_L \notin \mathcal{B}_1$ per il Lemma 5.2, si ha $\mathcal{B}_1 \cap \mathcal{B}_2 = \emptyset$.
Ogni $\ell \in L$ si scrive in modo unico nella forma $\ell = \ell_1 + \ell_2$, con $\ell_1 \in L_1$, $\ell_2 \in L_2$. Per $i = 1, 2$, l'addendo ℓ_i si scrive in modo unico come combinazione lineare di elementi di $\mathcal{B}_i$. Si conclude che ℓ si scrive in modo unico come combinazione lineare di elementi di $\mathcal{B}$, che è pertanto una base di L. ∎

(5.12) Teorema *Sia $f : M \to L$ un epimorfismo di R-moduli. Se L è libero, esiste un sottomodulo L^* di M tale che: $M = \mathrm{Ker} f \dot{+} L^*$ con $L^* \simeq L$.*
In particolare, se $\mathrm{Ker} f$ è libero, anche M è libero.

Dimostrazione.
Sia $\mathcal{B} = \{v_1, \ldots, v_n\}$ una base di L e siano $m_1, \ldots, m_n$ elementi di M tali che

$$f(m_i) = v_i, \quad 1 \leq i \leq n.$$

Consideriamo il sottomodulo $L^* = \langle m_1, \ldots, m_n \rangle$, generato dagli m_i.

Mostriamo innanzitutto che $M = \text{Ker } f + L^*$. Per ogni $m \in M$, si ha

$$f(m) = \sum_1^n x_i v_i = \sum_1^n x_i f(m_i) = f\left(\sum_1^n x_i m_i\right).$$

Ne segue $(m - \sum_1^n x_i m_i) \in \text{Ker } f$ e, dall'identità

$$m = (m - \sum_1^n x_i m_i) + \sum_1^n x_i m_i$$

si deduce $m \in$ Ker f $+ L^*$.

Mostriamo ora che $L^* \cap \text{Ker } f = \{0_M\}$. Infatti $\sum_1^n y_i m_i \in \text{Ker } f$ implica

$$0_L = f\left(\sum_1^n y_i m_i\right) = \sum_1^n y_i f(m_i) = \sum_1^n y_i v_i$$

da cui $y_1 = \cdots = y_n = 0_R$, per l'indipendenza di $\mathcal{B}$. Infine la restrizione f_{L^*} di f a L^* è un isomorfismo da L a L^*. Infatti è suriettiva perchè $\mathcal{B} \subseteq f(L^*)$ implica $L = \langle \mathcal{B} \rangle \leq f(L^*)$, ed è iniettiva perchè Ker $f_{L^*} = \text{Ker } f \cap L^* = \{0_M\}$. ■

6 Rango dei moduli liberi su anelli commutativi

(6.1) Teorema *Sia R un anello commutativo e sia $n \geq 0$.*

1) *Il modulo $({}_R R)^n$ non è generato da alcun sottoinsieme di cardinalità $m < n$;*

2) *tutte le basi (finite) di un R-modulo libero L hanno la stessa cardinalità .*

Dimostrazione.

1) Per $n \leq 1$ l'asserto è chiaro. Sia quindi $n \geq 2$. Supponiamo per assurdo che $S = \{v_1, \cdots, v_m\}$ sia un insieme di $m < n$ generatori per $({}_R R)^n$. Esprimiamo ogni vettore e_i della base canonica (5.9) nella forma $e_i = \sum_{j=1}^m a_{ji} v_j$ per opportuni coefficienti a_{ji} (non necessariamente unici).

Si ottiene la contraddizione desiderata considerando il seguenti prodotto di matrici:

$$\left(\begin{array}{c|c|c|c|c} v_1 & \dots & v_m & 0^n & \dots & 0^n \end{array} \right) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \\ 0 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 0 \end{pmatrix} =$$

$$\left(\begin{array}{c|c|c|c|c} \sum_{j=1}^m a_{j1} v_j & \dots & \sum_{j=1}^m a_{jm} v_j & \dots & \sum_{j=1}^m a_{jn} v_j \end{array} \right) = \left(\begin{array}{c|c|c|c|c} e_1 & \dots & e_m & \dots & e_n \end{array} \right) = I.$$

2) Siano $\mathcal{B}$ e $\mathcal{C}$ due basi finite di L. Posto $|\mathcal{B}| = n$ e $|\mathcal{C}| = m$, possiamo supporre $m \leq n$. Sia $\eta^{-1} : L \to ({}_R R)^n$ l'isomorfismo 5.4. Poichè $\eta^{-1}(\mathcal{C})$ ha cardinalità m e genera $({}_R R)^n$, non può essere $m < n$. ■

Questo fatto giustifica la seguente:

(6.2) Definizione *Se L è un modulo libero su un anello commutativo R, con una base di $n \geq 0$ elementi, diciamo che n è il* rango *di L.*

In particolare il modulo nullo ha rango 0.

(6.3) Teorema *L'anello R sia commutativo.*
1) *Siano L_1 e L_2 due R-moduli liberi. Allora $L_1 \oplus L_2$ è libero e:*

$$\text{rango}(L_1 \oplus L_2) = \text{rango}(L_1) + \text{rango}(L_2).$$

2) *Siano $N \leq M$ moduli su R. Se N e $\frac{M}{N}$ sono liberi, anche M è libero e:*

$$\text{rango}\left(\frac{M}{N}\right) = \text{rango } (M) - \text{rango } (N).$$

3) *Sia $L = L_1 + L_2$. Se L, L_1, L_2 e $L_1 \cap L_2$ sono liberi su R, allora:*

$$\text{rango}(L_1) + \text{rango}(L_2) = \text{rango}(L_1 \cap L_2) + \text{rango}(L).$$

Dimostrazione.
1) $L_1 \oplus L_2 = \text{Ker } \pi_2 \dot{+} \text{Ker } \pi_1$ con $\text{Ker } \pi_2 \simeq L_1$, $\text{Ker } \pi_1 \simeq L_2$.
Per il Lemma 5.11 anche $L_1 \oplus L_2$ è libero e vale l'asserto.

2) Sia $\pi : M \to \frac{M}{N}$ l'epimorfismo canonico. Per il Teorema 5.12 esiste un sottomodulo L^* di M tale che $L^* \simeq \frac{M}{N}$ e $M = \text{Ker } \pi \dot{+} L^* = N \dot{+} L^*$. La tesi segue dal Lemma 5.11.

3) Consideriamo l'applicazione $f : L_1 \to \frac{L}{L_2}$ tale che $l_1 \mapsto L_2 + l_1$.
f è un epimorfismo di moduli e $\text{Ker } f = L_1 \cap L_2$. Ne segue $\frac{L_1}{L_1 \cap L_2} \simeq \frac{L}{L_2}$.
Per il punto 2), $\text{rango}(L_1) - \text{rango}(L_1 \cap L_2) = \text{rango}(L) - \text{rango}(L_2)$, da cui l'asserto. ■

7 Matrici

In questo paragrafo supponiamo R commutativo.

Ricordiamo che $\mathrm{Mat}_{m,n}(R)$ indica l'insieme delle matrici $m \times n$ a elementi in R. Rispetto alle usuali operazioni di somma di matrici (componente per componente) e prodotto per scalari, $\mathrm{Mat}_{m,n}(R)$ è un R-modulo libero, isomorfo a ${}_RR)^{nm}$. Infatti una base di $\mathrm{Mat}_{m,n}(R)$ è costituita dall'insieme $\{E_{ij} \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$ delle matrici *elementari*, aventi 1 nella posizione (i, j) e 0 altrove.
Se $m = n$, l'insieme $\mathrm{Mat}_{n,n}(R)$ si indica con $\mathrm{Mat}_n(R)$. Esso è un anello rispetto alla somma e al prodotto (righe per colonne) di matrici.
Il gruppo $\mathrm{Mat}_n(R)^*$ delle matrici invertibili si indica con $\mathrm{GL}_n(R)$.
Si dimostra che il gruppo additivo R^n risulta un $\mathrm{Mat}_n(R)$-modulo rispetto al prodotto

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \dots & \dots & \dots \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} := \begin{pmatrix} \sum_{j=1}^n a_{1j}x_j \\ \dots \\ \sum_{j=1}^n a_{nj}x_j \end{pmatrix}. \tag{7.1}$$

(7.2) Osservazione *Si noti che uno stesso gruppo abeliano M può essere visto come modulo su diversi anelli, ottenendo strutture diverse.*

Per esempio, sia $M = \mathbb{Q}^n$.

• *Essendo M un gruppo abeliano, possiamo considerarlo come $\mathbb{Z}$-modulo. Come tale, non è finitamente generato. Infatti, se lo fosse, anche la sua immegine epimorfa $\mathbb{Q}$ lo sarebbe. Ma è facile vedere che il gruppo abeliano $\mathbb{Q}$ non è finitamente generato.*

• *Oppure possiamo vedere M come $\mathbb{Q}$-modulo. Come tale è libero, con una base di n elementi. In particolare è finitamente generato.*

• *Infine, per quanto visto sopra, possiamo considerarlo come $\mathrm{Mat}_n(\mathbb{Q})$-modulo. Come tale è generato, ad esempio, dal solo e_1. Ma $\{e_1\}$ non è indipendente.*

(7.3) Osservazione *Un gruppo abeliano M può essere visto come modulo sullo stesso anello R rispetto a prodotti diversi*

$$* :\ R \times M \to M, \quad \circ :\ R \times M \to M.$$

Ad esempio, nel Capitolo 4, vedremo che $\mathbb{K}^n$ puó essere visto come $\mathbb{K}[x]$-modulo in molti modi.

8 Esercizi

(8.1) Esercizio *Sia M uno dei seguenti gruppi additivi: $\mathbb{Z}$, $\mathbb{Z}_5$, $\mathbb{Z}_8$, $\mathbb{Z}_{12}$.*
In ciascun caso, per ogni $m \in M$, si determinino il periodo di m e il sottogruppo $< m >= \mathbb{Z}m$ generato da m.

(8.2) Esercizio *Nel modulo ${}_{\mathbb{Z}}\mathbb{Z}$, si considerino i sottoinsiemi $S = \{4\}$, $T = \{12, 20\}$. Si dimostri che $\langle S\rangle = \langle T\rangle$. Si dica inoltre se S è indipendente e se genera $\mathbb{Z}$.*

(8.3) Esercizio *Nello spazio vettoriale ${}_{\mathbb{Q}}\mathbb{Q}$, si considerino i sottoinsiemi $S = \{4\}$, $T = \{\frac{1}{3}, \frac{5}{7}\}$. Per ciascuno di essi si dica se è indipendente e se genera ${}_{\mathbb{Q}}\mathbb{Q}$.*

(8.4) Esercizio *Si consideri il gruppo abeliano $\mathbb{Q}$ come $\mathbb{Z}$-modulo. Per ciascuno degli insiemi $S = \{4\}$, $T = \{\frac{1}{3}, \frac{5}{7}\}$ si dica se è indipendente e se genera $\mathbb{Q}$.*

(8.5) Esercizio *Si consideri il gruppo abeliano $\mathbb{Q}$ come $\mathbb{Z}$-modulo. Si dimostri che non è finitamente generato.*

(8.6) Esercizio *Si provi che un R-omomorfismo è iniettivo se e solo se ha nucleo $(0\}$.*

(8.7) Esercizio *Si provi che il prodotto di due R-omomorfismi e l'inverso di un R-isomomorfismo sono R-omomorfismi.*

(8.8) Esercizio *Nel modulo ${}_{\mathbb{Z}}\mathbb{Z}$ si calcolino i seguenti sottomoduli:*

$$3\mathbb{Z} + 6\mathbb{Z}, \quad 3\mathbb{Z} + 5\mathbb{Z}, \quad 4\mathbb{Z} + 6\mathbb{Z}, \quad 3\mathbb{Z} \cap 6\mathbb{Z}, \quad 3\mathbb{Z} \cap 5\mathbb{Z}, \quad 4\mathbb{Z} \cap 6\mathbb{Z}.$$

(8.9) Esercizio *Sia* $S = \{\begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}\}$.

- *Considerando $\mathbb{R}^2$ come spazio vettoriale su $\mathbb{R}$, si dica se S è una base.*
- *Considerando $\mathbb{R}^2$ come $\mathbb{Z}$-modulo, si dica se S genera $\mathbb{R}^2$ e se è indipendente.*

(8.10) Esercizio *Si dica se $\mathbb{Z}_5$ è libero come $\mathbb{Z}_5$-modulo, e se è libero come $\mathbb{Z}$-modulo.*

(8.11) Esercizio *Sia R un anello commutativo. Considerando R^2 come R-modulo, si dimostri che non può essere generato da un unico elemento.*

(8.12) Esercizio *Considerando R^2 come $\mathrm{Mat}_2(\mathbb{R})$-modulo, si determini il sottomodulo $\langle e_1\rangle$ generato da $e_1 := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$.*

(8.13) Esercizio *Sia M un R-modulo finitamente generato. Si dimostri che, per ogni sottomodulo N di M, il modulo quoziente $\frac{M}{N}$ è finitamente generato.*

(8.14) Esercizio *Sia M un R-modulo. Si dimostri che $M \oplus M$ è finitamente generato se e solo se M è finitamente generato.*

(8.15) Esercizio
Considerando $\frac{\mathbb{C}[x]}{\langle x^2-1\rangle}$ come $\mathbb{C}[x]$- modulo, si trovi un elemento che lo genera.

(8.16) Esercizio *Considerando $\frac{\mathbb{C}[x]}{\langle x^2-1\rangle}$ come $\mathbb{C}$- modulo, se ne trovi una sua base.*

(8.17) Esercizio
Considerando $\frac{\mathbb{C}[x]}{\langle x^3-1\rangle}$ come $\mathbb{C}[x]$- modulo, si trovi un elemento che lo genera.

(8.18) Esercizio *Considerando $\frac{\mathbb{C}[x]}{\langle x^3-1\rangle}$ come $\mathbb{C}$- modulo, se ne trovi una sua base.*

(8.19) Esercizio *Si dimostri che $\frac{\mathbb{Z}_3[x]}{\langle x^3-1\rangle}$ ha ordine 27.*

(8.20) Esercizio *Si dimostri il Lemma 1.2*

Capitolo II

Omomorfismi fra moduli liberi

1 Vettore coordinate

Sia $\mathcal{B} = \{v_1, \ \dots \ , \ v_n\}$ una base di un R-modulo libero V. L'applicazione $\eta : ({}_RR)^n \to V$ definita da (5.4) nel precedente Capitolo, è bijettiva. Ha quindi inversa $\eta^{-1} : V \to ({}_RR)^n$.

(1.1) Definizione *Per ogni* $v = \sum_{i=1}^n x_i v_i \in V$*, diciamo che*

$$\eta^{-1}(v) = \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \tag{1.2}$$

è il vettore delle coordinate *di* v *rispetto a* $\mathcal{B}$ *e lo indichiamo con* $v_{\mathcal{B}}$*.*

Essendo η un isomorfiso, anche η^{-1} lo è . Pertanto, per ogni $v, w \in V$, $x \in R$ si ha:

$$(v + w)_{\mathcal{B}} = v_{\mathcal{B}} + w_{\mathcal{B}}, \quad (xv)_{\mathcal{B}} = xv_{\mathcal{B}}. \tag{1.3}$$

Detti $e_1, \ \cdots \ , \ e_n$ i vettori della base canonica di $({}_RR)^n$, da $\eta(e_i) = v_i$ segue:

$$(v_1)_{\mathcal{B}} = e_1, \ \dots, \ (v_n)_{\mathcal{B}} = e_n. \tag{1.4}$$

2 Matrice di un omomorfismo

(2.1) Definizione *Sia* $\alpha : V \to W$ *un* R*-omomorfismo fra moduli liberi. Consideriamo delle basi* $\mathcal{B} = \{v_1, \dots, v_n\}$ *di* V *e* $\mathcal{C} = \{w_1, \dots, w_m\}$ *di* W*. La matrice* $A \in \mathrm{Mat}_{m,n}(R)$*, le cui colonne* Ae_i*, per* $1 \leq i \leq n$*, sono i vettori* $(\alpha(v_i))_{\mathcal{C}}$ *si dice la* matrice di α rispetto $\mathcal{B}$ e $\mathcal{C}$*. Si dice anche che* α *è* l'omomorfismo indotto da A rispetto $\mathcal{B}$ e $\mathcal{C}$*.*

In modo esplicito:

$$\left\{ \begin{array}{ccc} \alpha(v_1) & = & a_{11}w_1 + \cdots + a_{m1}w_m \\ \cdots & \cdots & \cdots \\ \alpha(v_n) & = & a_{1n}w_1 + \cdots + a_{mn}w_m \end{array} \right. \iff A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}. \tag{2.2}$$

Se $V = W$ e $\mathcal{B} = \mathcal{C}$ si dice, più brevemente, che A è la matrice di α rispetto a $\mathcal{B}$.
La proprietà che caratterizza la matrice di un omomorfismo è espressa dal seguente:

(2.3) Lemma *Sia A la matrice di un R-omomorfismo $\alpha : V \to W$, rispetto a delle basi $\mathcal{B}$ e $\mathcal{C}$ di V e W rispettivamente. A è l'unica matrice tale che, per ogni $v \in V$:*

$$A\, v_{\mathcal{B}} \;=\; (\alpha(v))_{\mathcal{C}}\,. \tag{2.4}$$

Dimostrazione.
Si ha $(v_i)_{\mathcal{B}} = e_i$ per (1.4), $Ae_i = (\alpha(v_i))_{\mathcal{C}}$, per definizione di A. Pertanto

$$A\,(v_i)_{\mathcal{B}} \;=\; Ae_i = \;(\alpha(v_i))_{\mathcal{C}}\,, \quad 1 \le i \le n.$$

Sia $v = \sum_{i=1}^n x_i v_i$. Ricordando (1.3), risulta $v_{\mathcal{B}} = \sum_{i=1}^n x_i\,(v_i)_{\mathcal{B}}$. Ne segue:

$$Av_{\mathcal{B}} = A\sum_{i=1}^n x_i\,(v_i)_{\mathcal{B}} = \sum_{i=1}^n x_i A\,(v_i)_{\mathcal{B}} = \sum_{i=1}^n x_i\,(\alpha(v_i))_{\mathcal{C}} = \left(\sum_{i=1}^n x_i\alpha(v_i)\right)_{\mathcal{C}} = (\alpha(v))_{\mathcal{C}}\,.$$

Quindi A verifica la (2.4). Sia B tale che $B\,v_{\mathcal{B}} = (\alpha(v))_{\mathcal{C}}$, per ogni $v \in V$. Ne segue:

$$Be_i = B(v_i)_{\mathcal{B}} = (\alpha(v_i))_{\mathcal{C}} = A(v_i)_{\mathcal{B}} = Ae_i, \quad i = 1, \cdots, n.$$

Si conclude che le colonne di B sono ordinatamente uguali a quelle di A, ossia $B = A$. ∎

Ricordiamo che il prodotto di R-omomorfismi è un R-omomorfismo.

(2.5) Lemma *Siano V, W, U dei R-moduli liberi con rispettive basi $\mathcal{B}$, $\mathcal{C}$, $\mathcal{D}$ e siano*

$$V \;\xrightarrow{\alpha}\; W \;\xrightarrow{\beta}\; U$$

degli R-omomorfismi. Se A è la matrice di α rispetto $\mathcal{B}$, $\mathcal{C}$ e B quella di β rispetto $\mathcal{C}$, $\mathcal{D}$, allora BA è la matrice di $\beta\alpha : V \to U$ rispetto $\mathcal{B}$, $\mathcal{D}$.
In particolare, se $V \xrightarrow{\alpha} W$ è un R-isomorfismo, allora A ha inversa A^{-1}.

Dimostrazione. Per ogni $v \in V$ si ha:

$$(BA)v_{\mathcal{B}} = B(Av_{\mathcal{B}}) = B\,(\alpha(v)_{\mathcal{C}}) = \beta\,(\alpha(v))_{\mathcal{D}} = (\beta\alpha(v))_{\mathcal{D}}\,.$$

Per il Lemma 2.3 si conclude che BA è la matrice di $\beta\alpha$. In particolare, se α è un isomorfismo, esiste l'applicazione inversa $W \xrightarrow{\alpha^{-1}} V$ ed è a sua volta un R-omomorfismo. Poniamo $U = V$, $\mathcal{D} = \mathcal{B}$ e chiamiamo B la matrice di α^{-1}. Da $\alpha^{-1}\alpha = id_V$ segue $BA = I$, da cui $B = A^{-1}$. ∎

Fissata $A \in \mathrm{Mat}_{m,n}(R)$, l'applicazione $\mu_A : ({}_RR)^n \to ({}_RR)^m$, tale che

$$\begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} \to A \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}$$

è un R-omomorfismo. Inoltre A è la matrice di μ_A rispetto alle basi canoniche.

(2.6) Teorema *Se $m = n$, la μ_A è un isomorfismo se e solo se $A \in \mathrm{GL}_n(R)$.*

Dimostrazione. Se $A \in \mathrm{GL}_n(R)$, l'applicazione μ_A è bijettiva, avendo inversa $\mu_{A^{-1}}$. Infatti, per ogni $v \in R^n$, si ha

$$\mu_{A^{-1}}\mu_A(v) = A^{-1}Av = v, \quad \mu_A\mu_{A^{-1}}(v) = AA^{-1}v = v.$$

Se μ_A ha inversa, la sua matrice A, risp. alla base canonica, ha inversa per 2.5 . ■

A volte si può scomporre un omomorfismo in somma di certe sue restrizioni:

(2.7) Teorema *Dato un R-modulo $V = V_1 \dot{+} V_2$ con V_1 e V_2 liberi, con rispettive basi*

$$\mathcal{B}_1 = \{u_1, \cdots, u_m\}, \quad \mathcal{B}_2 = \{w_1, \cdots, w_\ell\},$$

sia $\alpha : V \to V$ un R-omomorfismo tale che V_1 e V_2 siano α-invarianti, ossia:

$$\alpha(V_1) \leq V_1, \quad \alpha(V_2) \leq V_2.$$

Dette A_1 la matrice della restrizione α_{V_1} rispetto $\mathcal{B}_1$ e A_2 quella della restrizione α_{V_2} rispetto $\mathcal{B}_2$, la matrice di α rispetto $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ è

$$A = \begin{pmatrix} A_1 & \\ & A_2 \end{pmatrix}.$$

Dimostrazione. $\mathcal{B}$ è una base di V per il Lemma 5.11 del Capitolo I. Posto

$$A_1 = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \dots & \dots & \dots \\ a_{m1} & \dots & a_{mm} \end{pmatrix}, \quad A_2 = \begin{pmatrix} b_{11} & \cdots & b_{1\ell} \\ \dots & \dots & \dots \\ b_{\ell 1} & \dots & b_{\ell\ell} \end{pmatrix},$$

si ha

$$(2.8) \qquad \begin{cases} \alpha(u_1) = a_{11}u_1 + \cdots + a_{m1}u_m + 0\,w_1 + \cdots + 0\,w_\ell \\ \dots \quad \dots \quad \dots \\ \alpha(u_m) = a_{1m}u_1 + \cdots + a_{mm}u_m + 0\,w_1 + \cdots + 0\,w_\ell \\ \alpha(w_1) = 0\,u_1 + \cdots + 0\,u_m + b_{1,1}\,w_1 + \cdots + b_{\ell 1}\,w_\ell \\ \dots \quad \dots \quad \dots \\ \alpha(w_\ell) = 0\,u_1 + \cdots + 0\,u_m + b_{1\ell}w_1 + \cdots + b_{\ell\ell}\,w_\ell \end{cases}$$

■

3 Cambiamenti di base

(3.1) Definizione *Siano date due basi di un R-modulo libero V:*

$$\mathcal{B} = \{v_1, \dots, v_n\}, \quad \mathcal{B}' = \{v'_1, \dots, v'_n\}.$$

La matrice P dell'applicazione identica $id_V : V \to V$, rispetto $\mathcal{B}'$ e $\mathcal{B}$, si dice la matrice di passaggio *da $\mathcal{B}$ a $\mathcal{B}'$. Ossia $Pe_i = (v'_i)_{\mathcal{B}}$ per ogni i. In modo esplicito:*

(3.2)
$$\begin{cases} id_V(v'_1) = v'_1 = p_{11}v_1 + \cdots + p_{n1}v_n \\ \cdots \quad \cdots \quad \cdots \\ id_V(v'_n) = v'_n = p_{1n}v_1 + \cdots + p_{nn}v_n \end{cases} \iff P = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \cdots & & \\ p_{n1} & \cdots & p_{nn} \end{pmatrix}.$$

Poichè id_V è un R-isomorfismo, P ha inversa per il Lemma 2.5.

(3.3) Lemma *Per ogni $v \in V$ si ha:*

$$Pv_{\mathcal{B}'} = v_{\mathcal{B}}, \quad v_{\mathcal{B}'} = P^{-1}v_{\mathcal{B}}. \tag{3.4}$$

Dimostrazione.
In (2.4), sostituendo $\alpha : V \to W$, A, $\mathcal{B}$ e $\mathcal{C}$ rispettivamente con $id_V : V \to V$, P, $\mathcal{B}'$ e $\mathcal{B}$, si ha: $Pv_{\mathcal{B}'} = v_{\mathcal{B}}$. ■

Nel caso di $V = R^n$ diamo delle formulazioni più esplicite.

(3.5) Lemma *Sia $\{e_1, \dots, e_n\}$ la base canonica di R^n.*
1) *Per ogni matrice $P \in \mathrm{GL}_n(R)$ si ha che $\mathcal{B} = \{Pe_1, \dots, Pe_n\}$ è una base di R^n e P è la matrice di passaggio dalla base canonica a $\mathcal{B}$;*
2) *viceversa, se $\mathcal{B} = \{v_1, \dots, v_n\}$ è una base di R^n, la matrice $P = \left(v_1 \mid \cdots \mid v_n \right)$ è la matrice di passaggio dalla base canonica a $\mathcal{B}$. In particolare $P \in \mathrm{GL}_n(R)$.*

Dimostrazione.
1) Poichè $P \in \mathrm{GL}_n(R)$, l'applicazione $\mu_P : R^n \to R^n$ tale che $v \to Pv$ è un R-isomorfismo per il Teorema 2.6 del Capitolo I. Ne segue che $\{\mu_P(e_1), \dots, \mu_P(e_n)\} = \{Pe_1, \dots, Pe_n\}$ è una base di $({}_RR)^n$ per il Teorema 5.10 del Capitolo 1. P è la matrice di passaggio dalla base canonica a $\mathcal{B}$ perchè ogni vettore Pe_i coincide con il proprio vettore coordinate rispetto alla base canonica.
2) P è la matrice di passaggio dalla base canonica a $\mathcal{B}$ perchè ogni vettore $Pe_i = v_i$ coincide con il proprio vettore coordinate rispetto alla base canonica. ■

4 Equivalenza fra matrici

Ricordiamo che $\mathrm{Mat}_{n,n}(R) := \mathrm{Mat}_n(R)$ è un anello e che $\mathrm{GL}_n(R) := \mathrm{Mat}_n(R)^*$ denota il gruppo delle matrici invertibili.

(4.1) Definizione *Date $A, B \in \mathrm{Mat}_{m,n}(R)$, diciamo che B è* equivalente *ad A se esistono due matrici $Q \in \mathrm{GL}_m(R)$, $P \in \mathrm{GL}_n(R)$ tali che $B = Q^{-1}AP$.*

Si verifica facilmente che la relazione di equivalenza fra matrici è riflessiva, simmetrica e transitiva e ripartisce quindi $\mathrm{Mat}_{m,n}(R)$ in classi di equivalenza.
Il significato geometrico dell'equivalenza fra matrici è evidenziato dal seguente:

(4.2) Lemma *Siano $A, B \in \mathrm{Mat}_{m,n}(R)$. Fissate una base $\mathcal{B}$ di V e una base $\mathcal{C}$ di W, sia $\alpha : V \to W$ l' R-omomorfismo indotto da A rispetto a $\mathcal{B}$, $\mathcal{C}$. Allora B é equivalente ad A se e solo α é l'omomorfismo indotto da B rispetto ad altre basi $\mathcal{B}'$ di V, $\mathcal{C}'$ di W.*

Dimostrazione.
Supponiamo che B sia la matrice di α rispetto $\mathcal{B}'$ e $\mathcal{C}'$. Dette P la matrice di passaggio da $\mathcal{B}$ a $\mathcal{B}'$ e Q la matrice di passaggio da $\mathcal{C}$ a $\mathcal{C}'$, per ogni $v \in V$ si ha:

$$(Q^{-1}AP)v_{\mathcal{B}'} \;=\; (Q^{-1}AP)P^{-1}v_{\mathcal{B}} \;=\; Q^{-1}Av_{\mathcal{B}} \;=\; Q^{-1}(\alpha(v))_{\mathcal{C}} = \;(\alpha(v))_{\mathcal{C}'}\,.$$

Ne segue che $Q^{-1}AP$ è la matrice di α rispetto $\mathcal{B}'$ e $\mathcal{C}'$, da cui $B = Q^{-1}AP$.
Viceversa, supponiamo $B = Q^{-1}AP$, con $P = (p_{ij})$, $Q = (q_{ij})$. Posto

$$\mathcal{B} = \{v_1, \ldots, v_n\}\,, \quad \mathcal{C} = \{w_1, \ldots, w_m\}\,,$$

consideriamo i vettori

$$v'_i = \sum_{j=1}^{n} p_{ji}v_j, \quad i = 1, \ldots, n; \qquad w'_i = \sum_{j=1}^{m} q_{ji}w_j, \quad i = 1, \ldots m$$

e definiamo

$$\mathcal{B}' = \left\{v'_1, \ldots, v'_n\right\}, \quad \mathcal{C}' = \left\{w'_1, \ldots, w'_m\right\}.$$

Si ha che P è la matrice di passaggio da $\mathcal{B}$ a $\mathcal{B}'$ e Q è la matrice di passaggio da $\mathcal{C}$ a $\mathcal{C}'$.
Per la prima parte della dimostrazione, $Q^{-1}AP$ è la matrice di α rispetto $\mathcal{B}', \mathcal{C}'$. ∎

5 Forme normali sui dominii a ideali principali

Nel resto della dispensa, D indica un *dominio a ideali principali*, cioè un anello commutativo, privo di divisori dello zero, in cui ogni ideale I è principale. Ricordiamo che un ideale I è principale se esiste $d \in I$ tale che $I = Dd = \{xd \mid x \in D\}$. Si scrive anche $I = \langle d \rangle$. Sono dominii a ideali principali, in quanto dominii euclidei:

• l'anello $\mathbb{Z}$ dei numeri interi;

• ogni *campo* (per esempio $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p := \frac{\mathbb{Z}}{p\mathbb{Z}}$ con p primo);

• l'anello $\mathbb{K}[x]$ dei polinomi nella indeterminata x, a coefficienti in un campo $\mathbb{K}$.

Gli unici ideali di un campo $\mathbb{K}$ sono $\{0_{\mathbb{K}}\}$ e $\mathbb{K}$. Invece $\mathbb{Z}$ e $\mathbb{K}[x]$ hanno infiniti ideali. Ogni ideale $I \neq \{0\}$ di $\mathbb{Z}$ è generato da i_0, dove i_0 è il minimo intero positivo appartenente ad I. Analogamente, ogni ideale $I \neq \{0\}$ di $\mathbb{K}[x]$ è generato da $m(x)$, dove $m(x)$ è il polinomio monico di grado minimo appartenente a I.

Ricordiamo che una matrice è *pseudodiagonale* se gli elementi non diagonali sono tutti nulli. Inoltre si dice *forma normale* ogni matrice pseudodiagonale tale che ogni elemento d_i sulla diagonale principale divida il successivo d_{i+1}.

Per [10, Teorema 3.3, Capitolo IV], due forme normali

$$\text{pseudodiag}\,(d_1, \ldots, d_m)\,,\ d_i | d_{i+1}, \quad \text{pseudodiag}\,\left(d'_1, \ldots, d'_m\right),\ d'_i | d'_{i+1}$$

sono equivalenti se e solo se $d'_i = \nu_i d_i$ con $\nu_i \in D^*$ per $i \leq m$.

Per [10, Teorema 2.4, Capitolo IV], ogni matrice $A \in \text{Mat}_{m,n}(D)$ è equivalente ad una forma normale $A' \in \text{Mat}_{m,n}(D)$, detta *forma normale* di A. Posto

$$A' = \text{pseudodiag}\,(d_1, \ldots, d_m)\,, \quad d_1 | d_2 | \ldots\ | d_m \tag{5.1}$$

$d_1, \ldots, d_m$ si chiama la sequenza dei *fattori invarianti* di A. Essa è unica, a meno di moltiplicazioni per elementi unitari, per il Teorema 3.3, citato sopra. Questo fatto giustifica la seguente:

(5.2) Definizione *Diciamo* rango *di una matrice $A \in \text{Mat}_{m,n}(D)$ il numero dei suoi fattori invarianti non nulli.*

Si noti che, se $\mathbb{K}$ è un campo, sempre per [10, Teorema 3.3, Capitolo IV], ogni forma normale in $\text{Mat}_{m,n}(\mathbb{K})$ può essere scelta in modo che le sue componenti siano $0_{\mathbb{K}}$ o $1_{\mathbb{K}}$.

(5.3) Esempio *Ogni matrice $A \in \text{Mat}_{2,3}(\mathbb{Q})$ è equivalente a una e una sola delle seguenti forme normali:*

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

Nel primo caso ha rango 0*, nel secondo ha rango* 1*, nel terzo ha rango* 2*.*

D'altra parte:

(5.4) Esempio *In* $A \in \mathrm{Mat}_{2,3}(\mathbb{Z})$ *le forme normali*

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

hanno entrambe rango 1*, ma non sono equivalenti.*

(5.5) Lemma *Una matrice* A *e la sua trasposta* A^t *hanno lo stesso rango.*

Dimostrazione. Sia A' una forma normale di A e siano X, Y matrici invertibili tali che $XAY = A'$. Allora anche X^t e Y^t sono invertibili. Da $Y^t A^t X^t = (A')^t$ si ha che $(A')^t$ è una forma normale di A^t. Chiaramente le componenti non nulle delle matrici pseudodiagonali A' e $(A')^t$ sono le stesse. Si conclude che A e A^t hanno lo stesso rango. ■

6 Esercizi

(6.1) Esercizio *Considerata la base di* $\mathbb{R}^3$

$$\mathcal{B}' = \left\{ \begin{pmatrix} -1 \\ 2 \\ 6 \end{pmatrix}, \begin{pmatrix} -3 \\ 4 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ -3 \\ -1 \end{pmatrix} \right\}$$

si calcolino:

1) *la matrice di passaggio* P *dalla base canonica* $\mathcal{B}$ *di* $\mathbb{R}^3$ *a* $\mathcal{B}'$*;*

2) *i vettori coordinate*

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}_{\mathcal{B}'}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}_{\mathcal{B}'}, \begin{pmatrix} 0 \\ 2 \\ -4 \end{pmatrix}_{\mathcal{B}'}, \begin{pmatrix} x \\ y \\ z \end{pmatrix}_{\mathcal{B}'}.$$

(6.2) Esercizio *Considerate le basi di* $\mathbb{R}^3$*:*

$$\mathcal{B} = \left\{ \begin{pmatrix} -1 \\ 2 \\ 6 \end{pmatrix}, \begin{pmatrix} -3 \\ 4 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ -3 \\ -1 \end{pmatrix} \right\},$$

$$\mathcal{B}' = \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 4 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \\ 1 \end{pmatrix} \right\}$$

si calcolino:

1) *la matrice di passaggio P da $\mathcal{B}$ a $\mathcal{B}'$;*

2) *i vettori coordinate*

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}_{\mathcal{B}'}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}_{\mathcal{B}'}, \begin{pmatrix} 0 \\ 2 \\ -4 \end{pmatrix}_{\mathcal{B}'}, \begin{pmatrix} x \\ y \\ z \end{pmatrix}_{\mathcal{B}'}.$$

(6.3) Esercizio *Dati gli omomorfismi $\alpha : \mathbb{Z}^3 \to \mathbb{Z}^2$, $\beta : \mathbb{Z}^2 \to \mathbb{Z}^2$ tali che:*

$$\alpha : \begin{pmatrix} x \\ y \\ z \end{pmatrix} \mapsto \begin{pmatrix} x+y-z \\ 3x-y \end{pmatrix}, \quad \beta : \begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 3x-4y \\ x \end{pmatrix}$$

si scriva la matrice di α, quella di β e quella di $\beta\alpha$

1) *rispetto alle basi canoniche di $\mathbb{Z}^3$ e $\mathbb{Z}^2$;*

2) *rispetto alle basi $\mathcal{B}$ di $\mathbb{Z}^3$ e $\mathcal{C}$ di $\mathbb{Z}^2$, dove:*

$$\mathcal{B} = \left\{ \begin{pmatrix} -1 \\ 2 \\ 6 \end{pmatrix}, \begin{pmatrix} -3 \\ 4 \\ 7 \end{pmatrix}, \begin{pmatrix} 3 \\ -3 \\ -1 \end{pmatrix} \right\}, \quad \mathcal{C} = \left\{ \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$$

(6.4) Esercizio *Si dica se l'applicazione $\mathbb{Z}^2 \to \mathbb{Z}^2$ tale che*

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x^2+y \\ x-y \end{pmatrix}$$

è uno $\mathbb{Z}$-omomorfismo, giustificando la risposta.

(6.5) Esercizio *Data l'applicazione lineare $\alpha : \mathbb{Q}^2 \to \mathbb{Q}^2$ tale che*

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} 3x-4y \\ x+2y \end{pmatrix}$$

1) *si trovino due basi $\mathcal{B}$ e $\mathcal{C}$ di $\mathbb{Q}^2$ tali che la matrice di α rispetto rispetto $\mathcal{B}$ e $\mathcal{C}$ sia quella identica;*

2) *si dimostri che non esistono due basi uguali, ossia $\mathcal{B} = \mathcal{C}$, tali che la matrice di α rispetto $\mathcal{B}$ e $\mathcal{B}$ sia quella identica.*

(6.6) Esercizio *Si trovi una base $\mathcal{B}$ di $V := \frac{\mathbb{Q}[x]}{\langle x^2-3 \rangle}$ come $\mathbb{Q}$-modulo e si scriva la matrice della applicazione lineare $\mu_x : V \to V$ tale che*

$$\langle x^2-3 \rangle + f(x) \mapsto \langle x^2-3 \rangle + xf(x)$$

rispetto a $\mathcal{B}$.

(6.7) Esercizio *Siano A equivalente ad A' e B equivalente a B'. Si dimostri che sono equivalenti le matrici:*

$$\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}, \quad \begin{pmatrix} A' & 0 \\ 0 & B' \end{pmatrix}.$$

.

(6.8) Esercizio *Si trovi una base $\mathcal{B}$ di $V := \frac{\mathbb{Q}[x]}{\langle x^4-9\rangle}$ come $\mathbb{Q}$-modulo e si scriva la matrice, rispetto a $\mathcal{B}$, della applicazione lineare $\mu_x : V \to V$ tale che*

$$\langle x^4 - 9\rangle + f(x) \mapsto \langle x^4 - 9\rangle + xf(x).$$

(6.9) Esercizio *Si trovi una base $\mathcal{B}$ di*

$$V := \frac{\mathbb{Q}[x]}{\langle x^2 - 3\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x^4 - 9\rangle}$$

come $\mathbb{Q}$-modulo e si scriva la matrice, rispetto a $\mathcal{B}$, della applicazione lineare $\mu_x : V \to V$ tale che $v \mapsto xv$.

(6.10) Esercizio *Si trovi una base $\mathcal{B}$ di*

$$V := \frac{\mathbb{Q}[x]}{\langle x - 3\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x + 1\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x\rangle}$$

come $\mathbb{Q}$-modulo e si scriva la matrice, rispetto a $\mathcal{B}$, della applicazione lineare $\mu_x : V \to V$ tale che $v \mapsto xv$.

Capitolo III

Moduli finitamente generati su PID

1 Basi di sottomoduli

Chiaramente i sottomoduli del D-modulo regolare ${}_DD$ sono gli ideali dell'anello D.

(1.1) Lemma *Se D è un dominio a ideali principali, i sottomoduli di ${}_DD$ sono liberi, di rango ≤ 1.*

Dimostrazione. Sia I un sottomodulo di D. Poichè I è un ideale dell'anello D, i cui ideali sono principali, esiste $d \in I$ tale che $I = \langle d \rangle$. Se $d = 0_D$, si ha che $I = \{0_D\}$ è libero di rango 0. Altrimenti $\{d\}$ è una base di I: infatti $I = Dd$ e $xd = 0_D$ implica $x = 0_D$, poichè D è privo di divisori dello zero. Quindi I è libero, di rango 1. ■

(1.2) Teorema *Sia V un D-modulo libero di rango n. Se D è un dominio a ideali principali, ogni sottomodulo W di V è libero, di rango $m \leq n$.*

Dimostrazione. Ragioniamo per induzione su n.
Se $n = 0$, si ha $V = \{0_V\}$. Ne segue $W = \{0_V\}$, che è quindi libero, di rango 0.
Sia ora $n > 0$. In virtù di (5.4) del Capitolo II, possiamo supporre $V = D^n$.
Consideriamo l'n-esima proiezione $\pi : D^n \to D$ tale che:

$$\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \mapsto x_n.$$

Chiaramente Ker π è l'insieme delle n-ple che hanno l'ultima componente nulla. Quindi:

$$\text{Ker } \pi \simeq D^{n-1} . \tag{1.3}$$

Il sottomodulo $\pi(W)$ di D è libero, di rango ≤ 1, per il Lemma precedente. Consideriamo la restrizione di π a W, ossia l'epimorfismo:

$$\pi_W : W \to \pi(W).$$

Per il Teorema 5.12 del Capitolo 1, esiste un sottomodulo L^* di W tale che

$$L^* \simeq \pi(W) \quad \text{e} \quad \mathrm{W} = \mathrm{Ker}\ \pi_{\mathrm{W}} \dot{+} \mathrm{L}^*.$$

Ora Ker $\pi_W = \mathrm{Ker}\ \pi \cap W \leq \mathrm{Ker}\ \pi$. Per 1.3, il modulo Ker π è libero, di rango $n-1$. Quindi, per l'ipotesi induttiva, Ker π_W è libero di rango $m \leq n-1$. D'altra parte $L^* \simeq \pi(W)$ è libero di rango $\ell \leq 1$. Pertanto W è libero, di rango $m+\ell$ per il Teorema 6.3 del Capitolo I. Si conclude che $m+\ell \leq (n-1)+1 = n$. ■

(1.4) Corollario *Sia V uno spazio vettoriale di dimensione n su $\mathbb{K}$. Ogni sottoinsieme indipendente $\mathcal{B} = \{v_1, \cdots, v_n\}$ è una base di V.*

Dimostrazione. Dobbiamo dimostrare che ogni $v \in V$ è combinazione lineare di elementi di $\mathcal{B}$. Se $v \in \mathcal{B}$, questo è chiaro. In caso contrario l'insieme $S := \{v_1, \cdots, v_n, v\}$ ha $n+1$ elementi. Non può quindi essere indipendente, altrimenti genererebbe un sottomodulo di rango $n+1$. Esistono quindi degli scalari non tutti nulli tali che $k_1v_1+\cdots+k_nv_n+kv = 0_V$. Se fosse $k = 0_{\mathbb{K}}$, avremmo $k_1v_1 + \cdots + k_nv_n = 0_V$ da cui anche $k_1 = \cdots = k_n = 0_{\mathbb{K}}$, per l'indipendenza di $\mathcal{B}$. Ne segue $k \neq 0_{\mathbb{K}}$ da cui $v = -k^{-1}k_1v_1 - \cdots - k^{-1}k_nv_n$. ■

Sia $A \in \mathrm{Mat}_{m,n}(D)$. Le colonne $Ae_1, \cdots, Ae_n$ di A sono elementi di D^m. Analogamente le righe di A sono elementi del trasposto di D^n. Possiamo quindi considerare il sottomodulo di $({}_DD)^m$, generato dalle colonne di A, e quello del trasposto di $({}_DD)^n$, generato dalle righe di A. Questi moduli sono entrambi liberi, per il Teorema precedente. Abbastanza sorprendetemente hanno lo stesso rango. Infatti:

(1.5) Teorema *Data $A \in \mathrm{Mat}_{m,n}(D)$, dove D è un dominio a ideali principali, sia $\mu_A : D^n \to D^m$ il D-omomorfismo indotto da A rispetto alle basi canoniche, ossia:*

$$\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \mapsto A \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}. \tag{1.6}$$

Il sottomodulo generato dalle colonne di A coincide con l'immagine $\mu_A(D^n) = \mathrm{Im}\ \mu_A$, che ha lo stesso rango r di A, essendo r il numero delle componenti non nulle di una forma normale A' di A. Il sottomodulo generato dalle righe di A, ha anch'esso rango r.

Dimostrazione. Per il Lemma 3.8 del Capitolo I, si ha:

$$\text{Im } \mu_A \;=\; \langle \mu_A(e_1),\ \cdots,\ \mu_A(e_n)\rangle \;=\; \langle Ae_1,\ \cdots,\ Ae_n\rangle \ .$$

Sia ora $A' = \text{pseudodiag}\,(d_1,\ \cdots,\ d_r,\ 0, \cdots)$, dove $d_i | d_{i+1}$, una forma normale di A.
Se A ha rango $r = 0$, si ha $d_1 = 0$, $A' = 0_{\text{Mat}_{m,n}(D)}$. Ne segue $A = 0_{\text{Mat}_{m,n}(D)}$ e l'asserto è ovvio. Sia quindi $r > 0$, ossia $d_r \neq 0$. Dette Q, P due matrici invertibili tali che $A' = Q^{-1}AP$, si ha che A' è la matrice di μ_A rispetto alle basi $\mathcal{B}' = \{Pe_1, \cdots, Pe_n\}$ e $\mathcal{C}' = \{Qe_1, \cdots, Qe_m\}$ di $({}_DD)^n$ e $({}_DD)^m$. Posto $Pe_i = v_i$, $Qe_i = w_i$ otteniamo quindi:

$$\text{Im } \mu_A = \langle \mu_A(v_1), \cdots, \mu_A(v_n)\rangle \;=\; \langle d_1w_1, \cdots, d_rw_r\rangle\,.$$

Pertanto Im μ_A è generato dall'insieme $\mathcal{C}' = \{d_1w_1, \cdots, d_rw_r\}$. Si verifica facilmente che, essendo D privo di divisori dello zero, $\mathcal{C}'$ è indipendente ed è quindi una base di Im μ_A. Si conclude che Im μ_A ha rango r.
Infine, il rango di A^t è anch'esso r, per il Lemma 5.5 del Capitolo I. Applicando ad A^T il risultato appena dimostrato per A, si ha che il sottomodulo generato dalle colonne di A^T ha rango r. Poichè le righe di A coincidono con le colonne di A^T, si ha l'asserto. ∎

(1.7) Corollario *Sia $AX = 0_{\mathbb{K}^n}$ un sistema lineare omogeneo, a coefficienti in un campo $\mathbb{K}$, in m equazioni indipendenti e $n \geq m$ indeterminate. L'insieme W delle sue soluzioni è un sottospazio di $\mathbb{K}^n$ avente dimensione $n - m$.*

Dimostrazione. La matrice A dei coefficienti del sistema appartiene a $\text{Mat}_{m,n}(\mathbb{K})$. Il rango di A è m, dato che stiamo supponendo che le equazioni siano indipendenti. Per il Teorema precedente, l'immagine dell'applicazione lineare

$$\mu_A : \mathbb{K}^n \to \mathbb{K}^m$$

definita in (1.6) ha dimensione m. Notando che $W = \text{Ker } \mu_A$ si ha che W è un sottospazio. Inoltre, tenendo presente il Teorema 5.12 del Capitolo 1, $n = \dim(\mathbb{K}^n) = \dim(\text{Ker } \mu_A) + \dim(\text{Im } \mu_A)$, da cui $\dim W = n - m$. ∎

(1.8) Teorema *Siano V un D-modulo libero di rango n e W un suo sottomodulo di rango t. Se D è un dominio a ideali principali, esistono una base $\mathcal{B} = \{v_1, \cdots, v_n\}$ di V e una sequenza $d_1, \cdots, d_t$ di elementi non nulli di D, ciascuno dei quali divide il successivo, tali che $\mathcal{C} = \{d_1v_1, \cdots, d_tv_t\}$ è una base di W.*

Dimostrazione. Sia $\alpha : W \to V$ l'inclusione $w \mapsto w$. Per il Lemma 4.2 del Capitolo II, esistono una base $\mathcal{C} = \{w_1, \cdots, w_t\}$ di W e una base $\mathcal{B} = \{v_1, \cdots, v_n\}$ di V tali che la matrice di α rispetto $\mathcal{C}$ e $\mathcal{B}$ è una forma normale

$$A' = \begin{pmatrix} d_1 & 0 & \cdots & 0 \\ 0 & d_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & d_t \\ \cdots & \cdots & \cdots & \cdots \end{pmatrix}, \quad d_1 | d_2 | \cdots | d_t \ .$$

Ne segue che $w_i = \alpha(w_i) = d_i v_i$ $(1 \leq i \leq t)$ e si conclude che $\mathcal{C} = \{d_1 v_1, \cdots, d_t v_t\}$. ■

2 Ideali annullatori

Sia M un D-modulo.

(2.1) Definizione *Diciamo* annullatore *di un elemento $m \in M$, e lo indichiamo con* $\mathrm{Ann}\,(m)$*, l'insieme degli elementi $d \in D$ tali che $dm = 0_M$.*

(2.2) Lemma $\mathrm{Ann}\,(m)$ *è un ideale di D.*

Dimostrazione.
1) $0_D \in \mathrm{Ann}\,(m)$ poichè $0_D m = 0_M$.
2) $x_1, x_2 \in \mathrm{Ann}\,(m) \quad \Rightarrow \quad (x_1 + x_2) \in \mathrm{Ann}\,(m)$.
Infatti $(x_1 + x_2)m = x_1 m + x_2 m = 0_M - 0_M = 0_M$.
3) $d \in D,\ x \in \mathrm{Ann}\,(m) \quad \Rightarrow \quad (dx) \in \mathrm{Ann}\,(m)$.
Infatti $(dx)m = d(xm) = d0_M = 0_M$. ■

(2.3) Definizione *Chiamiamo* annullatore *di M, e lo indichiamo con* $\mathrm{Ann}\,(M)$*, l'insieme degli elementi $d \in D$ tali che $dm = 0_M$ per ogni $m \in M$.*

Notando che $\mathrm{Ann}\,(M) = \bigcap_{m \in M} \mathrm{Ann}\,(m)$, si ha subito che è un ideale di D, in quanto intersezione di ideali.

(2.4) Lemma *Sia $f : M \to M'$ un epimorfismo di D-moduli. Allora*

$$\mathrm{Ann}\,(M) \leq \mathrm{Ann}\,(M').$$

In particolare D-moduli isomorfi hanno lo stesso annullatore.

Dimostrazione. Sia $x \in \mathrm{Ann}\,(M)$. Per ogni $m' \in M'$, detta m una sua preimmagine in M, si ha: $xm' = xf(m) = f(xm) = f(0_M) = 0_{M'}$. Pertanto $\mathrm{Ann}\,(M) \leq \mathrm{Ann}\,(M')$. Infine, se f è un isomorfismo, considerando l'isomorfismo $f^{-1} : M' \to M$ otteniamo $\mathrm{Ann}\,(M') \leq \mathrm{Ann}\,(M)$ e concludiamo $\mathrm{Ann}\,(M') = \mathrm{Ann}\,(M)$. ■

(2.5) Definizione *Un elemento $m \in M$ si dice* di torsione *se* $\mathrm{Ann}\,(m) \neq \{0_D\}$.

(2.6) Lemma *Per ogni $n \geq 0$ l'unico elemento di torsione di $({}_DD)^n$ è lo zero.*

Dimostrazione. Sia $d \begin{pmatrix} d_1 \\ \cdots \\ d_n \end{pmatrix} = \begin{pmatrix} 0_D \\ \cdots \\ 0_D \end{pmatrix}$. Ne segue $dd_i = 0_D$ per ogni $i \leq n$.
Pertanto $d \neq 0$ implica $d_i = 0$ per $i \leq n$, essendo D privo di divisori dello zero. ■

(2.7) Lemma *L'insieme T degli elementi di torsione di M è un sottomodulo.*

Dimostrazione.
1) $0_M \in T$ dato che $\mathrm{Ann}\,(0_M) = D$.
2) $t_1, t_2 \in T \quad \Rightarrow \quad (t_1 + t_2) \in T$.
Siano $x_1,\ x_2$ elementi non nulli di D tali che $x_1t_1 = x_2t_2 = 0_M$. Si ha $x_1x_2 \neq 0_D$ e $x_1x_2(t_1 + t_2) = x_2(x_1t_1) + x_1(x_2t_2) = 0_M$. Quindi $(t_1 + t_2) \in T$.
3) $d \in D,\ t \in T \quad \Rightarrow \quad (dt) \in T$.
Sia x un elemento non nullo di D tale che $xt = 0_M$. Ne segue $x(dt) = (xd)t = (dx)t = d(xt) = d0_M = 0_M$ e si conclude che $dt \in T$. ■

(2.8) Definizione
• *T è detto il* sottomodulo di torsione *di M.*
• *Se $M = T$ si dice che M è di torsione.*

(2.9) Lemma *Sia $f : M \to M'$ un D-omomorfismo. Detto T il sottomodulo di torsione di M e T' quello di M', si ha $f(T) \leq T'$. In particolare D-moduli isomorfi hanno sottomoduli di torsione isomorfi.*

Dimostrazione. Sia $t \in T$. Esiste $0 \neq x \in D$ tale che $xt = 0_M$. Ne segue $xf(t) = f(xt) = f(0_M) = 0_{M'}$. Pertanto $f(t) \in T'$. Abbiamo così dimostrato che $f(T) \leq T'$.

Ora, se f è un isomorfismo, anche $f^{-1} : M' \to M$ lo è . Per quanto appena dimostrato $f^{-1}(T') \leq T$. Applicando f si ha $T' \leq f(T)$. Si conclude che $f(T) = T'$. Basta infine notare che la restrizione di f a T è un isomorfismo da T a T'. ■

(2.10) Lemma *M_1 e M_2 siano sottomoduli di M. T e L siano D-moduli.*
1) *se $M = M_1 + M_2$, allora* $\mathrm{Ann}\,(M) = \mathrm{Ann}\,(M_1) \cap \mathrm{Ann}\,(M_2)$.
2) *Se $M = T \oplus L$ dove T è di torsione e L è libero, allora il sottomodulo di torsione T' di M è isomorfo a T.*

Dimostrazione.
1) Sia $x \in \mathrm{Ann}\,(M)$. Poichè x annulla tutti gli elementi di M, annulla anche quelli dei suoi sottoinsiemi M_1 e M_2. Quindi $\mathrm{Ann}\,(M) \leq \mathrm{Ann}\,(M_1) \cap \mathrm{Ann}\,(M_2)$. Viceversa, sia $y \in \mathrm{Ann}\,(M_1) \cap \mathrm{Ann}\,(M_2)$. Ogni elemento m di M si scrive nella forma $m = m_1 + m_2$, per opportuni $m_1 \in M_1$, $m_2 \in M_2$. Ne segue $ym = ym_1 + ym_2 = 0_M + 0_M = 0_M$. Concludiamo $\mathrm{Ann}\,(M_1) \cap \mathrm{Ann}\,(M_2) \leq \mathrm{Ann}\,(M)$.
2) L'applicazione $f : T \to M$ tale che $t \mapsto \begin{pmatrix} t \\ 0_L \end{pmatrix}$ è un D-monomorfismo.
Essendo T di torsione, per il Lemma 2.9 si ha $f(T) \leq T'$, dove:

$$f(T) = \left\{ \begin{pmatrix} t \\ 0_L \end{pmatrix} \mid t \in T \right\}.$$

D'altra parte $T' \leq f(T)$. Infatti sia $m = \begin{pmatrix} t \\ l \end{pmatrix}$ un elemento di T', dove $t \in T$, $l \in L$. Esiste $d \neq 0$ tale che $dm = 0_M$, ossia $\begin{pmatrix} dt \\ dl \end{pmatrix} = \begin{pmatrix} 0_T \\ 0_L \end{pmatrix}$. In particolare $dl = 0_L$. Ma L, essendo libero, è privo di torsione per il Lemma 2.6: quindi $l = 0_L$. Si conclude che $f(T) = T'$. Chiaramente la restrizione di f a T è un D-isomorfismo da T a T'. ■

3 Teorema di Struttura

Un D-modulo M si dice *finitamente generato* (f.g.), se è generato da un sottoinsieme finito. In tal caso indichiamo con $\mathrm{d}(M)$ il *minimo numero di generatori* di M. Nel seguito il D-modulo regolare ${}_DD$ verrà indicato, per brevità , semplicemente con D.

(3.1) Lemma *Siano I un ideale di D e $\frac{D}{I}$ il modulo quoziente.*
1) $\mathrm{Ann}\,\left(\frac{D}{I}\right) = I$;
2) *se $I \neq D$, allora* $\mathrm{d}\left(\frac{D}{I}\right) = 1$.

Dimostrazione.
1) Sia $x \in \text{Ann}\left(\frac{D}{I}\right)$. In particolare $x(I+1_D) = I+x = I+0_D$ implica $x \in I$. Viceversa se $i \in I$, per ogni $x \in D$ si ha $ix \in I$ da cui $i(I+x) = I+ix = I+0_D$.
2) $\frac{D}{I} \neq 0$ è generato da $I+1_D$. ■

Come al solito, indichiamo con D^* l'insieme degli elementi unitari di D, ossia degli elementi $u \in D$ che hanno inverso u^{-1} in D.

(3.2) Teorema *Sia M un D-modulo f.g., e sia* $\mathrm{d}(M) = n$. *Esiste una sequenza*

$$d_1,\ \cdots,\ d_n \quad \text{(sequenza dei fattori invarianti di } M) \tag{3.3}$$

dove ogni $d_i \in D$, $d_1 \notin D^*$ e d_i divide d_{i+1} per $i \leq n-1$, tale che:

$$M \simeq \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_n \rangle} \quad \text{(forma normale di } M). \tag{3.4}$$

Sia $t \geq 0$ tale che $d_i \neq 0_D$ per $i \leq t$ e $d_{t+1} = 0_D$. Allora, posto

$$T := \{0\} \text{ se } t = 0, \quad T := \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_t \rangle} \text{ se } t > 0, \tag{3.5}$$

T è isomorfo al sottomodulo di torsione di M. Per $t > 0$, risulta $\text{Ann}\,(T) = \langle d_t \rangle$. *Quindi*

$$M \simeq T \oplus D^{n-t}$$

dove T è di torsione e D^{n-t} è libero, di rango $n-t$.

Dimostrazione. Se d(M)=0, si ha $M = \{0_M\} = D^0$. Possiamo quindi supporre $n > 0$. Sia $\{m_1, \cdots, m_n\}$ un insieme di generatori per M. L'applicazione

$$\Phi : D^n \to M \quad \text{tale che} \quad \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \mapsto \sum_{i=1}^{n} x_i m_i$$

è un epimorfismo di D-moduli. Per il Teorema 3.12 del Capitolo I si ha

$$\frac{D^n}{\text{Ker } \Phi} \simeq M.$$

Sia t il rango di Ker Φ. Per il Teorema 1.8 di questo Capitolo esistono una base $\mathcal{B} = \{v_1, \cdots, v_n\}$ di D^n e una sequenza $d_1, \cdots, d_t$ di elementi non nulli di D, ciascuno dei quali divide il successivo, tali che $\mathcal{C} = \{d_1 v_1, \cdots, d_t v_t\}$ è una base di Ker Φ. A meno di un isomorfismo di D^n possiamo supporre che $\mathcal{B} = \{v_1, \cdots, v_n\}$ sia la base canonica di

D^n, quindi

$$\text{Ker } \Phi \;=\; \left\langle \begin{pmatrix} d_1 \\ \cdots \\ 0_D \\ 0_D \\ \cdots \\ 0_D \end{pmatrix}, \cdots, \begin{pmatrix} 0_D \\ \cdots \\ d_t \\ 0_D \\ \cdots \\ 0_D \end{pmatrix} \right\rangle \;=\; \left\{ \begin{pmatrix} x_1 d_1 \\ \cdots \\ x_t d_t \\ 0_D \\ \cdots \\ 0_D \end{pmatrix} \;\mid\; x_i \in D \right\}.$$

Si verifica facilmente che l'applicazione

$$f:\; D^n \;\to\; \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_t \rangle} \oplus D^{n-t}$$

tale che

$$\begin{pmatrix} x_1 \\ \cdots \\ x_t \\ x_{t+1} \\ \cdots \\ x_n \end{pmatrix} \;\mapsto\; \begin{pmatrix} \langle d_1 \rangle + x_1 \\ \cdots \\ \langle d_t \rangle + x_t \\ x_{t+1} \\ \cdots \\ x_n \end{pmatrix}$$

è un epimorfismo di moduli e che Ker $f =$ Ker Φ. Si conclude

$$M \;\simeq\; \frac{D^n}{\text{Ker } \Phi} \;=\; \frac{D^n}{\text{Ker } f} \;\simeq\; \frac{D}{\langle d_1 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_t \rangle} \oplus D^{n-t}.$$

Supponiamo, per assurdo, $\langle d_1 \rangle = D$. L'addendo $\frac{D}{\langle d_1 \rangle} = \frac{D}{D}$ sarebbe nullo. Pertanto M sarebbe isomorfo a $\frac{D}{\langle d_2 \rangle} \oplus \cdots \oplus \frac{D}{\langle d_t \rangle} \oplus D^{n-t}$ e avremmo la contraddizione $\mathrm{d}(M) \leq n-1$. Da $\text{Ann}\,(\frac{D}{\langle d_i \rangle}) = \langle d_i \rangle$ si ha $\text{Ann}\,(T) \;=\; \langle d_1 \rangle \cap \cdots \cap \langle d_t \rangle \;=\; \langle d_t \rangle$. Quindi T è di torsione. Per il Lemma 2.10, con $M_1 = T$ e $M_2 = D^{n-t}$ si conclude che T è isomorfo al sottomodulo di torsione di M. ■

Se $\mathbb{K}$ è un campo, ogni $\mathbb{K}$-modulo V è libero: tale risultato, nel caso V finitamente generato, segue anche dal precedente Teorema. Vale infatti:

(3.6) Corollario *Sia V uno spazio vettoriale su $\mathbb{K}$ e sia $\mathrm{d}(V) = n$. Allora $V \simeq \mathbb{K}^n$.*

Dimostrazione. Si ha necessariamente $d_1 = 0_{\mathbb{K}}$, altrimenti d_1 sarebbe unitario. ■

(3.7) Corollario *Sia M un gruppo abeliano finitamente generato, con $\mathrm{d}(M) = n$:*

- *$M \simeq \mathbb{Z}^n$, oppure*
- *$M \simeq \mathbb{Z}_{d_1} \oplus \cdots \mathbb{Z}_{d_t} \oplus \mathbb{Z}^{n-t}$, $t \leq n$,*

dove $d_1, \cdots, d_t$ è una sequenza di interi ≥ 2, ciascuno dei quali divide il successivo.

Dimostrazione. Si considera M come $\mathbb{Z}$-modulo, e si applica il Teorema 3.2 di questo Capitolo. Basta poi osservare che, per ogni intero positivo d, risulta $\frac{\mathbb{Z}}{\langle d\rangle} = \mathbb{Z}_d$. ■

In altre parole ogni gruppo abeliano finitamente generato è somma diretta di n gruppi ciclici, essendo n il minimo numero di elementi che lo generano. Inoltre gli eventuali addendi finiti possono essere ordinati in modo che l'ordine di ciascuno divida quello del successivo.

4 Fattori invarianti e divisori elementari

Una proprietà importante dei moduli finitamente generati, di torsione, è quella di poter essere "cancellati" in un isomorfismo fra somme dirette. Vale infatti:

(4.1) Teorema *Siano M_1, M_2, T e T' dei D-moduli. Si supponga che sia $T \simeq T'$, con T finitamente generato, di torsione. Allora:*

$$M_1 \oplus T \;\simeq\; M_2 \oplus T' \quad \Rightarrow \quad M_1 \;\simeq\; M_2.$$

Una dimostrazione si trova in [4].

(4.2) Corollario *Sia M un D-modulo f.g. La sua forma normale* (3.4)*, è unica.*

Dimostrazione. Supponiamo che M abbia due forme normali, necessariamente isomorfe:

$$\frac{D}{\langle d_1\rangle} \oplus \cdots \oplus \frac{D}{\langle d_t\rangle} \oplus \cdots \oplus \frac{D}{\langle d_n\rangle} \;\simeq\; \frac{D}{\langle c_1\rangle} \oplus \cdots \oplus \frac{D}{\langle c_h\rangle} \oplus \cdots \oplus \frac{D}{\langle c_k\rangle} \tag{4.3}$$

dove $d_i, c_i \in D$, $d_1, c_1 \notin D^*$, $d_i | d_{i+1}$ $(i \leq n-1)$, $c_i | c_{i+1}$ $(i \leq k-1)$.
I sottomoduli di torsione T e T' delle due forme normali sono isomorfi per il Lemma 2.9.
Caso 1 $T = \{0\}$, ossia $d_1 = \cdots = d_n = 0_D$. Ne segue $T' = \{0\}$, da cui $c_1 = \cdots =$
$= c_k = 0_D$. Infine $D^n \simeq D^k$ implica $n = k$.
Caso 2 Possiamo supporre:

$$T = \frac{D}{\langle d_1\rangle} \oplus \cdots \oplus \frac{D}{\langle d_t\rangle}, \quad T' = \frac{D}{\langle c_1\rangle} \oplus \cdots \oplus \frac{D}{\langle c_h\rangle}. \tag{4.4}$$

Poiché moduli isomorfi hanno lo stesso annullatore:

$$\langle d_t\rangle = \mathrm{Ann}\,(T) = \mathrm{Ann}\,(T') = \langle c_h\rangle.$$

Semplificando $\frac{D}{\langle d_t\rangle} = \frac{D}{\langle c_h\rangle}$ in (4.4) e applicando l'induzione si ha:

$$t - 1 = h - 1, \qquad \langle d_i\rangle = \langle c_i\rangle, \quad i = 1, \cdots, t-1.$$

In particolare $t = h$. Infine, semplificando $T \simeq T'$ in (4.3) si ha:

$$D^{n-t} \simeq D^{k-t}.$$

si conclude $n - t = k - t$, da cui $n = k$. ■

Chiaramente la sequenza (3.3) dei fattori invarianti di M determina la sua forma normale (3.4). Viceversa la forma normale di M determina (a meno di fattori unitari) la sequenza dei suoi fattori invarianti.

Ogni dominio a ideali principali D è fattoriale (si veda il Teorema 6.4.5 di [8]). Per comodità del lettore riportiamo il Teorema Cinese del Resto (Teorema 7.6.4 di [8]).

(4.5) Teorema *(Cinese del resto). Siano $a, b \in D$ tali che* M.C.D.$(a, b) = 1$. *Allora, per ogni $b_1, b_2 \in D$, il sistema di congruenze lineari*

$$\begin{cases} x \equiv b_1 \pmod{a} \\ x \equiv b_2 \pmod{b} \end{cases} \tag{4.6}$$

ha soluzioni in D.

Dimostrazione. Esistono $y, z \in D$ tali che $ay + bz = 1$. Moltiplicando per b_1 e per b_2:

$$\begin{matrix} ayb_1 + bzb_1 = b_1 \\ ayb_2 + bzb_2 = b_2 \end{matrix}.$$

Ne segue

$$\begin{matrix} bzb_1 \equiv b_1 \pmod{a} \\ ayb_2 \equiv b_2 \pmod{b} \end{matrix}.$$

Si conclude che $c = bzb_1 + ayb_2$ è soluzione del sistema (4.6). ■

(4.7) Teorema *Dato $d \in D$, con $d \neq 0_D$, $d \notin D^*$, sia $d = p_1^{m_1} \dots p_k^{m_k}$ la sua fattorizzazione in irriducibili $p_i \in D$, dove $p_i \neq p_j$, per $i \neq j$. Allora:*

$$\frac{D}{\langle d \rangle} \simeq \frac{D}{\langle p_1^{m_1} \rangle} \oplus \cdots \oplus \frac{D}{\langle p_k^{m_k} \rangle} \quad \text{(decomposizione primaria)}. \tag{4.8}$$

$p_1^{m_1}, \cdots, p_k^{m_k}$ *si dicono i* divisori elementari *di* $\frac{D}{\langle d \rangle}$.

Dimostrazione. Se $k \geq 2$, poniamo $a = p_1^{m_1}$, $b = p_2^{m_2} \dots p_k^{m_k}$. Sia ha $d = ab$ con M.C.D.$(a, b) = 1$. Si vede facilmente che l'applicazione

$$f : D \to \frac{D}{\langle a \rangle} \oplus \frac{D}{\langle b \rangle} \quad \text{tale che} \quad x \mapsto \begin{pmatrix} \langle a \rangle + x \\ \langle b \rangle + x \end{pmatrix}$$

è un D-omomorfismo. Inoltre f è suriettiva. Sia infatti $\begin{pmatrix} \langle a\rangle + b_1 \\ \langle b\rangle + b_2 \end{pmatrix}$ un generico elemento del codominio. Per il Teorema Cinese del resto esiste $c \in D$ tale che

$$\begin{cases} c \equiv b_1 \pmod{a} \\ c \equiv b_2 \pmod{b} \end{cases}$$

ossia

$$f(c) = \begin{pmatrix} \langle a\rangle + c \\ \langle b\rangle + c \end{pmatrix} = \begin{pmatrix} \langle a\rangle + b_1 \\ \langle b\rangle + b_2 \end{pmatrix}.$$

Infine Ker $f = \langle a\rangle \cap \langle b\rangle = \langle d\rangle$. Si conclude che

$$\frac{D}{\langle d\rangle} \simeq \frac{D}{\langle a\rangle} \oplus \frac{D}{\langle b\rangle} = \frac{D}{\langle p_1^{m_1}\rangle} \oplus \frac{D}{\langle p_2^{m_2} \dots p_k^{m_k}\rangle}$$

e l'asserto segue per induzione su k. ■

(4.9) Definizione *Sia* $T = \frac{D}{\langle d_1\rangle} \oplus \cdots \oplus \frac{D}{\langle d_t\rangle}$.
La somma delle decomposizioni primarie degli addendi $\frac{D}{\langle d_i\rangle}$, $i \leq t$, *si dice la* decomposizione primaria *di* T. *L'unione dei loro divisori elementari, considerati con le rispettive molteplicità, si dicono i* divisori elementari *di* T.

(4.10) Esempio *Sia* $T = \frac{Z}{\langle 6\rangle} \oplus \frac{Z}{\langle 12\rangle} \oplus \frac{Z}{\langle 120\rangle}$.
La decomposizione primaria di T *è*

$$\frac{Z}{\langle 2\rangle} \oplus \frac{Z}{\langle 3\rangle} \oplus \frac{Z}{\langle 4\rangle} \oplus \frac{Z}{\langle 3\rangle} \oplus \frac{Z}{\langle 8\rangle} \oplus \frac{Z}{\langle 3\rangle} \oplus \frac{Z}{\langle 5\rangle}.$$

I divisori elementari sono 2, 3, 4, 3, 8, 3, 5.

due D*-moduli non nulli, finitamente generati e di torsione, sono isomorfi se e solo se hanno gli stessi divisori elementari.*

Riassumendo quanto visto:

• *Due* D*-moduli non nulli, finitamente generati, sono isomorfi se e solo se hanno la stessa forma normale o, equivalentemente, la stessa sequenza di fattori invarianti (a meno di elementi unitari).*

• *Due* D*-moduli non nulli, finitamente generati, di torsione sono isomorfi se e solo se hanno la stessa decomposizione primaria (a meno di permutazioni degli addendi) o, equivalentemente, gli stessi divisori elementari (a meno di elementi unitari), contati con le relative molteplicità .*

5 Esercizi

(5.1) Esercizio *Si dimostri che gli unici ideali di un campo* $\mathbb{K}$ *sono* $\{0_{\mathbb{K}}\}$ *e* $\mathbb{K}$.

(5.2) Esercizio *Si dimostri che* $\mathbb{K}[x]$ *è un dominio a ideali principali.*

(5.3) Esercizio *Nell'anello* $\mathbb{Z}$*, si dimostri che*

$$\langle 3\rangle = \langle z\rangle \quad \Leftrightarrow \quad z = \pm 3.$$

(5.4) Esercizio *Nell'anello* $\mathbb{Q}[x]$*, si dimostri che*

$$\langle x^2-1\rangle = \langle f(x)\rangle \quad \Leftrightarrow \quad f(x) = q(x^2-1),\ 0 \neq q \in \mathbb{Q}.$$

(5.5) Esercizio *Sia* $M =$ *un* D*-modulo. Si dimostri che:*
1) *se* N *è immagine epimorfa di* M *allora* $\mathrm{d}(N) \leq \mathrm{d}(M)$*;*
2) *se* $M = M_1 + M_2$ *allora* $\mathrm{d}(M) \leq \mathrm{d}(M_1) + \mathrm{d}(M_2)$.

(5.6) Esercizio *Siano* $d_1, d_2 \in D$*. Si dimostri che*

$$\langle d_1\rangle \geq \langle d_2\rangle \quad \Leftrightarrow \quad d_1 | d_2.$$

(5.7) Esercizio *Si calcolino gli annullatori dei seguenti* $\mathbb{Z}$*-moduli:*

$$\mathbb{Z}, \quad \frac{\mathbb{Z}}{\langle 2\rangle}, \quad \frac{\mathbb{Z}}{\langle 5\rangle}, \quad \frac{\mathbb{Z}}{\langle 2\rangle} \oplus \frac{\mathbb{Z}}{\langle 5\rangle}, \quad \frac{\mathbb{Z}}{\langle 6\rangle} \oplus \frac{\mathbb{Z}}{\langle 9\rangle}.$$

(5.8) Esercizio *Sia* $M = M_1 + M_2$*. Si dimostri che* $\mathrm{Ann}\,(M) = \mathrm{Ann}\,(M_1) \cap \mathrm{Ann}\,(M_2)$.

(5.9) Esercizio *Si dimostri che l'applicazione* $f : \mathbb{Z} \to \mathbb{Z}_2 \oplus \mathbb{Z}_5$ *tale che* $z \mapsto \begin{pmatrix} [z]_2 \\ [z]_5 \end{pmatrix}$ *è un epimorfismo di* $\mathbb{Z}$*-moduli. Per ciascun elemento del codominio, si indichi una preimmagine in* $\mathbb{Z}$*. Si determini* $\mathrm{Ker}\ f$.

(5.10) Esercizio *Si dica se l'applicazione* $f : \mathbb{Z} \to \mathbb{Z}_2 \oplus \mathbb{Z}_4$ *tale che*

$$z \mapsto \begin{pmatrix} [z]_2 \\ [z]_4 \end{pmatrix}$$

è un omorfismo di $\mathbb{Z}$*-moduli, e se è suriettiva.*

(5.11) Esercizio *Si dimostri che l'applicazione* $f : \mathbb{Q}[x] \to \frac{\mathbb{Q}[x]}{\langle x^2+2\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x^3+1\rangle}$ *tale che*

$$f(x) \mapsto \begin{pmatrix} \langle x^2+2\rangle + f(x) \\ \langle x^3+1\rangle + f(x) \end{pmatrix}$$

è un epimorfismo di $\mathbb{Q}[x]$*-moduli. Si indichi una preimmagine di*

$$\begin{pmatrix} \langle x^2+2\rangle + x + 4 \\ \langle x+1\rangle + x^2 \end{pmatrix}$$

in $\mathbb{Q}[x]$*. Si determini* $\operatorname{Ker} f$*.*

(5.12) Esercizio *Si dica se l'applicazione* $f : \mathbb{Q}[x] \to \frac{\mathbb{Q}[x]}{\langle x^2-1\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x-1\rangle}$ *tale che*

$$f(x) \mapsto \begin{pmatrix} \langle x^2-1\rangle + f(x) \\ \langle x-1\rangle + f(x) \end{pmatrix}$$

è un epimorfismo di $\mathbb{Q}[x]$*-moduli e se è suriettiva.*

(5.13) Esercizio *Per i seguenti* $\mathbb{Q}[x]$*-moduli si dia un insieme di generatori minimale come* $\mathbb{Q}[x]$*-modulo e un insieme di generatori minimale come* $\mathbb{Q}$*-modulo:*

$$M = \frac{\mathbb{Q}[x]}{\langle x+4\rangle}\ , \quad N = \frac{\mathbb{Q}[x]}{\langle x^3+2x-1\rangle}.$$

Si dimostri che M *e* N*, come* $\mathbb{Q}[x]$*-moduli, non hanno base.*

(5.14) Esercizio *Sia* I *l'deale di* $\mathbb{K}[x]$ *generato dal polinomio* $d(x)$*, di grado* $n > 0$*. Si provi che ad ogni laterale di* I *appartiene un unico polinomio* $r(x)$ *di grado* $\leq n-1$*.*

(5.15) Esercizio *Si determini una base del* $\mathbb{Q}$*-modulo:*

$$\frac{\mathbb{Q}[x]}{\langle x+4\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x^3+2x-1\rangle}.$$

(5.16) Esercizio *Si determinino l'ordine, i divisori elementari, la decomposizione primaria, la forma normale, i fattori invarianti, l'annullatore, il minimo numero di generatori dei seguenti gruppi abeliani:*

$$\mathbb{Z}_{20} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}_{50}, \quad \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{27}.$$

(5.17) Esercizio *Si determinino i gruppi abeliani non isomorfi di ordine* 5^4*.*

(5.18) Esercizio *Si determini la decomposizione primaria del* $\mathbb{C}[x]$*-modulo:*

$$V = \frac{\mathbb{C}[x]}{\langle x^4+16\rangle}.$$

Si calcoli una base di V come $\mathbb{C}$-modulo.

(5.19) Esercizio *Si determinino i divisori elementari, la decomposizione primaria, la forma normale, i fattori invarianti, l'annullatore, il minimo numero di generatori del seguente $\mathbb{C}[x]$-modulo:*

$$V = \frac{\mathbb{C}[x]}{\langle x^4 - 16 \rangle} \oplus \frac{\mathbb{C}[x]}{\langle x^4 + 4x^2 \rangle}.$$

Si calcoli una base di V come $\mathbb{C}$-modulo.

Capitolo IV

Forme canoniche delle matrici

1 La relazione di coniugio

Sia $\mathbb{K}$ un campo. Il gruppo delle matrici invertibili di $\mathrm{Mat}_n(\mathbb{K})$ si indica con $\mathrm{GL}_n(\mathbb{K})$.

(1.1) Definizione *Date $A, B \in \mathrm{Mat}_n(\mathbb{K})$, diciamo che B è* coniugata *ad A se esiste una matrice $P \in \mathrm{GL}_n(\mathbb{K})$ tale che $B = P^{-1}AP$.*

La relazione di coniugio fra matrici è di equivalenza. Le corrispondenti classi di equivalenza si dicono *classi di coniugio*. Scopo di questo capitolo è individuare, in ogni classe di coniugio, una matrice atta a rappresentarla in modo canonico.
Il significato geometrico del coniugio fra matrici (che é un caso particolare di equivalenza) si ottiene dal Lemma 4.2 del Capitolo II, ponendo $V = W$, $\mathcal{B} = \mathcal{C}$, $\mathcal{B}' = \mathcal{C}'$, $Q = P$. Precisamente:

(1.2) Lemma *Siano $A, B \in \mathrm{Mat}_n(\mathbb{K})$. Fissata una base $\mathcal{B}$ di V, sia $\alpha : V \to W$ l' R-omomorfismo indotto da A rispetto a $\mathcal{B}$. Allora B é coniugata ad A se e solo α é l'omomorfismo indotto da B rispetto ad un'altra base $\mathcal{B}'$ di V.*

2 $\mathbb{K}[x]$-moduli

Consideriamo l'anello $\mathbb{K}[x]$ dei polinomi nella indeterminata x a coefficienti nel campo $\mathbb{K}$. Poiché $\mathbb{K} = \mathbb{K}x^0$ è un sottoanello di $\mathbb{K}[x]$, ogni $\mathbb{K}[x]$-modulo V è, a maggior ragione, un $\mathbb{K}$-modulo, ossia uno spazio vettoriale su $\mathbb{K}$. Inoltre, se W é un $\mathbb{K}[x]$ modulo, ogni $\mathbb{K}[x]$-omomorfismo da V a W è una applicazione $\mathbb{K}$-lineare.
In particolare, per il Lemma 3.5 del Capitolo I, la applicazione

$$\mu_x : V \to V \quad \text{tale che} \quad v \mapsto xv, \quad \forall\, v \in V$$

è un $\mathbb{K}[x]$-omomorfismo.

(2.1) Lemma *Siano V, W due $\mathbb{K}[x]$-moduli. Una applicazione $\mathbb{K}$-lineare $\varphi : V \to W$ è un $\mathbb{K}[x]$-omomorfismo se e solo se, per ogni $v \in V$, $\varphi(xv) = x\varphi(v)$*

Dimostrazione. La condizione è necessaria per definizione di $\mathbb{K}[x]$-omomorfismo. Viceversa, supponiamo $\varphi(xv) = x\varphi(v)$, per ogni $v \in V$, e verifichiamo innanzitutto che $\varphi(x^i v) = x^i \varphi(v)$ per ogni $i \geq 0$. Per $i = 0$, il polinomio $x^0 = 1_{\mathbb{K}} x^0$ è l'unità di $\mathbb{K}[x]$: quindi l'uguaglianza segue per definizione di $\mathbb{K}[x]$-modulo. Per $i > 0$, si ha:

$$\varphi(x^i v) = \varphi\left(x\left(x^{i-1}v\right)\right) = x\varphi\left(x^{i-1}v\right) = xx^{i-1}\varphi(v) = x^i\varphi(v).$$

Sia ora $f(x) = \sum_0^n k_i x^i$. Per la $\mathbb{K}$-linearità di φ e quanto appena dimostrato:

$$\varphi(f(x)v) = \varphi\left(\sum_0^n k_i\left(x^i v\right)\right) = \sum_0^n k_i\varphi\left(x^i v\right) = \sum_0^n k_i x^i \varphi\left(v\right) = f(x)\varphi(v).$$

■

Fissata $A \in \mathrm{Mat}_n(\mathbb{K})$, per ogni polinomio $f(x) = k_0 x^0 + \cdots + k_m x^m \in \mathbb{K}[x]$ poniamo

$$f(A) := k_0 A^0 + \cdots + k_m A^m \ .$$

(2.2) Esempio $A = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$, $f(x) = -x^0 + 7x^2 + x^3$:

$$f(A) = -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + 7\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} + \begin{pmatrix} 0 & 4 \\ 2 & 0 \end{pmatrix} \quad = \begin{pmatrix} 13 & 4 \\ 2 & 13 \end{pmatrix} \ .$$

Si verifica facilmente che l'applicazione $\varphi_A : \mathbb{K}[x] \to \mathrm{Mat}_n(\mathbb{K})$ tale che

$$\varphi_A\left(f(x)\right) := f(A), \quad \forall\ f(x) \in \mathbb{K}[x]$$

è un omomorfismo di anelli. Chiaramente il gruppo additivo $\mathbb{K}^n$ è un modulo sull'anello $\mathrm{Mat}_n(\mathbb{K})$, rispetto al prodotto di matrici. Per il Lemma 1.2 del Capitolo 1, $\mathbb{K}^n$ risulta $\mathbb{K}[x]$-modulo rispetto al prodotto indotto da φ_A, ossia:

$$f(x)\begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} := f(A)\begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix}. \tag{2.3}$$

In particolare, per $f(x) = x$, si ha

$$xv := Av, \quad \forall\ v \in \mathbb{K}^n. \tag{2.4}$$

(2.5) Definizione *Indichiamo con ${}_A\mathbb{K}^n$ il $\mathbb{K}[x]$-modulo definito da* (2.3).

${}_A\mathbb{K}^n$ é caratterizzato, come $\mathbb{K}[x]$ modulo, dalla condizione $\mu_x = \mu_A$ derivante da (2.4).

(2.6) Teorema *Sia V un $\mathbb{K}[x]$-modulo, di dimensione n su $\mathbb{K}$, e sia $A \in \mathrm{Mat}_n(\mathbb{K})$. Allora $V \simeq {}_A\mathbb{K}^n$ se e solo se A è la matrice di $\mu_x : V \to V$ rispetto una base $\mathcal{B}$ di V.*

Dimostrazione. A sia la matrice di μ_x rispetto $\mathcal{B}$. Abbiamo allora:

$$Av_{\mathcal{B}} = (\mu_x(v))_{\mathcal{B}} = (xv)_{\mathcal{B}}, \quad \forall\ v \in V.$$

L'applicazione $\eta^{-1} : V \to \mathbb{K}^n$ tale che $\eta^{-1}(v) = v_{\mathcal{B}}$ è un isomorfismo di $\mathbb{K}$-moduli.
Inoltre da:

$$\eta^{-1}(xv) = (xv)_{\mathcal{B}} = Av_{\mathcal{B}} = x\, v_{\mathcal{B}} = x\, \eta^{-1}(v)$$

segue che η^{-1} è un isomorfismo di $\mathbb{K}[x]$-moduli, per il Lemma 2.1. Quindi $V \simeq_A \mathbb{K}^n$.
Viceversa, supponiamo $V \simeq {}_A\mathbb{K}^n$ e sia $\gamma : V \to {}_A\mathbb{K}^n$ un $\mathbb{K}[x]$-isomorfismo. Poniamo $\mathcal{B} = \{v_1, \ldots, v_n\}$ dove i v_i sono le preimmagini dei vettori e_i della base canonica di $\mathbb{K}^n$. Da $\gamma(v_i) = e_i$, segue che $\gamma(v) = v_{\mathcal{B}}$, per ogni $v \in V$. Poichè γ è un $\mathbb{K}[x]$-omomorfismo si ha $\gamma(xv) = x\gamma(v)$, ossia $(\mu_x(v))_{\mathcal{B}} = Av_{\mathcal{B}}$. Quindi A è la matrice di μ_x rispetto a $\mathcal{B}$. ■

(2.7) Corollario *Siano $A, B \in \mathrm{Mat}_n(\mathbb{K})$. La matrice B è coniugata ad A se e solo se*

$${}_B\mathbb{K}^n \simeq {}_A\mathbb{K}^n.$$

Dimostrazione. Consideriamo il $\mathbb{K}[x]$-modulo $V := {}_A\mathbb{K}^n$. L' applicazione lineare indotta da A rispetto alla base canonica $\mathcal{B}$ di $\mathbb{K}^n$ é $\mu_A = \mu_x$. Per il Lemma 1.2, la matrice B é coniugata ad A se e solo se μ_x ha matrice B rispetto una base $\mathcal{B}'$ di $\mathbb{K}^n$. Per il Teorema precedente, μ_x ha matrice B rispetto $\mathcal{B}'$ se e solo se $V \simeq {}_B\mathbb{K}^n$. ■

(2.8) Teorema *Data $A \in \mathrm{Mat}_n(\mathbb{K})$, esiste una sequenza di polinomi monici non costanti $d_1(x), \cdots, d_t(x)$ di $\mathbb{K}[x]$, ciascuno dei quali divide il successivo, tali che:*

$$ {}_A\mathbb{K}^n \quad \simeq \quad \frac{\mathbb{K}[x]}{\langle d_1(x)\rangle} \oplus \cdots \oplus \frac{\mathbb{K}[x]}{\langle d_t(x)\rangle}. \tag{2.9}$$

Dimostrazione.
Essendo $\mathbb{K}[x]$ un dominio a ideali principali, basta dimostrare che ${}_A\mathbb{K}^n$ è un $\mathbb{K}[x]$-modulo finitamente generato, di torsione, e applicare il Teorema 3.2 del Capitolo III.

$\mathbb{K}^n$ è generato da n elementi come $\mathbb{K}$-modulo. Quindi è finitamente generato come $\mathbb{K}$-modulo e, a maggior ragione, come $\mathbb{K}[x]$-modulo. Resta da vedere che, per ogni $v \in \mathbb{K}^n$, esiste un polinomio non nullo $f(x) \in \mathbb{K}[x]$ tale che $f(x)v = 0_{\mathbb{K}^n}$. Ciò è evidente se $A^i v = A^j v$ per qualche $i \neq j$, non negativi. Basta infatti porre $f(x) = x^i - x^j$. Altrimenti il sottoinsieme $\{v,\ Av,\ \cdots,\ A^n v\}$ di $\mathbb{K}^n$ ha cardinalità $n+1$ ed è quindi dipendente. Detti $k_0, \cdots, k_n$ degli scalari non tutti nulli tali che $k_0 v + k_1 Av + \cdots k_n A^n v = 0_{\mathbb{K}^n}$, poniamo $f(x) = k_0 + k_1 x + \cdots + k_n x^n$. ■

(2.10) Definizione *La sequenza dei fattori invarianti del $\mathbb{K}[x]$-modulo ${}_A\mathbb{K}^n$ si dice la sequenza degli* invarianti di similarità *di A. L'ultimo elemento della sequenza (i.e., il minimo comune multiplo dei suoi elementi) si dice il* polinomio minimo *di A.*

(2.11) Lemma *Il polinomio minimo di A é il generatore dell'ideale* $\operatorname{Ker}\varphi_A$.

Dimostrazione. Si ha $f(A) = 0_{\mathrm{Mat}_n(\mathbb{K})}$ se e solo se $f(A)v = 0_{\mathbb{K}^n}$ per ogni $v \in \mathbb{K}^n$. Pertanto $\operatorname{Ker}\varphi_A$ coincide con l'annullatore di ${}_A\mathbb{K}^n$. Per il Teorema 3.2 del Capitolo 3, tale annullatore é l'ideale generato dall' ultimo dei fattori invarianti, ossia dal polinomio minimo di A. ■

Nelle notazioni di (2.9), la sequenza degli invarianti di similarità di A é

$$d_1(x),\ \cdots,\ d_t(x).$$

Il polinomio minimo di A é $d_t(x)$. Per il Lemma 2.11, per ogni $f(x) \in \mathbb{K}[x]$ si ha $f(A) = 0_{\mathrm{Mat}_n(\mathbb{K})}$ se e solo se $d_t(x)$ divide $f(x)$. In particolare

$$d_t(A) = 0_{\mathrm{Mat}_n(\mathbb{K})}.$$

Poichè moduli isomorfi hanno lo stesso annullatore, matrici coniugate hanno lo stesso polinomio minimo.

3 Forme canoniche razionali

(3.1) Definizione *Sia $d(x) = k_0 + k_1 x + k_2 x^2 \cdots + k_{s-1}x^{s-1} + x^s \in \mathbb{K}[x]$. La matrice*

$$C_{d(x)} := \begin{pmatrix} 0 & 0 & \cdots & -k_0 \\ 1 & 0 & \cdots & -k_1 \\ 0 & 1 & \cdots & -k_2 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 1 & -k_{s-1} \end{pmatrix} \in \mathrm{Mat}_s(\mathbb{K}) \tag{3.2}$$

è detta la matrice companion *del polinomio* $d(x)$.

(3.3) Esempio $d(x) = 3 - 6x + 2x^3 + x^4, \quad C_{d(x)} := \begin{pmatrix} 0 & 0 & 0 & -3 \\ 1 & 0 & 0 & 6 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -2 \end{pmatrix}.$

(3.4) Teorema *Fissato* $d(x)$ *monico, di grado* s*, consideriamo il* $\mathbb{K}[x]$*-modulo*

$$V = \frac{K[x]}{\langle d(x) \rangle}.$$

1) $\mathcal{B} := \left\{ \langle d(x) \rangle + x^0,\ \langle d(x) \rangle + x,\ \cdots,\ \langle d(x) \rangle + x^{s-1} \right\}$ *è una base di* V *su* $\mathbb{K}$*;*

2) *la matrice di* μ_x *rispetto a* $\mathcal{B}$ *è la matrice companion* $C_{d(x)}$ *del polinomio* $d(x)$.

Dimostrazione. Poniamo $I = \langle d(x) \rangle$.

1) $\mathcal{B}$ genera V come $\mathbb{K}$-modulo. Infatti, dato $I + f(x) \in V$, si ha:

$$f(x) = q(x)d(x) + r_0 + r_1 x + \cdots + r_{s-1}x^{s-1}$$

da cui $I + f(x) = I + r_0 x^0 + r_1 x + \cdots + r_{s-1}x^{s-1} =$

$$r_0 \left(I + x^0\right) + r_1 \left(I + x\right) + \cdots + r_{s-1} \left(I + x^{s-1}\right). \tag{3.5}$$

Vediamo che $\mathcal{B}$ è indipendente. Una combinazione lineare del tipo (3.5) è uguale al laterale $I + 0_{\mathbb{K}[x]}$ solo se il polinomio $r(x) = r_0 x^0 + \cdots + r_{s-1}x^{s-1}$ appartiene a I. Poichè gli elementi non nulli di I hanno grado $\geq s$, deve essere $r(x) = 0_{\mathbb{K}[x]}$, ossia $r_0 = r_1 = \cdots = r_{s-1} = 0_{\mathbb{K}}$.

2) Se $0 \leq i \leq s-2$ si ha

$$\mu_x(I + x^i) = x(I + x^i) = I + x^{i+1}.$$

Se $i = s - 1$ si ha $\mu_x \left(I + x^{s-1}\right) =$

$$I + x^s = I - d(x) + x^s = -k_0 \left(I + x^0\right) - k_1 \left(I + x\right) + \cdots - k_{s-1} \left(I + x^{s-1}\right).$$

■

(3.6) Corollario *Consideriamo il* $\mathbb{K}[x]$*-modulo*

$$V := \frac{\mathbb{K}[x]}{\langle d_1(x) \rangle} \oplus \cdots \oplus \frac{\mathbb{K}[x]}{\langle d_t(x) \rangle}.$$

Esiste una base $\mathcal{B}$ di V tale che la matrice di $\mu_x : V \to V$ rispetto a $\mathcal{B}$ è :

$$C = \begin{pmatrix} C_{d_1(x)} & & \\ & \dots & \\ & & C_{d_t(x)} \end{pmatrix} . \tag{3.7}$$

Dimostrazione. Per $t = 1$, l'enunciato è vero per il punto 2) del Teorema 3.4.
Se $t > 1$, indicando con π la proiezione sulle prime $t-1$ componenti, abbiamo:

$$\text{Ker } \pi_t \sim \frac{\mathbb{K}[x]}{\langle d_1(x)\rangle} \oplus \cdots \oplus \frac{\mathbb{K}[x]}{\langle d_{t-1}(x)\rangle}, \qquad \text{Ker } \pi \sim \frac{\mathbb{K}[x]}{\langle d_t(x)\rangle}.$$

Per induzione, esiste una base $\mathcal{B}_1$ di Ker π_t tale che la μ_x ha matrice

$$\begin{pmatrix} C_{d_1(x)} & & \\ & \dots & \\ & & C_{d_{t-1}(x)} \end{pmatrix}.$$

Per il Teorema 3.4 esiste una base $\mathcal{B}_2$ di Ker π rispetto alla quale la μ_x ha matrice $C_{d_t(x)}$. Essendo $V = \text{Ker } \pi_t \dot{+} \text{Ker } \pi$, si conclude che $\mathcal{B} = \mathcal{B}_1 \cup \mathcal{B}_2$ è una base di V e che la μ_x ha matrice C rispetto a $\mathcal{B}$. (si veda il Teorema 2.7 del Capitolo II). ■

(3.8) Definizione *Una* forma canonica razionale *è una matrice diagonale a blocchi*

$$C = \begin{pmatrix} C_{d_1(x)} & & \\ & \dots & \\ & & C_{d_t(x)} \end{pmatrix} = \text{blockdiag}\left(C_{d_1(x)},\ \cdots,\ C_{d_t(x)}\right) \tag{3.9}$$

dove $d_i(x)$ divide $d_{i+1}(x)$ per $i \leq t-1$.

(3.10) Teorema *Ogni matrice $A \in \text{Mat}_n(\mathbb{K})$ è coniugata ad una e una sola forma canonica razionale.*

Dimostrazione. Detta $d_1(x),\ \cdots,\ d_t(x)$ la sequenza dei fattori invarianti di ${}_A\mathbb{K}^n$, consideriamo la forma canonica razionale C definita da (3.9). Per il Corollario 3.6 esiste una base di ${}_A\mathbb{K}^n$ rispetto alla quale μ_x ha matrice C. Dal Teorema 2.6 segue ${}_A\mathbb{K}^n \sim_C \mathbb{K}^n$ e dal Corollario 2.7 segue A coniugata a C. Infine, se A fosse coniugata ad un' altra forma canonica razionale

$$B = \text{blockdiag}\left(C_{c_1(x)},\ \cdots,\ C_{c_h(x)}\right)$$

si avrebbe ${}_C\mathbb{K}^n \simeq_B \mathbb{K}^n$, ossia:

$$\frac{\mathbb{K}[x]}{\langle d_1(x)\rangle} \oplus \cdots \oplus \frac{\mathbb{K}[x]}{\langle d_t(x)\rangle} \quad \simeq \quad \frac{\mathbb{K}[x]}{\langle c_1(x)\rangle} \oplus \cdots \oplus \frac{\mathbb{K}[x]}{\langle c_h(x)\rangle}.$$

Per il Corollario 4.2 del Capitolo III, deve essere $t = h$, $d_i(x) = c_i(x)$ per ogni $i \leq t$. Concludiamo che $C = B$. ■

(3.11) Definizione *Se A ha sequenza di invarianti di similarità $d_1(x), \cdots, d_t(x)$, la matrice $C = \text{blockdiag}\left(C_{d_1(x)}, \cdots, C_{d_t(x)}\right)$ si dice la* forma canonica razionale *di A.*

Possiamo così riassumere le considerazioni precedenti.

Due matrici $A, B \in \text{Mat}_n(\mathbb{K})$ sono coniugate se e solo se:

- *hanno la stessa forma canonica razionale o, equivalentemente,*
- *hanno gli stessi invarianti di similarità.*

(3.12) Esempio

Le forme canoniche razionali di $\text{Mat}_2(\mathbb{K})$ sono dei tipi:

a) $t = 2$, $d_1(x) = d_2(x) = x - k$,

$$\begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}$$

b) $t = 1$, $d_1(x) = x^2 + k_1x + k_0$,

$$\begin{pmatrix} 0 & -k_0 \\ 1 & -k_1 \end{pmatrix}.$$

(3.13) Esempio *Le forme canoniche razionali di $\text{Mat}_3(\mathbb{K})$ sono dei tipi:*

a) $t = 3$, $d_1(x) = d_2(x) = d_3(x) = x - k$,

$$\begin{pmatrix} k & 0 & 0 \\ 0 & k & 0 \\ 0 & 0 & k \end{pmatrix}$$

b) $t = 2$, $d_1(x) = x - k$, $d_2(x) = (x - h)(x - k)$,

$$\begin{pmatrix} k & 0 & 0 \\ 0 & 0 & -kh \\ 0 & 1 & k + h \end{pmatrix}.$$

b) $t = 1$, $d_1(x) = x^3 + k_2x^2 + k_1x + k_0$,

$$\begin{pmatrix} 0 & 0 & -k_0 \\ 1 & 0 & -k_1 \\ 0 & 1 & -k_2 \end{pmatrix}.$$

4 Il polinomio caratteristico

Se $A \in \mathrm{Mat}_n(\mathbb{K})$, gli elementi di $(xI - A)$ appartengono all'anello $\mathbb{K}[x]$, ossia

$$(xI - A) \in \mathrm{Mat}_n(\mathbb{K}[x]).$$

(4.1) Definizione *Il determinante della matrice $xI - A$ si dice il* polinomio caratteristico *di A.*

(4.2) Lemma *Matrici coniugate hanno lo stesso polinomio caratteristico.*

Dimostrazione. Se $A = P^{-1}BP$, si ha:

$$xI - A \;=\; xI - P^{-1}BP \;=\; P^{-1}xIP - P^{-1}BP \;=\; P^{-1}(xI - B)P.$$

Ne segue $\det(xI - A) = (\det(P))^{-1}\det(xI - B)\det(P) = \det(xI - B)$. ∎

(4.3) Teorema $C = \mathrm{blockdiag}\left(C_{d_1(x)},\ \cdots,\ C_{d_t(x)}\right)$ *ha polinomio caratteristico* $\prod_1^t d_i(x)$.

Dimostrazione. Cominciamo a dimostrare che il polinomio caratteristico di una matrice companion $C_{d(x)}$ è $d(x)$, ragionando per induzione sul grado s di $d(x)$.
Se $s = 1$ si ha $d(x) = k_0 + x$, $C_{d(x)} = (-k_0)$, $\det(x - C_{d(x)}) = x + k_0 = d(x)$.
Se $s > 1$, detto $e(x) := k_1 + k_2x + \cdots + x^{s-1}$ il quoziente della divisione di $d(x)$ per x, si ha:

$$C_{d(x)} = \begin{pmatrix} 0 & 0 & \dots & -k_0 \\ 1 & & & \\ \dots & & C_{e(x)} & \\ 0 & & & \end{pmatrix}, \qquad xI - C_{d(x)} = \begin{pmatrix} x & 0 & \dots & k_0 \\ -1 & & & \\ \dots & & xI - C_{e(x)} & \\ 0 & & & \end{pmatrix}.$$

Sviluppando il determinante di $xI - C_{d(x)}$ secondo la prima riga, e applicando l'ipotesi induttiva, si ha: $\det\left(xI - C_{d(x)}\right) = xe(x) + (-1)^{s+1}(-1)^{s-1}k_0 = d(x)$.
La tesi si ottiene applicando il precedente risultato ai singoli blocchi di C. Infatti:

$$\det(xI - C) = \prod_{i=1}^{t} \det(xI - C_{d_i(x)}) = \prod_{i=1}^{t} d_i(x).$$

∎

(4.4) Corollario *Il polinomio caratteristico di una matrice è il prodotto dei suoi invarianti di similarità.*

Dimostrazione. Siano $d_1(x), \cdots, d_t(x)$ gli invarianti di similarità di A. Essendo A coniugata a $C = \text{blockdiag}\left(C_{d_1(x)}, \cdots, C_{d_t(x)}\right)$, si conclude che il polinomio caratteristico di A è uguale a quello di C, ossia $\prod_1^t d_i(x)$. ■

(4.5) Teorema (di Hamilton Cayley). *Ogni matrice annulla il proprio polinomio caratteristico.*

Dimostrazione. Sia $A \in \text{Mat}_n(\mathbb{K})$. Nelle notazioni del precedente Corollario si ha $\det(xI - A) = \prod_{i=1}^t d_i(x)$, dove $d_t(x)$ è il polinomio minimo di A. Ne segue $d_t(A) = 0_{\text{Mat}_n(\mathbb{K})}$ per il Lemma 2.11. A maggior ragione $\prod_{i=1}^t d_i(A) = 0_{\text{Mat}_n(\mathbb{K})}$. ■

Per il calcolo degli invarianti di similarità di una matrice, può essere utile il seguente:

(4.6) Teorema *Gli invarianti di similarità di $A \in \text{Mat}_n(\mathbb{K})$ sono i fattori invarianti non unitari di $(xI - A)$ in $\text{Mat}_n(\mathbb{K}[x])$.*

Dimostrazione. Osserviamo preliminarmente che, se $d(x)$ è un polinomio monico di grado s, la forma normale di $\left(xI_s - C_{d(x)}\right)$ in $\text{Mat}_s(\mathbb{K}[x])$ è

$$\begin{pmatrix} I_{s-1} & 0 \\ 0 & d(x) \end{pmatrix}. \tag{4.7}$$

Infatti $\left(xI_s - C_{d(x)}\right)$ è equivalente alla matrice

$$\begin{pmatrix} I_{s-1} & & & 0 \\ x & x^2 & \dots x^{s-1} & 1 \end{pmatrix} \begin{pmatrix} 0 & & I_{s-1} \\ 1 & & 0 \end{pmatrix} \left(xI_s - C_{d(x)}\right) := T.$$

Poichè T è triangolare superiore, con $-1, -1, \dots, -1, d(x)$ sulla diagonale principale, si verifica facilmente che T è equivalente a 4.7.

Supponiamo ora che A abbia forma canonica razionale $C = \text{blockdiag}\left(C_{d_1(x)}, \cdots, C_{d_t(x)}\right)$. Da $C = P^{-1}AP$ segue $xI - C = P^{-1}(xI - A)P$. Quindi $xI - A$ e $xI - C$ sono equivalenti in $\text{Mat}_n(\mathbb{K}[x])$, e hanno così gli stessi fattori invarianti. Da quanto osservato nella prima parte della dimostrazione si deduce che $d_1(x), \dots, d_t(x)$ sono i fattori invarianti non unitari di $xI - C$. ■

5 La forma canonica di Jordan

In questo paragrafo supporremo $\mathbb{K}$ algebricamente chiuso.

(5.1) Lemma *Sia $A \in \mathrm{Mat}_n(\mathbb{K})$ e sia $V = \mathbb{K}^n$. Per ogni $\lambda \in \mathbb{K}$, L'insieme*

$$V_\lambda := \{v \in V \mid Av = \lambda v\}$$

è un sottospazio di V.

Dimostrazione. $A0_V = 0_V = \lambda 0_V$, quindi $0_V \in V_\lambda$.
Per ogni $v_1, v_2, v \in V_\lambda$ e per ogni $\mu \in \mathbb{K}$ si ha:
$A(v_1 + v_2) = Av_1 + Av_2 = \lambda v_1 + \lambda v_2 = \lambda(v_1 + v_2)$,
$A(\mu v) = \mu(Av) = \mu(\lambda v) = \lambda(\mu v)$.
Si conclude che $v_1 + v_2 \in V_\lambda$ e che $\mu v \in V_\lambda$. ■

(5.2) Definizione *Nelle notazioni del precedente Lemma, se $V_\lambda \neq \{0_V\}$ si dice che λ è un* autovalore *di A e che V_λ è il relativo* autospazio.

I valori λ per i quali $V_\lambda \neq \{0_V\}$ sono in numero finito. Infatti:

(5.3) Lemma *Gli autovalori di A sono le radici del polinomio caratteristico di A.*

Dimostrazione. Per ogni $\lambda \in \mathbb{K}$, il sistema lineare omogeneo

$$(A - \lambda I) \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} = \begin{pmatrix} 0_{\mathbb{K}} \\ \dots \\ 0_{\mathbb{K}} \end{pmatrix}$$

ha soluzioni non nulle se e solo se $\det(A - \lambda I) = 0_{\mathbb{K}}$, se e solo se λ è radice del polinomio $\det(A - xI) = (-1)^n \det(xI - A)$. ■

(5.4) Definizione *Per ogni $\lambda \in \mathbb{K}$ e per ogni intero $s \geq 0$ definiamo induttivamente il* blocco di Jordan *$J(s, \lambda)$ ponendo: $J(0, \lambda) := \emptyset$ e, per $s > 0$:*

$$J(s, \lambda) := \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 1 & & & \\ 0 & & & \\ \cdots & & J(s-1, \lambda) & \\ 0 & & & \end{pmatrix}. \tag{5.5}$$

Così, ad esempio:

$$J(1,\lambda) = (\lambda), \quad J(2,\lambda) = \begin{pmatrix} \lambda & 0 \\ 1 & \lambda \end{pmatrix}, \quad J(3,\lambda) = \begin{pmatrix} \lambda & 0 & 0 \\ 1 & \lambda & 0 \\ 0 & 1 & \lambda \end{pmatrix}.$$

(5.6) Lemma *Il blocco di Jordan $J(s,\lambda)$ ha λ come unico autovalore. Il corrispondente autospazio in $\mathbb{K}^s$ è $\langle e_s \rangle$ e ha quindi dimensione* 1.

Dimostrazione. Un calcolo diretto. ■

(5.7) Lemma *Esiste una base di $V := \frac{\mathbb{K}[x]}{\langle (x-\lambda)^s \rangle}$ rispetto alla quale la $\mu_x : V \to V$ ha matrice il blocco di Jordan $J(s,\lambda)$. Ne segue che $J(s,\lambda)$ è coniugata alla matrice companion $C_{(x-\lambda)^s}$ del polinomio $(x-\lambda)^s$.*

Dimostrazione. V ha dimensione $s = \deg((x-\lambda)^s)$.
Posto $I := \langle (x-\lambda)^s \rangle$, si verifica facilmente che il sottoinsieme

$$\mathcal{B}' := \left\{ I + (x-\lambda)^0, \quad I + (x-\lambda)^1, \quad \cdots, \quad I + (x-\lambda)^{s-1} \right\}$$

è indipendente, quindi una base di V per il Corollario 1.4 del Capitolo III.
Per ogni $i \geq 0$ si ha l'identità:

$$x(x-\lambda)^i = \lambda(x-\lambda)^i - \lambda(x-\lambda)^i + x(x-\lambda)^i = \lambda(x-\lambda)^i + (x-\lambda)^{i+1}.$$

Ne segue che, per $i \leq s-2$:
$\mu_x \left(I + (x-\lambda)^i \right) = I + x(x-\lambda)^i = \lambda \left(I + (x-\lambda)^i \right) \; + \; I + (x-\lambda)^{i+1}$,
$\mu_x \left(I + (x-\lambda)^{s-1} \right) = I + x(x-\lambda)^{s-1} = I + \lambda(x-\lambda)^{s-1} = \lambda \left(I + (x-\lambda)^{s-1} \right)$.
Ne segue che la matrice di μ_x, rispetto a $\mathcal{B}'$, è $J(s,\lambda)$.
D'altra parte sappiamo che la matrice di μ_x, rispetto alla base $\mathcal{B} = \left\{ I + x^0, I + x, \ldots, I + x^{s-1} \right\}$, è la matrice $C_{(x-\lambda)^s}$. Si conclude che $J(s,\lambda)$ è coniugata a $C_{(x-\lambda)^s}$. ■

(5.8) Corollario
1) *Sia $d(x) = (x-\lambda_1)^{s_1} \ldots (x-\lambda_m)^{s_m}$ dove $\lambda_i \neq \lambda_j$ per $i \neq j$.*
La matrice companion $C_{d(x)}$ è coniugata alla matrice:

$$J_{d(x)} := \begin{pmatrix} J(s_1,\lambda_1) & & \\ & \cdots & \\ & & J(s_m,\lambda_m) \end{pmatrix}. \tag{5.9}$$

2) *Ogni forma canonica razionale* $C = \begin{pmatrix} C_{d_1(x)} & & \\ & \cdots & \\ & & C_{d_t(x)} \end{pmatrix}$ *è coniugata a*

$$J = \begin{pmatrix} J_{d_1(x)} & & \\ & \cdots & \\ & & J_{d_t(x)} \end{pmatrix} \quad \text{(forma di Jordan di } C\text{)}.$$

Dimostrazione.

1) Detto s il grado di $d(x)$, per il punto 2) del Teorema 3.4 si ha:

$$C_{d(x)}\mathbb{K}^s \simeq \frac{\mathbb{K}[x]}{\langle d(x)\rangle}.$$

Dal Teorema 4.7 del Capitolo III segue:

$$\frac{\mathbb{K}[x]}{\langle d(x)\rangle} \;\simeq\; \frac{\mathbb{K}[x]}{\langle (x-\lambda_1)^{s_1}\rangle} \oplus \cdots \oplus \frac{\mathbb{K}[x]}{\langle (x-\lambda_m)^{s_m}\rangle} \;:=\; V.$$

Tenendo presente il Teorema 2.7 del Capitolo II si ha allora, per induzione su m, che esiste una base di V rispetto alla quale la $\mu_x : V \to V$ ha matrice $J_{d(x)}$. Si conclude che $J_{d(x)}$ e $C_{d(x)}$ sono coniugate.

2) Per il punto 1), per ogni $i \leq t$, posto $n_i = \deg(d_i(x))$ esiste $P_i \in \mathrm{GL}_{n_i}(\mathbb{K})$ tale che

$$P_i^{-1} C_{d_i(x)} P_i = J_{d_i(x)}.$$

La matrice diagonale a blocchi $P := \mathrm{blockdiag}\,(P_1, \cdots, P_t)$ è tale che $P^{-1}CP = J$. ∎

(5.10) Definizione *Nelle notazioni del precedente Corollario:*

1*) J è una* forma canonica di Jordan *di C;*

2*) dette $\lambda_1, \ldots, \lambda_m$ le radici distinte di $d_t(x)$, e posto:*

$$d_i(x) = (x-\lambda_1)^{s_{i_1}} \;\ldots\; (x-\lambda_m)^{s_{i_m}}, \quad 1 \leq i \leq t$$

i fattori di grado positivo fra

$$(x-\lambda_1)^{s_{1_1}},\ \cdots,\ (x-\lambda_m)^{s_{1_m}},\ \cdots,\ (x-\lambda_1)^{s_{t_1}},\ \cdots,\ (x-\lambda_m)^{s_{t_m}}$$

sono i divisori elementari *di C.*

(5.11) Esempio *La matrice $A \in \mathrm{Mat}_8(\mathbb{K})$ abbia invarianti di similarità $d_1(x) = (x-4)$, $d_2(x) = (x-3)(x-4)^2$, $d_3(x) = (x-3)(x-4)^3$. Allora i divisori elementari di A sono:*

$$(x-4),\ (x-3),\ (x-4)^2,\ (x-3),\ (x-4)^3.$$

Possiamo così riassumere le considerazioni precedenti.
Se $\mathbb{K}$ è algebricamente chiuso, due matrici di $\mathrm{Mat}_n(\mathbb{K})$ *sono coniugate se e solo se:*
• *sono coniugate a una stessa forma canonica di Jordan o, equivalentemente,*
• *hanno gli stessi divisori elementari (contati con le loro molteplicità) .*

(5.12) Lemma *Sia* $B = \mathrm{blockdiag}\,(B_1, \cdots, B_m) \in \mathrm{Mat}_n(\mathbb{K})$. *Allora B è coniugata ad ogni matrice B' ottenuta da B effettuando una qualunque permutazione π sui suoi blocchi dello stesso ordine.*

Dimostrazione. Sia $\beta : \mathbb{K}^n \to \mathbb{K}^n$ l'applicazione $v \mapsto Bv$, ossia l'applicazione lineare indotta da B rispetto alla base canonica ordinata $\mathcal{B} := \{e_1, \cdots, e_n\}$. Si vede facilmente che esiste una permutazione ρ degli e_i, dipendente da π, tale che la matrice di β rispetto alla base $\mathcal{B}' = \{e_{\rho(1)}, \cdots, e_{\rho(n)}\}$ è B'. Si conclude che B e B' sono coniugate. ■

(5.13) Definizione *Una matrice $A \in \mathrm{Mat}_n(\mathbb{K})$ si dice* diagonalizzabile *se è coniugata a una matrice diagonale.*

(5.14) Lemma *Sia $D \in \mathrm{Mat}_n(\mathbb{K})$ una matrice diagonale, e siano $\lambda_1, \cdots, \lambda_m$ gli elementi distinti della diagonale principale di D. Il polinomio minimo di D è*

$$(x - \lambda_1) \dots (x - \lambda_m).$$

Dimostrazione. D è una forma canonica di Jordan, i cui divisori elementari sono

$$x - \lambda_1, \cdots, x - \lambda_m.$$

Poichè il polinomio minimo di D è il m.c.m. dei suoi divisori elementari, si conclude l'asserto. ■

Seguono i criteri di diagonalizzazione forniti dal seguente:

(5.15) Teorema *Sia $\mathbb{K}$ algebricamente chiuso e sia $A \in Mat_n(\mathbb{K})$. Le seguenti condizioni sono equivalenti:*
1*) A è diagonalizzabile;*
2*) il polinomio minimo di A non ha radici multiple;*
3*) ogni forma canonica di Jordan J di A è diagonale;*
4*) $\mathbb{K}^n$ ha una base costituita da autovettori di A.*

Dimostrazione. Siano $d_1(x), \ldots, d_t(x)$ gli invarianti di similarità di A, ordinati in modo che ciascuno divida il successivo. In particolare $d_t(x)$ è il polinomio minimo di A.
1) $\Rightarrow$ 2). Ricordando che matrici coniugate hanno lo stesso polinomio minimo, se A è coniugata a una matrice diagonale D, allora $d_t(x)$ è anche il polinomio minimo di D. Per il Lemma precedente

$$d_t(x) = (x - \lambda_1) \cdots (x - \lambda_m)$$

con $\lambda_i \neq \lambda_j$ per $i \neq j$. Quindi $d_t(x)$ non ha radici multiple.
2) $\Rightarrow$ 3) Se $d_t(x)$ non ha radici multiple, è prodotto di fattori lineari a due a due distinti. E lo stesso fatto vale per tutti i $d_i(x)$, in quanto dividono $d_t(x)$. Ne segue che tutti i divisori elementari di J hanno grado 1 o, equivalentemente, che tutti i blocchi di J hanno ordine 1. Si conclude che J è diagonale.
3) $\Rightarrow$ 4) Se J è diagonale, i vettori della base canonica $\mathcal{B} = \{e_1, \cdots, e_n\}$ sono autovettori per J. Sia P una matrice invertibile tale che $P^{-1}AP = J$. Allora $\mathcal{B}' = \{Pe_1, \cdots, Pe_n\}$ è una base di $\mathbb{K}^n$. Inoltre la relazione:

$$APe_i = PJe_i = P\lambda_i e_i = \lambda_i e_i$$

dice che i Pe_i sono autovettori di A.
4) $\Rightarrow$ 1) Sia $\mathcal{B} = \{v_1, \cdots, v_n\}$ una base di autovettori di A e sia P la matrice le cui colonne sono i vettori $v_1, \cdots, v_n$. Ne segue $v_i = Pe_i$, $P^{-1}v_i = e_i$ da cui:

$$P^{-1}APe_i \;=\; P^{-1}Av_i \;=\; P^{-1}\lambda_i v_i \;=\; \lambda_i P^{-1}v_i = \lambda_i e_i \;.$$

Si conclude che la matrice $P^{-1}AP$ è diagonale. ∎

Dato $f(x) \in \mathbb{K}[x]$ indichiamo con $f'(x)$ il derivato formale di $f(x)$ e poniamo

$$d(x) = \text{M.C.D.}(f(x), f'(x)).$$

(5.16) Lemma *$f(x)$ ha una radice multipla se e solo se $d(x)$ ha grado > 0.*

Dimostrazione. Sia α una radice di $f(x)$ di molteplicità ≥ 2. Per definizione di molteplicità si ha $f(x) = (x - \alpha)^2 q(x)$. Ne segue $f'(x) = 2(x - \alpha)q(x) + (x - \alpha)^2 q'(x)$. Pertanto $(x - \alpha)$ divide $f'(x)$ e quindi anche $d(x)$. Viceversa, supponiamo che $d(x)$ abbia grado > 0 e sia $(x - \alpha)$ un suo fattore. Da $f(x) = (x - \alpha)g(x)$ segue $f'(x) =$

$g(x)+(x-\alpha)g'(x)$. Poichè $x-\alpha$ divide $f'(x)$, esso divide anche $g(x) = f'(x)-(x-\alpha)g'(x)$. Si conclude che $(x-\alpha)^2$ divide $f(x)$.

■

6 Esercizi

(6.1) Esercizio *Si determini una base $\mathcal{B}$ di $V = \frac{\mathbb{Q}[x]}{\langle x^3+4\rangle}$ come $\mathbb{Q}$-modulo e si scriva la matrice, rispetto a $\mathcal{B}$, della applicazione lineare:*

$$\mu_{f(x)} : V \to V \quad \text{tale che} \quad v \mapsto f(x)v$$

per i seguenti polinomi: $f(x) = x$, $f(x) = x^2$, $f(x) = x^3 + 2x + 4$. Di ciascuna delle matrici ottenute si scriva la forma canonica razionale.

(6.2) Esercizio *Si determini una base $\mathcal{B}$ di*

$$V = \frac{\mathbb{Q}[x]}{\langle x^2+4\rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x-3\rangle}$$

come $\mathbb{Q}$-modulo e si scriva la matrice, rispetto a $\mathcal{B}$, della applicazione lineare:

$$\mu_{f(x)} : V \to V \quad \text{tale che} \quad v \mapsto f(x)v$$

per i seguenti polinomi: $f(x) = x$, $f(x) = -3x + 2$, $f(x) = x^2 - 6x$. Di ciascuna delle matrici ottenute si scriva la forma canonica razionale.

(6.3) Esercizio *Si determinino la forma canonica razionale C, i divisori elementari, la forma canonica di Jordan J, autovalori e autospazi di J di una matrice A avente invarianti di similarità :*

$$d_1(x) = x + 5,\ d_2(x) = x + 5,\ d_3(x) = x(x+5)^2.$$

(6.4) Esercizio *Sia $d(x) = a(x)b(x)$, con $M.C.D.(a(x), b(x)) = 1$. Si dimostri che la matrice companion $C_{d(x)}$ è coniugata a $\begin{pmatrix} C_{a(x)} & 0 \\ 0 & C_{b(x)} \end{pmatrix}$.*

(6.5) Esercizio *Posto $i := e^{\frac{2\pi}{4}} \in \mathbb{C}$, si determinino la forma canonica di Jordan J, autovalori e autospazi di J, invarianti di similarità , forma canonica razionale C e autospazi di C di una matrice A avente divisori elementari:*

$$x + i,\ (x+i)^2,\ (x+1)^2.$$

(6.6) Esercizio *Posto* $\omega := e^{\frac{2\pi}{3}} \in \mathbb{C}$*, si determinino la forma canonica di Jordan* J*, autovalori e autospazi di* J*, invarianti di similarità , forma canonica razionale* C*, autospazi di* C *di una matrice* A *avente divisori elementari:*

$$x, x^2,\ (x+\omega)^2,\ (x+\overline{\omega})^2.$$

(6.7) Esercizio *Date*

$$A = \begin{pmatrix} 0 & 0 & -2\sqrt{2} \\ 1 & 0 & -6 \\ 0 & 1 & -3\sqrt{2} \end{pmatrix}, \quad B = \begin{pmatrix} -\sqrt{2} & 0 & 0 \\ 1 & -\sqrt{2} & 0 \\ 0 & 1 & -\sqrt{2} \end{pmatrix}$$

si trovi P *tale che* $P^{-1}AP = B$*.*

(6.8) Esercizio *Sia* A *una delle seguenti matrici:*

$$\begin{pmatrix} -1 & 0 & 0 \\ 2 & -3 & 1 \\ 4 & -4 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 5 & -1 & 1 \\ -2 & 4 & -1 \\ -16 & 12 & -5 \end{pmatrix}$$

Si determini la forma canonica razionale C *di* A*. Detta* α *l'applicazione lineare indotta da* A *rispetto alla base canonica, si trovi una base di* $\mathbb{Q}^3$ *rispetto alla quale* α *abbia matrice* C*.*

(6.9) Esercizio *Si determini la forma canonica razionale di*

$$\begin{pmatrix} 1 & 2 & -1 \\ 0 & 3 & 1 \\ -26 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 4 & 2 & 2 \\ 1 & 4 & 2 \\ -2 & -3 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 2 & -6 \\ 0 & 2 & 0 \\ 1 & -1 & 5 \end{pmatrix}$$

(6.10) Esercizio *Si calcolino autovalori, autospazi e forma canonica razionale di ciascuna delle seguenti matrici:*

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 0 & 2 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 4 \end{pmatrix}, \quad \begin{pmatrix} -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 3 & 1 & -1 & 0 \\ 2 & 1 & 1 & -1 \end{pmatrix}$$

(6.11) Esercizio *Sia* v *un autovettore di* A *relativo a* λ*. Si dimostri che* $P^{-1}v$ *è un autovettore di* $P^{-1}AP$ *relativo a* λ*.*

(6.12) Esercizio *Sia* v *un autovettore di* A *relativo a* λ*. Dimostrare che:*
i) v *è autovettore di* A^m *relativo a* λ^m *per ogni* $m \geq 0$*;*

ii) v è autovettore di $f(A)$ relativo a $f(\lambda^m)$ per ogni $f(x) \in \mathbb{K}[x]$.

(6.13) Esercizio *Siano $f(x) \in \mathbb{K}[x]$ e $A, B \in \mathrm{Mat}_n(\mathbb{K})$. Dimostrare che:*
i) Se A è coniugata a B, allora $f(A)$ è coniugata a $f(B)$;
ii) se A è diagonalizzabile, anche $f(A)$ è diagonalizzabile.

(6.14) Esercizio *Sia $A \in \mathrm{Mat}_n(\mathbb{C})$ tale che $A^{20} = I$. A è diagonalizzabile?*

(6.15) Esercizio *In $\mathrm{Mat}_2(\mathbb{C})$ si scrivano tutte le possibili forme di Jordan J, a due a due non coniugate, tali che $J^3 = I$.*

(6.16) Esercizio *In $\mathrm{Mat}_5(\mathbb{C})$ si scrivano tutte le possibili forme di Jordan J, a due a due non coniugate, tali che $J^4 = I$ e $\det J = 1$.*

Capitolo V

La geometria dei gruppi classici

1 Forme bilineari e forme Hermitiane

In questo Capitolo σ indica un automorfismo di un campo $\mathbb{K}$ tale che

$$\sigma^2 = \mathrm{Id}_{\mathbb{K}}.$$

Quindi σ può essere l'applicazione identica $\mathrm{Id}_{\mathbb{K}}$, oppure avere periodo 2.

Per esempio, σ può essere l'automorfismo coniugio del campo complesso $\mathbb{C}$:

$$a + ib \mapsto a - ib, \quad \forall\ a + ib \in \mathbb{C}.$$

Per ogni $\alpha \in \mathbb{K}$ conviene porre $\sigma(\alpha) := \alpha^{\sigma}$.

(1.1) Definizione *Sia V uno spazio vettoriale su $\mathbb{K}$. Una applicazione*

$$(\ ,\ ) : V \times V \to \mathbb{K}$$

tale che, per ogni $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathbb{K}$ e per ogni $v_1, v_2, w_1, w_2 \in V$:

$$(\lambda_1 v_1 + \lambda_2 v_2,\ \mu_1 w_1 + \mu_2 w_2) \ = \sum_{i,j=1}^{2} \lambda_i \mu_j{}^{\sigma}\, (v_i, w_j) \tag{1.2}$$

si dice:

- *una* forma bilineare *su V se $\sigma = \mathrm{Id}_{\mathbb{K}}$;*
- *una* forma hermitiana *su V se $\sigma \neq \mathrm{Id}_{\mathbb{K}}$ e $(v, w) = (w, v)^{\sigma}$, per ogni $v, w \in V$.*

Diciamo inoltre che la forma è :

- non singolare *se, per ogni vettore non nullo v di V, esiste $u \in V$ tale che $(u, v) \neq 0_{\mathbb{K}}$.*
- bilineare simmetrica *se $\sigma = \mathrm{Id}_{\mathbb{K}}$ e, per ogni $v, w \in V$, si ha $(v, w) = (w, v)$;*
- bilineare antisimmetrica *se $\sigma = \mathrm{Id}_{\mathbb{K}}$ e, per ogni $v, w \in V$, si ha $(v, w) = -(w, v)$.*

Chiaramente, per ogni $v \in V$:

$$((0_V, v)) = ((0_{\mathbb{K}} 0_V, v)) = 0_{\mathbb{K}} (0_V, v) = 0_{\mathbb{K}} = (v, 0_V) .$$

(1.3) Esempi

1) *Posto* $V = \mathbb{R}^n$*, l'applicazione*

$$(v, w) := v^T w, \quad \forall\ v, w \in V$$

è una forma bilineare simmetrica, non singolare su V*. Per* $n = 2$ *si ha:*

$$\left(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \right) := (x_1, x_2) \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = x_1 y_1 + x_2 y_2.$$

Nel caso $n = 3$ *tale forma induce la metrica usuale nello spazio* $\mathbb{R}^3$*.*

2) *Posto* $V = \mathbb{K}^n$ *e fissata una qualunque matrice* $J \in \mathrm{Mat}_n(\mathbb{K})$*, l'applicazione*

$$(v, w) := v^T A w, \quad \forall\ v, w \in V$$

è una forma bilineare su V*. Per* $\mathbb{K} = \mathbb{R}$*,* $A = I$ *si ha l'esempio* 1)*.*

Date una forma bilineare o hermitiana $(\ ,\ ) : V \times V \to \mathbb{K}$ e fissata una base

$$\mathcal{B} = \{v_1, \ldots, v_n\}$$

di V, per ogni

$$v = \sum_{i=1}^{n} k_i v_i, \quad w = \sum_{i=1}^{n} h_i v_i, \quad k_i, h_i \in \mathbb{K}$$

si ha, in virtù degli assiomi (1.2) della definizione 1.1:

$$(v, w) = \sum_{i,j=1}^{n} k_i h_j^{\sigma} (v_i, v_j). \tag{1.4}$$

Introducendo la matrice

$$J := ((v_i, v_j)) \in \mathrm{Mat}_n(\mathbb{K}). \tag{1.5}$$

e passando ai vettori coordinate, la (1.4) si scrive nella forma:

$$(v, w) = v_{\mathcal{B}}^T J w_{\mathcal{B}}^{\sigma}, \quad \forall\ v, w \in V. \tag{1.6}$$

J è l'unica matrice di $\mathrm{Mat}_n(\mathbb{K})$ che soddisfa (1.6).

Infatti se $A = (a_{ij})$ soddisfa (1.6), da $v_{i\mathcal{B}} = e_i$ per $1 \leq i \leq n$, segue:

$$(v_i, v_j) \;=\; {v_i}_{\mathcal{B}}{}^T A v_{j\mathcal{B}} \;=\; {e_i}^T A e_j = a_{ij}, \quad \forall\; i, j \leq n.$$

Si conclude $A = J$. È così giustificata la seguente:

(1.7) Definizione *$J = ((v_i, v_j))$ si dice la matrice della forma $(\ ,\ )$ rispetto a $\mathcal{B}$.*

In virtù di (1.6), ogni forma bilineare di $\mathbb{K}^n$ è del tipo descritto nell'esempio 2). In tale esempio A è la matrice della forma rispetto alla base canonica.

(1.8) Lemma *Sia $J = ((v_i, v_j))$ la matrice di una forma bilineare o hermitiana su V, rispetto a una base $\mathcal{B} = \{v_1, \ldots, v_n\}$.*

1) *La forma è non singolare se e solo se* $\det J \neq 0_{\mathbb{K}}$*;*

2) *se $\sigma = \mathrm{Id}_{\mathbb{K}}$, la forma è simmetrica se e solo se $J^T = J$;*

3) *se $\sigma = \mathrm{Id}_{\mathbb{K}}$, la forma è antisimmetrica se e solo se $J^T = -J$;*

4) *se $\sigma \neq \mathrm{Id}_{\mathbb{K}}$, la forma è hermitiana se e solo se $J^T = J^\sigma$.*

Dimostrazione.
1) Fissato $v \in V$, per ogni $v_i \in \mathcal{B}$ si ha $(v_i, v) = {e_i}^T J v^\sigma_{\mathcal{B}}$.
Sia $\det J \neq 0_{\mathbb{K}}$. Consideriamo $v \in V$ non nullo. Se fosse ${e_i}^T J v^\sigma_{\mathcal{B}} = 0_{\mathbb{K}}$ per ogni i, si avrebbe $J v^\sigma_{\mathcal{B}} = 0_{\mathbb{K}^n}$ da cui, moltiplicando per J^{-1}, la contraddizione $v^\sigma_{\mathcal{B}} = 0_{\mathbb{K}^n}$. Pertanto $(v_i, v) \neq 0_{\mathbb{K}}$ per almeno un indice i. Concludiamo che la forma è non degenere.
Viceversa la forma sia non degenere. Se fosse $\det J = 0_{\mathbb{K}}$, esisterebbe $w \in V$ non nullo tale che $J w^\sigma_{\mathcal{B}} = 0_{\mathbb{K}^n}$. Ne seguirebbe $(v, w) = v^T_{\mathcal{B}} J w^\sigma_{\mathcal{B}} = 0_{\mathbb{K}}$ per ogni $v \in V$, contraddizione. Si conclude $\det J \neq 0_{\mathbb{K}}$.

2) e 4). Se la forma è simmetrica o hermitiana si ha, in particolare,

$$(v_j, v_i) = (v_i, v_j)^\sigma, \quad 1 \leq i, j \leq n$$

da cui $J^T = J^\sigma$.
Viceversa, sia $J^T = J^\sigma$. Notando che $(v, w) = (v, w)^T$ per ogni $v, w \in V$:

$$(v, w) = v^T_{\mathcal{B}} J w^\sigma_{\mathcal{B}} = \left(v^T_{\mathcal{B}} J w^\sigma_{\mathcal{B}}\right)^T = \left(w^\sigma_{\mathcal{B}}\right)^T J^\sigma \left(v^\sigma_{\mathcal{B}}\right)^\sigma = \left(w^T_{\mathcal{B}} J v_{\mathcal{B}}\right)^\sigma = (w, v)^\sigma.$$

Si conclude che la forma è simmetrica se $\sigma = \mathrm{Id}_{\mathbb{K}}$, è hermitiana se $\sigma \neq \mathrm{Id}_{\mathbb{K}}$.

3) Se la forma è antisimmetrica, da

$$(v_j, v_i) = -(v_i, v_j), \quad 1 \leq i, j \leq n$$

segue $J^T = -J$. Viceversa, se $J^T = -J$, per ogni $v, w \in V$:

$$(v, w) = v_{\mathcal{B}}^T J w_{\mathcal{B}} = \left(v_{\mathcal{B}}^T J w_{\mathcal{B}}\right)^T = -w_{\mathcal{B}}^T J v_{\mathcal{B}} = -(w, v).$$

Si conclude che la forma è antisimmetrica. ■

(1.9) Lemma *Sia $J \in \mathrm{Mat}_n(\mathbb{K})$ la matrice di una forma bilineare o hermitiana su V, rispetto a una sua base $\mathcal{B}$. Una matrice $J' \in \mathrm{Mat}_n(\mathbb{K})$ è la matrice della stessa forma rispetto una conveniente base $\mathcal{B}'$ se e solo se esiste $P \in \mathrm{GL}_n(\mathbb{K})$ tale che:*

$$J' = P^T J P^\sigma. \tag{1.10}$$

Dimostrazione.
Supponiamo che J' sia la matrice della forma rispetto un'altra base $\mathcal{B}'$ e sia

$$P := \left(\ (v_1')_{\mathcal{B}} \ \middle| \ \dots \ \middle| \ (v_n')_{\mathcal{B}} \ \right)$$

la matrice di passaggio da $\mathcal{B}$ a $\mathcal{B}'$. Per ogni $v \in V$ si ha: $v_{\mathcal{B}} = P v_{\mathcal{B}'}$. Ne segue:

$$(v, w) = v_{\mathcal{B}}^T J w_{\mathcal{B}}^\sigma = \left(v_{\mathcal{B}'}^T P^T\right) J \left(P^\sigma w_{\mathcal{B}'}^\sigma\right) = v_{\mathcal{B}'}^T \left(P^T J P^\sigma\right) w_{\mathcal{B}'}^\sigma.$$

Pertanto $P^T J P^\sigma$ soddisfa (1.6), da cui $J' = P^T J P^\sigma$.
Viceversa, sia $J' = P^T J P^\sigma$, con $P \in \mathrm{GL}_n(\mathbb{K})$. Essendo P invertibile esiste una base $\mathcal{B}'$ di V tale che P è la matrice di passaggio da $\mathcal{B}$ a $\mathcal{B}'$. Per il punto precedente J' è la matrice della forma rispetto $\mathcal{B}'$. ■

(1.11) Definizione *Diremo che due matrici $J, J' \in \mathrm{Mat}_n(\mathbb{K})$ sono* congruenti *se esiste $P \in \mathrm{GL}_n(\mathbb{K})$ tale che $P^t J P^\sigma = J'$.*

É facile verificare che la congruenza è una relazione di equivalenza.
Per il precedente lemma, se J è la matrice di una forma bilineare o hermitiana rispetto una data base di V, allora J' è congruente a J se e solo se è la matrice della stessa forma rispetto una conveniente base $\mathcal{B}'$.

2 Ortogonalità

In questo paragrafo consideriamo una forma $(\ ,\ ) : V \times V \to \mathbb{K}$ che sia bilineare simmetrica o antisimmetrica, oppure hermitiana.

(2.1) Definizione *Due vettori $u, w \in V$ si dicono* ortogonali *se $(u, w) = 0_{\mathbb{K}}$.*

In virtù dell'assioma $(w, u) = \pm(u, w)^{\sigma}$ l'ortogonalità fra vettori è simmetrica.

(2.2) Lemma *Per ogni sottoinsieme W di V il sottoinsieme $W^{\perp}$ dei vettori di V ortogonali a tutti i vettori di W è un sottospazio. Pertanto*

$$W^{\perp} := \{v \in V \mid (v, w) = 0,\ \forall\ w \in W\}$$

è detto il sottospazio ortogonale *a W.*

Dimostrazione.
• $0_V \in W^{\perp}$ poichè $(0_V, w) = 0$ per ogni $w \in W$.
• Siano $v_1, v_2 \in W^{\perp}$ e $\lambda_1, \lambda_2 \in \mathbb{K}$. Ne segue

$$(\lambda_1 v_1 + \lambda_2 v_2, w) = \lambda_1 (v_1, w) + \lambda_2 (v_2, w) = 0_{\mathbb{K}} + 0_{\mathbb{K}} = 0_{\mathbb{K}}, \quad \forall\ w \in W.$$

Si conclude che $\lambda_1 v_1 + \lambda_2 v_2 \in W^{\perp}$, che è pertanto un sottospazio. ■

(2.3) Definizione *Siano U, W due sottospazi di V. Scriviamo $V = U \perp W$ e diciamo che V è* somma ortogonale *di U e W se*

1) *$V = U \dot{+} W$ è somma diretta di U e W;*

2) *$U \leq W^{\perp}$, ossia $(u, w) = 0_{\mathbb{K}}$ per ogni $u \in U$, $w \in W$.*

Un sottospazio W si dice *totalmente isotropo* se $W \leq W^{\perp}$.

(2.4) Lemma *Supponiamo che la forma sia non degenere.*
Per ogni sottospazio W di V si ha:

$$\dim(W^{\perp}) = \dim(V) - \dim(W).$$

In particolare:

i) la dimensione di un sottospazio totalmente isotropo è $\leq \frac{1}{2} \dim V$;

ii) se la restrizione della forma a W è non degenere, si ha $V = W \perp W^{\perp}$.
Inoltre la restrizione della forma a $W^{\perp}$ è non degenere.

Dimostrazione. Sia $\{w_1, \ldots, w_m\}$ una base di W. Per ogni $v \in V$ si ha:

$$v \in W^{\perp} \iff (w_i, v) = 0_{\mathbb{K}},\ 1 \leq i \leq m. \tag{2.5}$$

Detta $\mathcal{B} = \{w_1, \ldots, w_m, w_{m+1}, \ldots, w_n\}$ una base di V che estende quella scelta per W, sia J la matrice della forma rispetto $\mathcal{B}$. Si ha allora:

$$v \in W^\perp \iff {e_i}^T J v_{\mathcal{B}}^\sigma = 0_{\mathbb{K}},\ 1 \leq i \leq m. \tag{2.6}$$

Ossia i vettori $v \in W^\perp$ sono quelli per cui $v_{\mathcal{B}}^\sigma$ è soluzione del sistema

$$\begin{cases} {e_1}^T JX = 0_{\mathbb{K}} \\ \ldots \\ {e_m}^T JX = 0_{\mathbb{K}}, \end{cases} \qquad X := (x_1, \ldots x_n)^T .$$

Si tratta di un sistema lineare omogeneo in m equazioni e $n = \dim V$ indeterminate. Essendo J non degenere, le sue righe (in particolare le prime m righe) sono indipendenti. Ne segue che le equazioni del sistema sono indipendenti. Quindi le sue soluzioni formano un sottospazio di dimensione $n - m = \dim V - \dim W$.

i) Sia W totalmente isotropo. Da $W \leq W^\perp$ segue $\dim W^\perp \geq \dim W$. Quindi $\dim V - \dim W \geq \dim W$, da cui $\dim W \leq \frac{1}{2} \dim V$.

ii) Se la restrizione della forma a W è non degenere, allora $W \cap W^\perp = \{0_V\}$. Ne segue $\dim(W + W^\perp) = \dim W + \dim W^\perp = \dim V$, da cui $V = W \perp W^\perp$.
Infine sia u un vettore di $W^\perp$, ortogonale a tutti i vettori di $W^\perp$. Da $V = W \perp W^\perp$ segue che u è ortogonale a tutti i vettori di V. Quindi $u = 0_V$ perchè la forma considerata è non degenere. ■

3 Lemma di Witt

Sia data una forma bilineare o hermitiana non singolare $(\ ,\ ) : V \times V \to \mathbb{K}$.

(3.1) Definizione *Un'*isometria *è un'applicazione lineare iniettiva $f : V \to V$ tale che*

$$(f(v), f(w)) = (v, w), \quad \forall\ v, w \in V.$$

(3.2) Lemma (di Witt) *Siano U un sottospazio di V e $f : U \to V$ una applicazione lineare iniettiva tale che $(f(u_1), f(u_2)) = (u_1, u_2)$ per ogni $u_1, u_2 \in U$. Allora f si estende a una isometria $\widehat{f} : V \to V$.*

Per una dimostrazione si veda [1, 20, pag. 81], o anche [6, Capitolo 6, pag. 369].

(3.3) Corollario *Ogni sottospazio totalmente isotropo di V è contenuto in sottospazio totalmente isotropo massimale.*

Dimostrazione. Siano U, W sottospazi totalmente isotropi di V, con W di dimensione massima fra quelle dei sottospazi totalmente isotropi. Ogni applicazione lineare iniettiva $f : U \to W$ soddisfa l'ipotesi del Lemma di Witt, e può quindi essere estesa a un isometria $\widehat{f} : V \to V$. Ne segue $U \leq \widehat{f}^{-1}(W)$, con $\widehat{f}^{-1}(W)$ totalmente isotropo massimale. ■

4 Spazi simplettici

(4.1) Definizione *Uno spazio vettoriale V su $\mathbb{K}$ si dice* simplettico *se su di esso è definita una forma bilineare, non degenere, tale che ogni vettore $v \in V$ è isotropo, ossia*

$$(v, v) = 0_{\mathbb{K}}.$$

Scopo di questo paragrafo è dimostrare che esiste essenzialmente un unico spazio simplettico su $\mathbb{K}$ per ogni n pari.
Per la bilinearità, un prodotto simplettico è *antisimmetrico*. Infatti, per ogni $v, w \in \mathbb{K}^n$:

$$0 = (v + w, v + w) = (v, v) + (v, w) + (w, v) + (w, w) = (v, w) + (w, v).$$

Ne segue $(w, v) = -(v, w)$.

(4.2) Teorema *Sia V uno spazio simplettico su $\mathbb{K}$, di dimensione n.*

1) *$n = 2m$ è pari;*

2) *esiste una base $\mathcal{B}$ di V rispetto alla quale la forma ha matrice:*

$$J = \begin{pmatrix} \mathbf{0} & I_m \\ -I_m & \mathbf{0} \end{pmatrix}. \tag{4.3}$$

Dimostrazione. Induzione su n.
Se fosse $n = 1$, per qualunque base $\{v\}$ di V si avrebbe $(v, v) = 0_{\mathbb{K}}$, in contrasto con l'ipotesi che V è non degenere. Quindi $n \geq 2$.

Per la non-degenericità della forma, esistono $v_1, w \in V$ tali che $\lambda := (v_1, w) \neq 0_{\mathbb{K}}$.
In particolare v_1 e w sono linearmente indipendenti. Posto $w_1 := \lambda^{-1} w$, si ha:

$$(v_1, w_1) = \left(v_1, \lambda^{-1} w\right) = \lambda^{-1}(v_1, w) = 1_{\mathbb{K}}.$$

Se $n = 2$ abbiamo l'asserto. Infatti la matrice della forma rispetto $\mathcal{B} = \{v_1,\ w_1\}$ è

$$J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Per $n > 2$, il sottospazio $W := \langle v_1, w_1 \rangle$ è non singolare. Ne segue

$$V = W\ \perp\ W^{\perp}.$$

$W^{\perp}$ è non degenere, quindi è uno spazio simplettico di dimensione $n-2$. Per induzione su n si ha $n-2 = 2(m-1)$ pari. Inoltre $W^{\perp}$ ammette una base $\{v_2,\ \ldots,\ v_m,\ w_2,\ \ldots,\ w_m\}$ rispetto alla quale la matrice della forma è del tipo di (4.3). Scegliendo

$$\mathcal{B} = \{v_1,\ \ldots,\ v_m,\ w_1,\ \ldots,\ w_m\}$$

si ha la tesi. ■

5 Spazi ortogonali e spazi unitari

Su un campo $\mathbb{K}$ di caratteristica 2, le forme bilineari simmetriche sono antisimmetriche. Per tale ragione, per studiare gli spazi ortogonali in caratteristica 2, è necessario introdurre e classificare le forme quadratiche. Siccome qui non le trattiamo, per gli spazi ortogonali ci limitiamo al caso di caratteristica $\neq 2$.

(5.1) Definizione *Sia V uno spazio vettoriale su un campo $\mathbb{K}$.*

• *V si dice uno spazio* ortogonale *se $\mathbb{K}$ ha caratteristica $\neq 2$ ed è definita una forma bilineare simmetrica, non degenere $(\ ,\ ) : V \times V \to \mathbb{K}$.*

• *V si dice uno spazio* unitario *se $\mathbb{K}$ che ha un automorfismo di periodo 2 ed è definita una forma hermitiana, non degenere $(\ ,\ ) : V \times V \to \mathbb{K}$.*

(5.2) Definizione *Sia V uno spazio ortogonale o hermitiano e sia $\mathcal{B} = \{v_1,\ \ldots,\ v_n\}$ una sua base.*

• *$\mathcal{B}$ si dice* ortogonale *se $(v_i, v_j) = 0$ per ogni $i \neq j$.*

• *$\mathcal{B}$ si dice* ortonormale *se è ortogonale e $(v_i, v_i) = 1$ per ogni i.*

Equivalentemente $\mathcal{B}$ è una base ortogonale se la matrice della forma rispetto $\mathcal{B}$ è diagonale. $\mathcal{B}$ è una base ortonormale se la matrice della forma rispetto $\mathcal{B}$ è quella identica.

(5.3) Teorema *Sia V uno spazio ortogonale o Hermitiano su $\mathbb{K}$. Nel caso in cui V è ortogonale si supponga* $\operatorname{char}\mathbb{K} \neq 2$. *Allora V ha una base ortogonale.*

Dimostrazione. Basta dimostrare che esiste $v \in V$ tale che $(v,v) \neq 0_{\mathbb{K}}$. Infatti, in tal caso, il sottospazio $\langle v \rangle$ è non-degenere. Ne segue

$$V = \langle v \rangle \perp \langle v \rangle^{\perp}.$$

Poichhè $\langle v \rangle^{\perp}$ ha dimensione $n-1$ possiamo supporre, per induzione su n, che abbia una base ortogonale $\overline{\mathcal{B}}$. Pertanto $\{v\} \cup \overline{\mathcal{B}}$ è una base ortogonale di V.

Resta da dimostrare l'esistenza di $v \in V$ tale che $(v,v) \neq 0_{\mathbb{K}}$.

Per la non-degenericità della forma, esistono $u, w \in V$ tali che $\lambda := (u,w) \neq 0_{\mathbb{K}}$.
Se $(u,u) \neq 0_{\mathbb{K}}$ oppure $(w,w) \neq 0_{\mathbb{K}}$ siamo a posto. Quindi possiamo supporre

$$(u,u) = (w,w) = 0.$$

Se $\operatorname{car}\mathbb{K} \neq 2$, ponendo $v = \lambda^{-1}u + w$ si ha:

$$(v,v) = \lambda^{-1}(u,w) + \left(\lambda^{-1}\right)^{\sigma}(w,u) = \lambda^{-1}\lambda + (\lambda^{\sigma})^{-1}\lambda^{\sigma} = 21_{\mathbb{K}} \neq 0_{\mathbb{K}}.$$

Se $\operatorname{car}\mathbb{K} = 2$, allora V è unitario. Poichè l'automorfismo σ di $\mathbb{K}$ che definisce la forma hermitiana non è $\mathrm{Id}_{\mathbb{K}}$, esiste $\alpha \in \mathbb{K}$ tale che $\alpha^{\sigma} \neq \alpha$. Scegliendo $v = \lambda\alpha^{-1}u + w$ si ha

$$(v,v) = \alpha + \alpha^{\sigma} = \alpha - \alpha^{\sigma} \neq 0_{\mathbb{K}}.$$

■

(5.4) Osservazione *Se $\mathbb{K}$ ha caratteristica 2, una forma bilineare simmetrica può non ammettere basi ortogonali. Ad esempio, per $\mathbb{K} = \mathbb{Z}_2$, $n = 2$, consideriamo la forma bilineare indotta dalla matrice $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ rispetto alla base canonica di ${\mathbb{Z}_2}^2$. Tale forma è non degenere, ma non ammette basi ortogonali dato che tutti i vettori sono isotropi.*

(5.5) Corollario

1) *Uno spazio ortogonale V su $\mathbb{C}$ ha una base ortonormale;*

2) *uno spazio hermitiano V su $\mathbb{C}$, tale che $(v,v) > 0$ per ogni $v \neq 0_V$ in V, ha una base ortonormale;*

3) *uno spazio ortogonale V su $\mathbb{R}$, tale che $(v,v) > 0$ per ogni $v \neq 0_V$ in V, ha una base ortonormale.*

Dimostrazione.
Per il Teorema 5.3 esiste una base ortogonale $\mathcal{B} = \{v_1, \ldots, v_n\}$ di V. Poniamo

$$(v_i, v_i) := \lambda_i, \quad 1 \leq i \leq n.$$

1) Per ogni $i \leq n$ esiste $\mu_i \in \mathbb{C}$ tale che $\mu_i^2 = \lambda_i^{-1}$. Una base ortonormale è quindi:

$$\mathcal{B}' = \left\{\mu_1^{-1} v_1, \ldots, \mu_n^{-1} v_n\right\}.$$

2) e 3) Notiamo che, anche nel caso hermitiano, $(v,v) = (v,v)^\sigma \in \mathbb{R}$. La condizione $(v,v) \geq 0$ implica $\lambda_i > 0$. Esiste quindi $\mu_i \in \mathbb{R}$ tale che $\mu_i^2 = \lambda_i^{-1}$ per ogni $i \leq n$. Definendo $\mathcal{B}'$ come nel caso precedente si ottiene una base ortonormale. ■

(5.6) Osservazione *Dal Teorema* 5.3 *segue facilmente che uno spazio ortogonale V, di dimensione n su $\mathbb{R}$, ha una base ortogonale rispetto alla quale la forma ha matrice*

$$D = \operatorname{diag}\left(\underbrace{1, \ldots, 1}_{h}, \underbrace{-1, \ldots, -1}_{n-h}\right)$$

per qualche h tale che $0 \leq h \leq n$. Per il Teorema di Sylvester [7, Cap. VIII, pag 165] due matrici D e D' di questo tipo sono congruenti solo se hanno lo stesso numero di componenti uguali a 1.

Come si intuisce dai casi fin qui considerati, la classificazione delle forme bilineari simmetriche e hermitiane dipende in modo essenziale dal campo $\mathbb{K}$.

6 I gruppi classici

Siano $\mathbb{K}$ un campo e n un numero naturale ≥ 1.

(6.1) Definizione *Il gruppo delle matrici $n \times n$, a elementi in $\mathbb{K}$, con determinante $\neq 0$, si dice* gruppo generale lineare *di rango n su $\mathbb{K}$, e si indica con* $\mathrm{GL}_n(\mathbb{K})$.

Per il Teorema di Binet, l'applicazione

$$\delta : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^*$$

tale che $A \mapsto \det A$, è un epimorfismo di gruppi moltiplicativi. Il nucleo di δ è costituito dal *gruppo speciale lineare* $\mathrm{SL}_n(\mathbb{K})$ delle matrici di determinante 1. $\mathrm{SL}_n(\mathbb{K})$ è quindi un sottogruppo normale di $\mathrm{GL}_n(\mathbb{K})$. Inoltre, dal teorema degli omomorfismi segue che

$$\frac{\mathrm{GL}_n(\mathbb{K})}{\mathrm{SL}_n(\mathbb{K})} \sim \mathbb{K}^*.$$

Indichiamo con Z il centro di $\mathrm{GL}_n(\mathbb{K})$, cioè l'insieme degli elementi che commutano con tutti gli altri. Esso risulta essere l'insieme delle matrici scalari λI con $\lambda \in \mathbb{K}^*$.

(6.2) Definizione

• *Si dice* gruppo proiettivo generale lineare *il quoziente*

$$\frac{\mathrm{GL}_n(\mathbb{K})}{Z} := \mathrm{PGL}_n(\mathbb{K}).$$

• *Si dice* gruppo proiettivo speciale lineare *il quoziente*

$$\frac{\mathrm{SL}_n(\mathbb{K})}{Z \cap \mathrm{SL}_n(\mathbb{K})} := \mathrm{PSL}_n(\mathbb{K}).$$

Vediamo ora come i gruppi classici possono essere definiti come opportuni sottogruppi di $\mathrm{GL}_n(\mathbb{K})$), in relazione a geometrie rispettivamente simplettiche, ortogonali e unitarie.

(6.3) Definizione *Assegnata una forma bilineare o Hermitiana*

$$(\ ,\ ) : \mathbb{K}^n \times \mathbb{K}^n \to \mathbb{K}, \tag{6.4}$$

*un'*isometria *di* (6.4) *è un elemento* $g \in \mathrm{GL}_n(\mathbb{K})$ *tale che*

$$(gv, gw) = (v, w), \quad \forall\ v, w \in \mathbb{K}^n.$$

(6.5) Lemma *L'insieme* H *delle isometrie della forma* (6.4) *è un sottogruppo di* $\mathrm{GL}_n(\mathbb{K})$.

Dimostrazione. Da $(Iv, Iw) = (v, w)$ per ogni v, w segue $I \in H$. Se $x, y \in H$ allora

$$((xy)v, (xy)w) = (x(yv), x(yw)) = (xv, xw) = (v, w)\,,\ \forall\ v, w.$$

Pertanto $xy \in H$. Infine, se $x \in H$, per ogni v, w si ha

$$(v, w)\left(xx^{-1}v, xx^{-1}w\right) = \left(x^{-1}v, x^{-1}w\right),\ \forall\ v, w.$$

Pertanto $x^{-1} \in H$. ■

Vediamo ora come si puó caratterizzare H in modo piú esplicito. A tale scopo sia J la matrice di (6.4) rispetto alla base canonica $\mathcal{B}$ di $\mathbb{K}^n$. Poichè ogni vettore $v \in \mathbb{K}^n$ coincide con il proprio vettore coordinate $v_{\mathcal{B}}$, per ogni $v, w \in \mathbb{K}^n$ si ha:

$$(v, w) = v^T J w^\sigma$$

dove σ é l'automorfismo di $\mathbb{K}$ relativo a (6.4). Ne segue che un elemento g di $\mathrm{GL}_n(\mathbb{K})$ è una isometria se e solo se

$$v^T J w^\sigma = (gv)^T J (gw)^\sigma = v^T (g^T J g^\sigma) w^\sigma, \quad \forall\ v, w \in \mathbb{K}^n$$

se e solo se (applicando la precedente condizione ai vettori della base canonica):

$$g^T J g^\sigma = J.$$

Pertanto

$$H := \left\{ g \in \mathrm{GL}_n(\mathbb{K}) \mid g^T J g^\sigma = J \right\}.$$

(6.6) Lemma *Per ogni matrice invertibile P, il coniugato $P^{-1}HP$ è il gruppo delle isometrie della forma la cui matrice, rispetto alla base canonica, è*

$$J' = P^T J P^\sigma.$$

Dimostrazione. Per ogni $h \in H$: $(P^{-1}hP)^T J' (P^- hP)^\sigma = J'$ se e solo se $h^T J h^\sigma = J$. ■

(6.7) Osservazione *È importante osservare che due gruppi coniugati H e $P^{-1}HP$ sono isomorfi, tramite l'isomorfismo $h \mapsto P^{-1}hP$. Pertanto, se $\mathcal{B}$ e $\mathcal{B}'$ sono due basi di $\mathbb{K}^n$, e J, J' le corrispondenti matrici di una stessa forma, i relativi gruppi di isometrie sono in generale diversi, ma hanno la stessa struttura, essendo isomorfi.*

(6.8) Definizione *Il gruppo delle isometrie di uno spazio simplettico si dice* gruppo simplettico *e si indica con* $\mathrm{Sp}_n(\mathbb{K})$.

Per quanto visto, uno spazio simplettico ha dimensione pari $n = 2\ell$ e ammette una base rispetto alla quale il prodotto ha matrice

$$J = \begin{pmatrix} \mathbf{0} & I_\ell \\ -I_\ell & \mathbf{0} \end{pmatrix}.$$

Pertanto, a meno di coniugio, si può supporre

$$\mathrm{Sp}_{2\ell}(\mathbb{K}) = \left\{ g \in \mathrm{GL}_{2\ell}(\mathbb{K}) \mid g^t J g = J \right\}.$$

(6.9) Definizione *Supponiamo che* $\mathbb{K}$ *abbia caratteristica diversa da* 2*. Il gruppo delle isometrie di uno spazio ortogonale su* $\mathbb{K}$ *si dice* gruppo ortogonale

In generale, essendoci spazi ortogonali non isometrici, vi sono più gruppi ortogonali.

(6.10) Definizione *Supponiamo che* $\mathbb{K}$ *abbia un automorfismo* σ *di periodo* 2*. Il gruppo delle isometrie di uno spazio hermitiano* V*, di dimensione* n *su* $\mathbb{K}$*, si dice* gruppo unitario *e si indica con* $\mathrm{U}_n(\mathbb{K})$*.*

Se V ha una base ortonormale (ad esempio nel caso $\mathbb{K} = \mathbb{F}_{q^2}$), a meno di coniugio, si può supporre

$$\mathrm{U}_n(\mathbb{K}) = \left\{ g \in \mathrm{GL}_{2\ell}(\mathbb{K}) \mid g^T g^\sigma = I \right\}$$

dove g^σ si ottiene da g applicando l'automorfismo σ a tutti i suoi elementi.

Elenco dei simboli

Indice analitico

Bibliografia

[1] M.Aschbacher, Finite group theory, Cambridge University Press, 1986.

[2] R.W.Carter, Simple groups of Lie type, John Wiley and sons (1972).

[3] L.Dickson, Linear Groups, Dover Publications, Inc. (1958).

[4] B.Hartley, T.O.Hawkes, Rings, Modules and Linear Algebra, Chapman and Hall, 1970.

[5] Isaacs, I.M. Algebra: a graduate course, Brooks/Cole Publishing Company, 1994.

[6] N.Jacobson, Basic Algebra I, W.H.Freeman and company, San Francisco,1974.

[7] S.Lang, Linear Algebra, Addison-Wesley Publishing Company.

[8] M.C. Tamburini, Appunti di Algebra, Pubblicazioni dell' I.S.U. Iniversità Cattolica (2000).

[9] M.Chiara Tamburini, Algebra I Unità , Dispensa.

[10] M.Chiara Tamburini, Algebra II Unità , Dispensa.