UNIVERSITÀ CATTOLICA DEL SACRO CUORE

Facoltà di Scienze Matematiche, Fisiche e Naturali

ALGEBRA II UNITÀ

M. Chiara Tamburini

Anno Accademico 2009/2010

Indice

Capitolo I

Omomorfismi fra anelli

1 Ideali

Sia A un anello.

(1.1) Definizione *Un sottoinsieme I di A si dice un* ideale sinistro *se:*

1) $0_A \in I$;

2) *per ogni* $i_1, i_2 \in I$, *anche* $(i_1 + i_2) \in I$;

3) *per ogni* $a \in A$, *e per ogni* $i \in I$, *anche* $(ai) \in I$.

Analogamente I è un *ideale destro* se soddisfa le condizioni 1), 2) e

3′) per ogni $a \in A$, e per ogni $i \in I$, anche $(ia) \in I$.

Un ideale sinistro e destro si dice *bilatero*.

Sono utili le seguenti considerazioni.

a) Un ideale sinistro (destro) I di A è , in particolare, un sottogruppo di $(A, +, 0_A)$. Ciò segue dagli assiomi 1), 2) e dal fatto che, per ogni $i \in I$, anche $(-1_A)i = -i \in I$, per l'assioma 3).

b) Il singoletto $\{0_A\}$ e A stesso sono ideali di A (detti *impropri*).

c) Se A è un anello commutativo, ogni ideale sinistro è anche destro e viceversa.

(1.2) Esempio *L'insieme* $2\mathbb{Z}$ *dei numeri interi pari è un ideale dell'anello* $\mathbb{Z}$.

In generale, dato $a \in A$, indichiamo con Aa l'insieme dei suoi multipli. In simboli:

$$Aa := \{xa \mid x \in A\}\,.$$

(1.3) Lemma *Aa è il minimo ideale sinistro a cui a appartiene, ossia:*

1) *Aa è un ideale sinistro di A;*

2) $a \in Aa$;

3) *per ogni ideale sinistro* I *di* A *tale che* $a \in I$, *si ha* $Aa \leq I$.

Dimostrazione.

1) $0_A = 0_A a \in Aa$. Per ogni $xa,\ ya \in Aa$, anche $xa + ya = (x+y)a \in Aa$. Infine, per ogni $y \in A$ e per ogni $xa \in Aa$, anche $y(xa) = (yx)a \in Aa$.

2) $a = 1_A a \in Aa$.

3) Da $a \in I$ (ideale sinistro) segue $(xa) \in I$ per ogni $x \in A$. Pertanto $Aa \leq I$. ■

(1.4) Definizione *Se* A *è commutativo,* Aa *si dice l'ideale* principale generato da a.

Per ogni ideale sinistro (destro) I di A, vale il seguente fatto:

$$1_A \in I \implies A = I. \tag{1.5}$$

Infatti, se I è ideale sinistro, da $1_A \in I$ segue $A1_A \leq I$. Essendo $A1_A = A$ si conclude che $A = I$. Analoga dimsotrazione se I è ideale destro.

Una importante conseguenza è questa:

(1.6) Teorema *Gli unici ideali di un campo* $\mathbb{K}$ *sono* $\{0_\mathbb{K}\}$ *e* $\mathbb{K}$.

Dimostrazione.

Sia I un ideale di $\mathbb{K}$. Se $I \neq \{0_\mathbb{K}\}$, esiste $i \in I$ con $i \neq 0_\mathbb{K}$. Per definizione di campo, l'elemento i ha inverso i^{-1} in $\mathbb{K}$. Da $i \in I$ (ideale), segue $(i^{-1}i) \in I$, ossia $1_\mathbb{K} \in I$. Per (1.5) si conclude $\mathbb{K} = I$. ■

In virtù del seguente Lemma, dati due ideali I e J, il massimo ideale in essi contenuto è la loro intersezione $I \cap J$, mentre il mininmo ideale che li contiene è la loro somma

$$I + J := \{i + j \mid i \in I,\ j \in J\}.$$

(1.7) Lemma *Siano* I, J *due ideali sinistri di* A. *Allora:*

1) $I \cap J$ *è un ideale sinistro di* A;

2) $I + J$ *è un ideale sinistro di* A;

3) $I \cup J \subseteq I + J$;

4) *per ogni ideale sinistro* X *che contiene* $I \cup J$ *si ha* $I + J \leq X$.

Analoghe proprietà valgono per gli ideali destri.

Dimostrazione.

1) Per definizione di ideale $0_A \in I$ e $0_A \in J$, da cui $0_A \in I \cap J$. Siano ora $x_1, x_2 \in I \cap J$. Da $x_1, x_2 \in I$ segue $(x_1 + x_2) \in I$. Analogamente da $x_1, x_2 \in J$ segue $(x_1 + x_2) \in J$. Pertanto $(x_1 + x_2) \in I \cap J$. Infine siano $a \in A$, $x \in I \cap J$. Da $x \in I$ segue $ax \in I$. Da $x \in J$ segue $ax \in J$. Si conclude $ax \in I \cap J$.

2) Chiaramente $0_A = 0_A + 0_A \in I + J$. Da $(i_1 + j_1), (i_2 + j_2) \in I + J$ segue:

$$(i_1 + j_1) + (i_2 + j_2) = (i_1 + i_2) + (j_1 + j_2) \in I + J.$$

Infine, se $a \in A$ e $i + j \in I + J$, anche $a(i + j) = (ai) + (aj) \in I + J$.

3) Per ogni $i \in I$ si ha $i = i + 0_A$, quindi $I \leq I + J$. In modo analogo $J \leq I + J$.

4) Sia $i + j \in I + J$. Da $i \in I \leq X$ e da $j \in J \leq X$ si deduce $i, j \in X$. Pertanto, essendo X un ideale, $i + j \in X$. ■

2 Anelli quoziente

Un ideale I di un anello A dà luogo alla relazione definita ponendo, per ogni $a, a' \in A$:

$$a \equiv a' \pmod{I} \iff (a - a') \in I. \tag{2.1}$$

Poichè $(I, +, 0_A)$ è un sottogruppo di $(A, +, 0_A)$, tale relazione è di equivalenza in A. Per ogni $a \in A$, la sua classe di equivalenza è il laterale $I + a := \{i + a \mid i \in I\}$. Quindi:

$$a \equiv a' \pmod{I} \iff I + a = I + a'. \tag{2.2}$$

Per le precedenti affermazioni si veda il Teorema **4.2** del Capitolo 2 di [4].

(2.3) Lemma *Sia I un ideale bilatero di A. Per ogni $a, a', b, b' \in A$:*

$$\begin{cases} a \equiv a' \pmod{I} \\ b \equiv b' \pmod{I} \end{cases} \implies \begin{array}{ll} 1) & a + b \equiv a' + b' \pmod{I} \\ 2) & ab \equiv a'b' \pmod{I}. \end{array} \tag{2.4}$$

Dimostrazione.

1) I è un sottogruppo normale del gruppo additivo di A, essendo questo abeliano. Pertanto, per il Lemma **5.5** di [4], si ha $a + b \equiv a' + b' \pmod{I}$.

2) Da $a - a' = i_1 \in I$ e da $b - b' = i_2 \in I$ segue: $ab - a'b' = (a' + i_1)(b' + i_2) - a'b' = (a'i_2 + i_1b' + i_1i_2) \in I$. Pertanto $ab \equiv a'b' \pmod{I}$. ■

(2.5) Teorema *L'insieme* $\frac{A}{I}$ *dei laterali di* I *in* A *è un anello rispetto alle operazioni di somma e prodotto così definite. Per ogni* $a, b \in A$*:*

$$(I + a) + (I + b) := I + (a + b)$$

$$(I + a)(I + b) := I + (ab).$$

Esso è detto l' anello quoziente *di* A *rispetto a* I*.*

Dimostrazione.

$\frac{A}{I}$ è un gruppo rispetto alla somma per il Teorema 5.7 del Capitolo 2 di [4]. Chiaramente è abeliano, essendolo A. Il prodotto fra laterali è ben definito per il precedente Lemma. Esso è associativo:

$$((I + a)(I + b))(I + c) = I + (ab)c = I + a(bc) = (I + a)((I + b)(I + c)).$$

Il laterale $I + 1_A$ è elemento neutro rispetto al prodotto:

$$(I + 1_A)(I + a) = I + 1_A a = I + a, \quad (I + a)(I + 1_A) = I + a1_A = I + a.$$

Valgono infine le proprietà distributive della somma rispetto al prodotto:

$$(I + a)((I + b) + (I + c)) = (I + a)(I + (b + c)) =$$

$$I + a(b + c) = I + ab + ac = (I + ab) + (I + ac) = (I + a)(I + b) + (I + a)(I + c).$$

In modo analogo si verifica l'altra proprietà distributiva. ■

(2.6) Esempio *L'anello quoziente* $\frac{\mathbb{Z}}{n\mathbb{Z}}$*,* $n \geq 2$*.*

Per ogni laterale $n\mathbb{Z} + a$*, esiste un unico intero non negativo* $r \leq n - 1$*, tale che* $n\mathbb{Z} + a = n\mathbb{Z} + r$*. Tale* r *è il resto della divisione di* a *per* n*.*

Pertanto gli elementi dell'anello $\frac{\mathbb{Z}}{n\mathbb{Z}}$ *sono gli* n *laterali*

$$n\mathbb{Z} + 0,\ n\mathbb{Z} + 1,\ \ldots,\ n\mathbb{Z} + (n - 1).$$

La somma e il prodotto sono definite da:

$$(n\mathbb{Z} + a) + (n\mathbb{Z} + b) := n\mathbb{Z} + (a + b), \quad (n\mathbb{Z} + a)(n\mathbb{Z} + b) := n\mathbb{Z} + (ab).$$

Poichè ogni laterale $n\mathbb{Z} + a$ *coincide con la classe di resti* $[a]_n$*, è lo stesso scrivere:*

$$[a]_n + [b]_n := [a + b]_n, \quad [a]_n [b]_n := [ab]_n.$$

L' anello $\frac{\mathbb{Z}}{n\mathbb{Z}}$ *si dice anche l'anello delle* classi di resti modulo n *e si indica con* $\mathbb{Z}_n$.

Dato $f(x) \in \mathbb{K}[x]$, indichiamo con $< f(x) >$ l'ideale generato da $f(x)$. Ossia

$$< f(x) >:= \mathbb{K}[x]f(x). \tag{2.7}$$

(2.8) Lemma *Sia* $f(x)$ *un polinomio di grado* $n \geq 1$*, a coefficienti in un campo* $\mathbb{K}$*. Per ogni elemento* $< f(x) > +a(x)$ *dell'anello quoziente* $\frac{\mathbb{K}[x]}{<f(x)>}$*, esiste un unico polinomio* $r(x)$ *di grado* $\leq n-1$ *tale che*

$$< f(x) > +a(x) =< f(x) > +r(x).$$

Esso è il resto della divisione di $a(x)$ *per* $f(x)$.

Dimostrazione. Siano $q(x)$ e $r(x)$ il quoziente e il resto della divisione di $a(x)$ per $f(x)$. Da $a(x)-r(x) = q(x)f(x) \in < f(x) >$ segue $< f(x) > +a(x) =< f(x) > +r(x)$. Inoltre, per definizione, $r(x)$ ha grado $\leq n-1$. Supponiamo ora che $s(x)$ sia un polinomio di $\mathbb{K}[x]$, di grado $\leq (n-1)$, tale che $< f(x) > +r(x) =< f(x) > +s(x)$. Ne segue che $f(x)$ divide il polinomio $(r(x) - s(x))$, il cui grado è $\leq n-1$. Poichè i multipli non nulli di $f(x)$ hanno grado $\geq n$, si conclude che $r(x)-s(x)$ è il polinomio nullo, ossia $s(x) = r(x)$. ■

In particolare, se $\mathbb{K}$ è finito e $f(x)$ ha grado n:

$$\left|\frac{\mathbb{K}[x]}{< f(x) >}\right| = |\mathbb{K}|^n . \tag{2.9}$$

(2.10) Esempio $\left|\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}\right| = 2^2 = 4$. *Gli elementi dell'anello* $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}$ *sono:*

$$\langle x^2+x+1\rangle + 0 \qquad \langle x^2+x+1\rangle + 1$$
$$\langle x^2+x+1\rangle + x \qquad \langle x^2+x+1\rangle + x + 1.$$

Abbreviando $< f(x) > +r(x)$ *in* $r(x)$*, le tavole di somma e prodotto sono:*

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	1	x	x^2
1	1	x	x^2
x	x	x^2	1
x^2	x^2	1	x

.

(2.11) Definizione *Siano* A *un anello commutativo e* $I \neq A$ *un suo ideale.*

Si dice che:

- *I è primo se, per ogni $a, b \in A$: $(ab) \in I \Longrightarrow (a \in I$ oppure $b \in I)$;*
- *I è massimale se l'unico ideale che contiene propriamente I è A stesso.*

Per esempio l'ideale nullo $\{0\}$ è primo se e solo se A è privo di divisori dello zero. Più in generale si ha:

(2.12) Teorema *Sia $I \neq A$ un ideale di un anello commutativo A. L'anello quoziente $\frac{A}{I}$ è privo di divisori dello zero se e solo se I è primo.*

Dimostrazione.

Supponiamo I primo. Siano $I+a,\ I+b$ elementi di $\frac{A}{I}$ tali che $(I+a)(I+b) = I+0$. Ne segue $I + ab = I + 0$, ossia $(ab) \in I$. Per ipotesi, $a \in I$, oppure $b \in I$. Nel primo caso $I + a = I + 0$, nel secondo $I + b = I + 0$. Si conclude che $\frac{A}{I}$ è privo di divisori dello zero. Viceversa, supposto $\frac{A}{I}$ privo di divisori dello zero, siano $a, b \in A$ tali che $ab \in I$. Ne segue $(I+a)(I+b) = I+ab = I+0$. Per ipotesi, $I+a = I+0$ oppure $I+b = I+0$. Nel primo caso $a \in I$, nel secondo $b \in I$. Si conclude che I è primo. ■

Per il Teorema 1.6, in un campo $\mathbb{K}$ l'ideale nullo $\{0_{\mathbb{K}}\}$ è massimale. Più in generale:

(2.13) Teorema *Sia I un ideale di un anello commutativo A. L'anello quoziente $\frac{A}{I}$ è un campo se e solo se I è massimale.*

Dimostrazione.

Supponiamo $\frac{A}{I}$ campo. Poichè un campo ha almeno due elementi, $I \neq A$. Sia J un ideale di A tale che $I < J$. Scelto $j \in J \setminus I$, il laterale $I + j$ è diverso da $I + 0$ e ha quindi inverso $I + \overline{j}$. Da $(I + j)(I + \overline{j}) = I + 1_A$ si ha $I + j\overline{j} = I + 1_A$, ossia $\left(j\overline{j} - 1_A\right) \in I < J$. Notando che $j\overline{j} \in J$, si ottiene che $1_A = \left(j\overline{j} - \left(j\overline{j} - 1_A\right)\right) \in J$, da cui $J = A$ per (1.5). Si conclude che I è massimale.

Viceversa, supposto I massimale, dimostriamo che $\frac{A}{I}$ è un campo, ossia che ogni laterale $I + a \neq I + 0_A$ ha inverso. A tale scopo, consideriamo l'ideale principale Aa, generato da a, e l'ideale somma

$$J := I + Aa = \{i + xa \mid i \in I, x \in A\}.$$

Da $I \leq J$ e $a \in J \setminus I$ si deduce $I \neq J$, quindi $J = A$, per la massimalità di I. Ne segue $1_A \in J$. Esistono pertanto $\overline{i} \in I$ e $\overline{x} \in A$ tali che $1_A = \overline{i} + \overline{x}a$. Concludiamo $I + 1_A = I + \overline{x}a = (I + \overline{x})(I + a)$, ossia $I + \overline{x} = (I + a)^{-1}$. ■

3 Omomorfismi

Siano $A,\ B$ due anelli.

(3.1) Definizione *Un omomorfismo da A a B è una applicazione $f : A \to B$ tale che $f(1_A) = 1_B$ e, per ogni $a, b \in A$:*

1) $f(a + b) = f(a) + f(b)$;

2) $f(ab) = f(a)f(b)$.

Si noti che f è un omomorfismo dal gruppo $(A, +, 0_A)$ al gruppo $(B, +, 0_B)$, in virtù dell'assioma 1). In particolare: $f(0_A) = 0_B$ e $f(-a) = -f(a)$ per ogni $a \in A$. Poniamo:

$$\text{Ker } f := \{a \in A \mid f(a) = 0_B\}.$$

(3.2) Definizione *Un omomorfimo $f : A \to B$ si dice:*

- *un monomorfismo se è iniettivo;*
- *un epimorfismo se è suriettivo;*
- *un isomorfismo se è un monomorfismo e un epimorfismo.*

Conviene definire sottoanello di un anello R ogni sottogruppo S di $(R, +0_R)$ tale che $1_R \in S$ e, per ogni $r_1, r_2 \in S$, anche $r_1 r_2 \in S$.

(3.3) Teorema *Sia $f : A \to B$ un omomorfismo di anelli.*

1) *Per ogni sottoanello S di A, la sua immagine $f(S)$ è un sottoanello di B;*

2) *per ogni ideale I di B la sua preimmagine $f^{-1}(I)$ è un ideale di A;*

In particolare Im $f = f(A)$ *è un sottoanello di B e* Ker f *è un ideale di A.*

Dimostrazione.

1) $0_A \in S$, quindi $f(0_A) = 0_B \in f(S)$. Siano $f(s_1), f(s_2) \in f(S)$. Da $s_1,\ s_2 \in S$ segue $(s_1 - s_2) \in S$, quindi $f(s_1) - f(s_2) = f(s_1 - s_2) \in f(S)$. Pertanto $f(S)$ è un sottogruppo di $(B, +, 0_B)$. Inoltre $1_A \in S$ implica $f(1_A) = 1_B \in f(S)$. Sempre da $s_1,\ s_2 \in S$ segue $(s_1 s_2) \in S$. Pertanto $f(s_1)f(s_2) = f(s_1 s_2) \in f(S)$. Si conclude che $f(S)$ è un sottoanello.

2) In particolare I è un sottogruppo di $(B, +, 0_B)$. Da $f(0_A) = 0_B \in I$ segue $0_A \in f^{-1}(I)$. Siano $s_1, s_2 \in f^{-1}(I)$. Da $f(s_1),\ f(s_2) \in I$ segue che $f(s_1 - s_2) = (f(s_1) - f(s_2)) \in I$. Pertanto $(s_1 - s_2) \in f^{-1}(I)$. Abbiamo visto così che $f^{-1}(I)$ è un sottogruppo di $(A, +, 0_A)$. Per ogni $a \in A$ e per ogni $s \in f^{-1}(I)$ si ha $f(as) = f(a)f(s)$. Da $f(s) \in I$ segue $f(a)f(s) \in I$, ossia $f(as) \in I$. Pertanto $as \in f^{-1}(I)$. Analogamente si verifica che $sa \in f^{-1}(I)$. Concludiamo che $f^{-1}(I)$ è un ideale.

Infine, considerando il sottoanello $S = A$, si ha che Im $f = f(A)$ è un sottoanello di B, e considerando l'ideale $I = \{0_B\}$ si ha che la sua preimmagine Ker $f := f^{-1}(\{0_B\})$ è un ideale di A. ■

(3.4) Definizione

- *B si dice* immagine epimorfa *di A, se esiste un epimorfismo $f : A \to B$:*
- *A si dice* isomorfo *a B, e si scrive $A \sim B$, se esiste un isomorfismo $f : A \to B$.*

La relazione di isomorfismo fra anelli è riflessiva, simmetrica e transitiva. Dal punto di vista dell'algebra, anelli isomorfi sono identificati.

Le immagini epimorfe di un anello A sono, a meno di isomorfismi, tutti e soli i suoi anelli quoziente. Vale infatti il seguente:

(3.5) Teorema fondamentale sugli omomorfismi

1) *Siano I un ideale di A e $\frac{A}{I}$ il corrispondente anello quoziente. La proiezione canonica $\pi : A \to \frac{A}{I}$ definita ponendo*

$$\pi(a) := I + a$$

è un epimorfismo di anelli. Inoltre Ker $\pi = I$.

2) *Siano $f : A \to B$ un omomorfismo di anelli e $\pi : A \to \frac{A}{\text{Ker } f}$ la proiezione canonica. Allora f induce un unico isomorfismo di anelli*

$$\overline{f} : \frac{A}{\text{Ker } f} \to \text{Im } f$$

tale che $\overline{f}\pi = f$. In particolare

$$\frac{A}{\text{Ker } f} \sim \text{Im } f.$$

Dimostrazione.

1) π è un epimorfismo di gruppi additivi e Ker $\pi = I$, per il Teorema 7.7 di [4]. Inoltre $\pi(1_A) = I + 1_A$, unità moltiplicativa di $\frac{A}{I}$ e, per ogni $a, b \in A$:

$$\pi(ab) := I + (ab) = (I + a)(I + b) = \pi(a)\pi(b).$$

2) Sempre per il Teorema 7.7 di [4]. ponendo

$$\overline{f}\,(\text{Ker } f + a) := f(a)$$

si definisce un isomorfismo di gruppi additivi $\overline{f} : \frac{A}{\text{Ker } f} \to \text{Im } f$ che soddisfa la condizione $\overline{f}\pi = f$. Inoltre tale condizione determina univocamente $\overline{f}$.

Infine $\overline{f}\,(\text{Ker } f + 1_A) = f(1_A) = 1_B$ e

$$\overline{f}\,((\text{Ker } f + a)(\text{Ker } f + b)) = \overline{f}\,(\text{Ker } f + ab) = f(ab) = f(a)f(b).$$

Si conclude che $\overline{f}$ è un isomorfismo di anelli. ■

4 Esercizi

(4.1) Esercizio *In $\mathbb{Q}$ si calcoli l'ideale principale generato da 7.*

(4.2) Esercizio *In $\mathbb{R}$ si calcoli l'ideale principale generato da $\sqrt{5}$.*

(4.3) Esercizio *Sia I un ideale sinistro (destro) dell'anello A e sia $i \in I$. Si dimostri che se i è unitario, allora $I = A$.*

(4.4) Esercizio *Si dimostri che $7\mathbb{Z} := \{7z \mid z \in \mathbb{Z}\}$ è un ideale di $\mathbb{Z}$ e che è proprio.*

(4.5) Esercizio *Posto $< 7 >:= 7\mathbb{Z}$, si dimostri che la proiezione canonica $\pi : \mathbb{Z} \to \frac{\mathbb{Z}}{<7>}$ tale che $\pi(z) :=< 7 > +z$, è un epimorfismo di anelli, e si calcoli* Ker π.

(4.6) Esercizio *Verificare direttamente che:*

$$6\mathbb{Z} - 10 = 6\mathbb{Z} + 2, \quad 15\mathbb{Z} + 64 = 15\mathbb{Z} + 4, \quad 10\mathbb{Z} - 2 = 10\mathbb{Z} + 28.$$

(4.7) Esercizio *Si dimostri che $x\mathbb{Q}[x] := \{xf(x) \mid f(x) \in \mathbb{Q}[x]\}$ è un ideale di $\mathbb{Q}[x]$ e che è proprio.*

(4.8) Esercizio *Posto $< x >:= x\mathbb{Q}[x]$, si dimostri che la proiezione canonica*

$$\pi : \mathbb{Q}[x] \to \frac{\mathbb{Q}[x]}{< x >}$$

tale che $\pi\,(f(x)) :=< x > +f(x)$ è un epimorfismo di anelli, e si calcoli Ker π.

(4.9) Esercizio *Nell'anello $\mathbb{Q}[x]$, indicando con $< g(x) >$ l'ideale principale generato da $g(x)$, verificare direttamente che:*

$$\begin{aligned} < x^2 + 1 > + x^3 + 2x &= < x^2 + 1 > + x \\ < x^4 > + x^6 + x - 1 &= < x^4 > + x - 1 \\ < x - 1 > + x^2 - 1 &= < x - 1 > \quad . \end{aligned}$$

(4.10) Esercizio *Si scrivano gli elementi e le tavole di somma e prodotto degli anelli* $\mathbb{Z}_3$, $\mathbb{Z}_4$, $\mathbb{Z}_5$, $\mathbb{Z}_6$. *Per ciascuno di tali anelli si dica se sono campi.*

(4.11) Esercizio *Si scrivano gli elementi e le tavole di somma e prodotto dell'anello* $\frac{\mathbb{Z}_2[x]}{\langle x^2+1\rangle}$, *abbreviando* $\langle x^2+1\rangle + r(x)$ *in* $r(x)$. *Si dica se tale anello è un campo.*

(4.12) Esercizio *Si scrivano gli elementi e le tavole di somma e prodotto dell'anello* $\frac{\mathbb{Z}_3[x]}{\langle x^2+1\rangle}$. *Si dica se tale anello è un campo. In caso affermativo si indichi un generatore del gruppo moltiplicativo dei suoi elementi non nulli.*

Capitolo II

Dominii a ideali principali

1 Definizione ed esempi

Ricordiamo che, dato un anello A, l'insieme A^* degli elementi che hanno inverso moltiplicativo in A, è un gruppo rispetto al prodotto. Diciamo inoltre che A è un *dominio di integrità* se è commutativo e privo di divisori dello zero. Un elemento $b \in A$ *divide* $a \in A$, e si scrive $b|a$, se esiste $q \in A$ tale che $a = bq$. Per il Lemma 1.4, Capitolo IV di [4], la relazione "divide" in A è riflessiva e transitiva. D'altra parte, dati a, b non nulli

$$(a|b \text{ e } b|a) \Longleftrightarrow b = a\lambda,\ \lambda \in A^*. \tag{1.1}$$

Ricordiamo che, per il Lemma 1.3, l'ideale principale Aa, generato da a, è il minimo ideale di A al quale appartiene a.

(1.2) Lemma *Siano a, b due elementi non nulli di un dominio di integrità A.*

1) *$Aa \leq Ab$ se e solo se $b|a$;*

2) *$Aa = Ab$ se e solo se $b = \lambda a$, con $\lambda \in A^*$.*

In particolare $A = Ab$ se e solo se $b \in A^*$.

Dimostrazione.

1) Se $Aa \leq Ab$, si ha $a \in Ab$. Esiste quindi $q \in A$ tale che $a = qb$. Viceversa, se esiste $q \in A$ tale che $a = qb$, si ha: $Aa = A(qb) = (Aq)b \leq Ab$.

2) Se $Aa = Ab$ allora, per il punto precedente, $a|b$ e $b|a$. Da (1.1) segue $b = \lambda a$, con $\lambda \in A^*$. Viceversa se $b = \lambda a$, con $\lambda \in A^*$, si ha anche $a = \lambda^{-1}b$. Da $b = \lambda a$ si deduce $Ab \leq Aa$, da $a = \lambda^{-1}b$ si deduce $Aa \leq Ab$ e si conclude $Aa = Ab$.

L'ultima osservazione segue dal punto 2), con $a = 1_A$. ■

(1.3) Definizione *Un* dominio a ideali principali D *è un dominio di integrità in cui ogni ideale* I *è principale, ovvero esiste* $\bar{i} \in I$ *tale che* $I = D\bar{i}$.

(1.4) Teorema *Sia* I *un ideale non nullo di un dominio euclideo* D*, rispetto*

$$\varphi : D \setminus \{0_D\} \to \mathbb{N}$$

e sia n_0 *il minimo di* $\varphi(I \setminus \{0_D\})$*. Per ogni* $i_0 \in I \setminus \{0_D\}$ *tale che* $\varphi(i_0) = n_0$ *si ha*

$$I = Di_0.$$

In particolare ogni dominio euclideo è a ideali principali.

Dimostrazione. Da $i_0 \in I$ segue $Di_0 \leq I$ per definizione di ideale. Viceversa sia $i \in I$. Per definizione di dominio euclideo, esistono $q, r \in D$ tali che $i = i_0 q + r$, con $\varphi(r) < \varphi(i_0)$ oppure $r = 0_D$. Poichè $i_0 q \in I$, anche $r = (i - i_0 q) \in I$. Ne segue $r = 0_D$, da cui $i \in Di_0$.

In particolare abbiamo dimostrato che ogni ideale non nullo di D è principale. Chiaramente anche l'ideale $\{0_D\} = D0_D$ è principale. ■

In quanto dominii euclidei, i seguenti anelli sono dominii a ideali principali:

- l'anello $\mathbb{Z}$ dei numeri interi,
- ogni campo $\mathbb{K}$,
- l'anello $\mathbb{K}[x]$ dei polinomi a coefficienti in $\mathbb{K}$.

2 Fattorialità dei dominii a ideali principali

Ricordiamo che, in base alla Definizione 1.13 del Capitolo IV di [4]), un elemento $p \in D$, non nullo e non invertibile, è *irriducibile* se ha solo fattorizzazioni banali, ossia se, per ogni $a, b \in D$:

$$p = ab \implies (a \in D^* \text{ oppure } b \in D^*).$$

Scopo di questo paragrafo è dimostrare che ogni elemento non nullo di un dominio a ideali principali D si scrive, in modo essenzialmente unico, come prodotto di un numero finito di elementi irriducibili. Ossia che D è fattoriale, secondo la definizione 1.18, Capitolo IV di [4].

(2.1) Teorema *Due elementi* a, b *di un dominio a ideali principali* D *hanno sempre un massimo comun divisore* $d \in D$*. Inoltre* d *può essere scritto nella forma* $d = a\overline{x} + b\overline{y}$*, per opportuni* $\overline{x}, \overline{y} \in D$.

Dimostrazione. Considerati gli ideali principali Da e Db, generati rispettivamente da a e da b, sappiamo che la loro somma $Da + Db$ è un ideale. Esiste quindi $d \in Da + Db$ tale che $Da + Db = Dd$. In particolare:

$$d = \overline{x}a + \overline{y}b \quad \text{con } \overline{x}, \overline{y} \in D. \tag{2.2}$$

Da $Da \leq Da + Db = Dd$ segue $Da \leq Dd$, ossia $d|a$. Analogamente $d|b$. Infine sia $c \in D$ un divisore comune di a e di b. Sostituendo $a = \overline{a}c$, $b = \overline{b}c$ $(\overline{a}, \overline{b} \in D)$ nella relazione (2.2), si ottiene $d = c(\overline{x}\overline{a} + \overline{y}\overline{b})$, ovvero $c|d$. Si conclude che $d = \text{M.C.D.}(a, b)$. ■

Per il Corollario 2.6 e il Lemma 3.1 del Capitolo *IV* di [4] si ha allora:

(2.3) Lemma *In un dominio a ideali principali, un elemento è irriducibile se e solo se è primo.*

(2.4) Teorema *In un dominio a ideali principali D ogni catena ascendente di ideali $I_1 < I_2 < \ldots < I_k < \ldots$ è finita.*

Dimostrazione.

Si verifica facilmente che l'unione insiemistica $I := \cup_j I_j$ di tutti gli ideali della catena è un ideale. Esiste quindi $d \in I$ tale che $I = Dd$. Chiaramente d appartiene a un ideale I_n della catena, per qualche indice n. Ne segue $I \leq I_n$ da cui $I = I_n$. Pertanto I_n è l'ultimo ideale della catena. ■

(2.5) Corollario *Ogni dominio a ideali principali D è fattoriale.*

Dimostrazione.

1) Ogni elemento unitario è prodotto di 0 irriducibili. Ogni elemento irriducibile, è prodotto di 1 irriducibile (se stesso !). Sia ora a un elemento riducibile, e sia $a = a_1 a_2$ una sua fattorizzazione non banale in D, ossia $a_1 \notin D^*$, $a_2 \notin D^*$. In virtù del Lemma 1.2 si ottiene l' inclusione propria di ideali:

$$Da < Da_1.$$

Se a_1 è riducibile, possiamo inserire un nuovo ideale nella catena. Infatti, considerata una fattorizzazione non banale $a_1 = b_1 b_2$ in D, otteniamo

$$Da < Da_1 < Db_1.$$

In virtù del Teorema 2.4, il procedimento di inserzione di ideali ha termine dopo un numero finito di iterazioni. Si perviene a un fattore irriducibile p_1 di a. Posto $a = p_1q_1$, per il ragionamento precedente q_1 deve avere un fattore irriducibile p_2. Posto $q_1 = p_2q_2$ si ha $Da < Dq_1 < Dq_2$. Per il Teorema 2.4 il procedimento ha termine, ossia a è prodotto di un numero finito, ≥ 2, di elementi irriducibili.

2) L'essenziale unicità della fattorizzazione di un elemento si basa sul fatto che ogni elemento irriducibile è primo. Si dimostra in modo analogo a quanto fatto nel Teorema 3.2 Capitolo *IV* di [4]. L'induzione su φ va sostituita con l'induzione su $k = k(a)$, dove $k(a)$ rappresenta il minimo numero dei fattori di ogni fattorizzazione di $a \in A$. ■

3 Ideali massimali nei dominii a ideali principali

(3.1) Teorema *Siano D un dominio a ideali principali e p un suo elemento non nullo.*

1) *L'ideale Dp è massimale se e solo se p è irriducibile;*

2) *l'anello quoziente $\frac{D}{Dp}$ è un campo se e solo se p è irriducibile.*

Dimostrazione.

1) Supponiamo Dp massimale. Se p, per assurdo, fosse riducibile, ammetterebbe una fattorizzazione non banale $p = ab$, ossia $a \notin D^*$, $b \notin D^*$. In virtù del Lemma 1.2 si avrebbe $Dp < Da < D$, in contrasto con l'ipotesi Dp massimale. Viceversa, supponiamo p irriducibile. Per assurdo, sia I un ideale di D tale che $Dp < I < D$. Essendo I principale, esiste $\bar{i} \in I$ tale che $I = D\bar{i}$. Da $Dp < D\bar{i}$ segue che $\bar{i}$ divide p. Per l'irriducibilità di p si ha $p = \lambda\bar{i}$ con $\lambda \in D^*$. Si conclude $Dp = D\bar{i}$, contraddizione con l'ipotesi $Dp < I = D\bar{i}$.

2) Per il Teorema 2.13 del Capitolo I, l'anello quoziente $\frac{D}{Dp}$ è un campo se e solo se l'ideale Dp è massimale. Dal punto precedente segue l'asserto. ■

Di conseguenza, indicando con $< d >$ l'ideale principale Dd:

- l'anello $\mathbb{Z}_n = \frac{\mathbb{Z}}{<n>}$ è un campo se e solo se n è primo;
- l'anello $\frac{\mathbb{K}[x]}{<f(x)>}$ è un campo se e solo se $f(x)$ è irriducibile.

(3.2) Esempio *$\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ sono campi, di rispettivi ordini:* $2, 3, 5, 7, 11$.

(3.3) Esempio $\frac{\mathbb{Z}_2[x]}{\langle x^2+x+1\rangle}$ *(si veda esempio* 2.10 *del Capitolo I) è un campo con* 4 *elementi. Esso è detto* campo di Galois *di ordine* 4 *e viene indicato con* $\mathbb{F}_4$.

(3.4) Teorema *(di Fermat) Per ogni primo p e per ogni $a \in \mathbb{Z}$, non divisibile per p:*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dimostrazione.

$\mathbb{Z}_p$ è un campo con p elementi. Il suo gruppo moltiplicativo $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]_p\}$ ha quindi ordine $p-1$ e, per il Teorema di Lagrange, ogni suo elemento ha periodo che divide $p-1$. Ne segue che, per ogni intero a, non divisibile per p, si ha $([a]_p)^{p-1} = [1]_p$, ossia $a^{p-1} \equiv 1 \pmod{p}$. ■

(3.5) Esempio

$37^{70} \equiv 1 \pmod{71}$,

$48^{96} \equiv 1 \pmod{97}$.

4 Il Teorema cinese del resto

Sia Dd l'ideale principale generato da $d \in D$. In conformità con (2.1) del Capitolo 1, per ogni $a, a' \in A$ si ha

$$a \equiv a' \pmod{Dd} \iff (a - a') \in Dd \iff d|(a - a').$$

D'ora in poi, anzichè scrivere $a \equiv a' \pmod{Dd}$, scriveremo più semplicemente

$$a \equiv a' \pmod{d}$$

in analogia con le notazioni usate quando $D = \mathbb{Z}$.

Per il Lemma 2.3 del Capitolo I la congruenza $\pmod{d}$ è una relazione di equivalenza in D, compatibile con somma e prodotto. Ossia:

$$\begin{cases} a \equiv a' \pmod{d} \\ b \equiv b' \pmod{d} \end{cases} \Longrightarrow \begin{cases} a + b \equiv a' + b' \pmod{d} \\ ab \equiv a'b' \pmod{d} \end{cases}$$

(4.1) Definizione *Siano $a, b, d \in D$. Una* soluzione *della* congruenza lineare

$$ax \equiv b \pmod{d} \tag{4.2}$$

è un elemento $c \in D$ tale che $ac \equiv b \pmod{d}$.

(4.3) Teorema *(cinese del resto) Siano $d_1, \ldots, d_n$ elementi a due a due coprimi di un dominio a ideali principali D. Scelti comunque $b_1, \ldots, b_n \in D$, esistono in D soluzioni del sistema di congruenze lineari*

$$\left\{ \begin{array}{ccc} x \equiv b_1 & \pmod{d_1} \\ \ldots & \ldots \\ x \equiv b_n & \pmod{d_n}. \end{array} \right. \tag{4.4}$$

Detta c una soluzione, le altre sono tutti e soli gli elementi $c' \in D$ tali che

$$c' \equiv c \pmod{\prod_{\ell=1}^{n} d_\ell}.$$

Dimostrazione.

Per $1 \leq i \leq n$, poniamo $t_i := \prod_{\ell \neq i} d_\ell$. Risulta

$$\text{M.C.D.}(t_i, d_i) = 1_D, \quad 1 \leq i \leq n.$$

Infatti se fosse, ad esempio, $M.C.D.(t_1, d_1) \neq 1_D$, esisterebbe un primo p che divide sia t_1 sia d_1. Ne segue che p dovrebbe dividere uno dei fattori di $t_1 = d_2 \cdots d_n$. A meno dell'ordine possiamo supporre che $p | d_2$, in contrasto con l'ipotesi $\text{M.C.D.}(d_2, d_1) = 1_D$.

Per $1 \leq i \leq n$, esistono pertanto $y_i, z_i \in D$ tali che $t_i y_i + d_i z_i = 1_D$.

Ne segue :

$$\begin{array}{lll} t_i y_i \equiv 1_D & \pmod{d_i} & 1 \leq i \leq n \\ t_j y_j \equiv 0_D & \pmod{d_i} & 1 \leq i \neq j \leq n \ . \end{array} \tag{4.5}$$

Posto

$$c = \sum_{j=1}^{n} t_j y_j b_j,$$

verifichiamo che c è soluzione di (4.4). Infatti, fissato un qualunque indice i, si ha :

$$c = t_i y_i b_i + \sum_{j \neq i} t_j y_j b_j \ \equiv \ b_i \pmod{d_i}.$$

Determiniamo ora le altre soluzioni, ponendo $d = \prod_1^n d_\ell$. Sia $c' \equiv c \pmod{d}$. Ne segue $c' \equiv c \pmod{d_i}$ per $i \leq n$, quindi c' è soluzione del sistema. Viceversa, sia $\overline{x} \in D$ una soluzione di (4.4). Si ha $\overline{x} \equiv b_i \equiv c \pmod{d_i}$ per $1 \leq i \leq n$. In altre parole d_i divide $(\overline{x} - c)$ per $1 \leq i \leq n$. Si conclude che $\text{m.c.m.}(d_1, \ldots, d_n) = d$ divide $(\overline{x} - c)$, ossia che $\overline{x} \equiv c \pmod{d}$. ■

5 La decomposizione primaria

Dati due anelli A e B, il loro prodotto cartesiano

$$A \times B := \left\{ \begin{pmatrix} a \\ b \end{pmatrix} \mid a \in A,\ b \in B \right\}$$

risulta un anello rispetto alle operazioni definite ponendo:

$$\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} := \begin{pmatrix} a_1 + a_2 \\ b_1 + b_2 \end{pmatrix}, \quad \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} := \begin{pmatrix} a_1 a_2 \\ b_1 b_2 \end{pmatrix}. \tag{5.1}$$

La verifica è lasciata per esercizio.

(5.2) Definizione *Il precedente anello si dice la* somma diretta *di A e B e si indica con $A \oplus B$.*

(5.3) Teorema *Sia D un dominio a ideali principali e siano $d, d_1, d_2 \in D$ tali che $d = d_1 d_2$ con M.C.D.$(d_1, d_2) = 1_D$. Allora:*

$$\frac{D}{Dd} \ \sim \ \frac{D}{Dd_1} \oplus \frac{D}{Dd_2}.$$

Dimostrazione.

Consideriamo l'applicazione $f : D \to \frac{D}{Dd_1} \oplus \frac{D}{Dd_2}$ definita ponendo, per ogni $a \in D$:

$$f(a) := \begin{pmatrix} Dd_1 + a \\ Dd_2 + a \end{pmatrix}.$$

Si ha che $f(1_D) := \begin{pmatrix} Dd_1 + 1_D \\ Dd_2 + 1_D \end{pmatrix}$ è l' unità moltiplicativa di $\frac{D}{Dd_1} \oplus \frac{D}{Dd_2}$.

Inoltre, per ogni $a, b \in D$:

$$f(a+b) := \begin{pmatrix} Dd_1 + a + b \\ Dd_2 + a + b \end{pmatrix} = \begin{pmatrix} Dd_1 + a \\ Dd_2 + a \end{pmatrix} + \begin{pmatrix} Dd_1 + b \\ Dd_2 + b \end{pmatrix} = f(a) + f(b).$$

$$f(ab) := \begin{pmatrix} Dd_1 + ab \\ Dd_2 + ab \end{pmatrix} = \begin{pmatrix} Dd_1 + a \\ Dd_2 + a \end{pmatrix} \begin{pmatrix} Dd_1 + b \\ Dd_2 + b \end{pmatrix} = f(a) f(b).$$

Pertanto f è un omomorfismo di anelli.

Verifichiamo ora che Ker $f = Dd$. Infatti $a \in$ Ker f se e solo se

$$\begin{cases} Dd_1 + a = Dd_1 \\ Dd_2 + a = Dd_2 \end{cases} \iff a \in Dd_1 \cap Dd_2 = Dd.$$

Infine f è suriettiva per il Teorema cinese del resto. A tale scopo, notiamo che l' elemento

$$\begin{pmatrix} Dd_1 + b_1 \\ Dd_2 + b_2 \end{pmatrix}$$

del codominio, ha come preimmagine in D una qualunque soluzione c del sistema

$$\begin{cases} x \equiv b_1 & (\text{mod } d_1) \\ x \equiv b_2 & (\text{mod } d_2) \end{cases}.$$

Infatti:

$$f(c) = \begin{pmatrix} Dd_1 + c \\ Dd_2 + c \end{pmatrix} = \begin{pmatrix} Dd_1 + b_1 \\ Dd_2 + b_2 \end{pmatrix}.$$

Per il Teorema fondamentale degli omomorfismi, f induce un isomorfismo

$$\overline{f} : \frac{D}{Dd} \ \to \ \frac{D}{Dd_1} \oplus \frac{D}{Dd_2}.$$

■

(5.4) Corollario *Sia $d = p_1^{m_1} \dots p_n^{m_n}$ una fattorizzazione di d, dove $p_1, \dots, p_n$ sono $n \geq 2$ elementi irriducibili di D, a due a due coprimi (non associati). Allora*

$$\frac{D}{Dd} \ \sim \ \frac{D}{Dp_1^{m_1}} \oplus \dots \oplus \frac{D}{Dp_n^{m_n}} \quad \text{(decomposizione primaria)}. \tag{5.5}$$

Dimostrazione. Ragioniamo per induzione su n, ponendo $d_1 = p_1^{m_1}$, $d_2 = p_2^{m_2} \dots, p_n^{m_n}$. Dall'ipotesi che i p_i sono a due a due coprimi, segue che M.C.D.$(d_1, d_2) = 1_D$. Pertanto, per il Teorema 5.3, si ha

$$\frac{D}{Dd} \ \sim \ \frac{D}{Dp_1^{m_1}} \oplus \frac{D}{D\left(p_2^{m_2} \dots, p_n^{m_n}\right)}.$$

Per $n = 2$ l'asserto si ottiene direttamente. Per $n > 2$ l'asserto si ottiene per induzione. (Conviene tener presenti gli Esercizi 6.15 e 6.16). ■

(5.6) Esempio $\mathbb{Z}_{300} \ \sim \ \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25}$.

(5.7) Esempio $\frac{\mathbb{Q}[x]}{\langle x^2-1 \rangle} \sim \frac{\mathbb{Q}[x]}{\langle x-1 \rangle} \oplus \frac{\mathbb{Q}[x]}{\langle x+1 \rangle}$.

6 Esercizi

(6.1) Esercizio *Si verifichi che*

$$\begin{cases} a \equiv a' & (\text{mod } d) \\ b \equiv b' & (\text{mod } d) \end{cases} \implies \begin{cases} a + b \equiv a' + b' & (\text{mod } d) \\ ab \equiv a'b' & (\text{mod } d) \end{cases}$$

(6.2) Esercizio *Si dimostri che le congruenze* $x \equiv 8 \pmod 5$ *e* $x \equiv 23 \pmod 5$ *sono equivalenti, ossia hanno le stesse soluzioni in* $\mathbb{Z}$.

(6.3) Esercizio *Si dimostri che le congruenze*

$$X \equiv x+1 \pmod{x^2+4}, \quad X \equiv 3x^3 - x^2 + 13x - 3 \pmod{x^2+4}$$

sono equivalenti, ossia hanno le stesse soluzioni in $\mathbb{Q}[x]$.

(6.4) Esercizio *Si determinino tutte le soluzioni intere del sistema*

$$\begin{cases} x \equiv 3 & \pmod 5 \\ x \equiv 0 & \pmod 7. \end{cases} \tag{6.5}$$

(6.6) Esercizio *Si determinino tutte le soluzioni intere del sistema*

$$\begin{cases} x \equiv 1 & \pmod{14} \\ x \equiv -1 & \pmod{15} \\ x \equiv 4 & \pmod{11}. \end{cases} \tag{6.7}$$

(6.8) Esercizio *In* $\mathbb{Q}[x]$ *si determinino tutte le soluzioni del sistema*

$$\begin{cases} X \equiv 2x & \pmod{x^2-1} \\ X \equiv 2x & \pmod{x^2+1}. \end{cases} \tag{6.9}$$

(6.10) Esercizio *In* $\mathbb{Q}[x]$ *si determinino tutte le soluzioni del sistema*

$$\begin{cases} X \equiv 0 & \pmod{x+2} \\ X \equiv x+1 & \pmod{x^4+3}. \end{cases} \tag{6.11}$$

(6.12) Esercizio *Si calcoli l'ordine e la decomposizione primaria di ciascuno dei seguenti anelli*

$$\mathbb{Z}_{15}, \quad \mathbb{Z}_{45}, \quad \mathbb{Z}_{15} \oplus \mathbb{Z}_{45}, \quad \mathbb{Z}_{28} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{135}.$$

(6.13) Esercizio *Si trovi la decomposizione primaria dei seguenti anelli*

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

(6.14) Esercizio *Si calcoli l'ordine e la decomposizione primaria di ciascuno dei seguenti anelli*

$$\frac{\mathbb{Z}_3[x]}{\langle x^3\rangle}, \quad \frac{\mathbb{Z}_5[x]}{\langle x^2+1\rangle}, \quad \frac{\mathbb{Z}_2[x]}{\langle x^3+x+1\rangle}.$$

(6.15) Esercizio *Siano A, B, C anelli. Si dimostri che $A \oplus (B \oplus C) \sim (A \oplus B) \oplus C$.*

(6.16) Esercizio *Siano A, B, A', B' anelli, con $A \sim A'$, $B \sim B'$. Si dimostri che $A \oplus B \sim A' \oplus B'$.*

(6.17) Esercizio *Siano A, B anelli. Si dimostri che $A \oplus B \sim B \oplus A$.*

Capitolo III

Matrici

In questo capitolo R indica un anello commutativo.

1 Operazioni sulle matrici

Per ogni $m, n \geq 1$, indichiamo con $\mathrm{Mat_{m,n}(R)}$ l'insieme delle matrici $m \times n$ a elementi in R. Se $n = m$, tale insieme si indica anche con $\mathrm{Mat_n(R)}$. Se $C = (c_{ij}) \in \mathrm{Mat_{m,n}(R)}$, la sua *trasposta* C^t è la matrice le cui righe sono le colonne di C. Quindi $C^t = (c_{ji}) \in \mathrm{Mat_{n,m}(R)}$. La somma e il prodotto in R inducono, in modo naturale, le seguenti operazioni *componente per componente* fra matrici di $\mathrm{Mat_{m,n}(R)}$. Precisamente, per ogni:

$$C = \begin{pmatrix} c_{11} & \dots & c_{1n} \\ \dots & \dots & \dots \\ c_{m1} & \dots & c_{mn} \end{pmatrix}, \quad D = \begin{pmatrix} d_{11} & \dots & d_{1n} \\ \dots & \dots & \dots \\ d_{m1} & \dots & d_{mn} \end{pmatrix},$$

e per ogni $r \in R$, si pone

$$C + D := \begin{pmatrix} c_{11} + d_{11} & \dots & c_{1n} + d_{1n} \\ \dots & \dots & \dots \\ c_{m1} + d_{m1} & \dots & c_{mn} + d_{mn} \end{pmatrix}, \quad rC := \begin{pmatrix} rc_{11} & \dots & rc_{1n} \\ \dots & \dots & \dots \\ rc_{m1} & \dots & rc_{mn} \end{pmatrix}. \tag{1.1}$$

Si definisce il prodotto di un elemento di $\mathrm{Mat_{1,s}(R)}$ per un elemento di $\mathrm{Mat_{s,1}(R)}$, ossia di un *vettore riga* per un *vettore colonna* con s componenti, mediante:

$$\begin{pmatrix} a_1 & \dots & a_s \end{pmatrix} \begin{pmatrix} b_1 \\ \dots \\ b_s \end{pmatrix} := a_1 b_1 + \cdots + a_s b_s = \sum_{k=1}^{s} a_k b_k. \tag{1.2}$$

Questo consente di definire il prodotto *righe per colonne* di due matrici

$$A = (a_{ij}) \in \mathrm{Mat_{m,s}(R)}, \quad \mathrm{B} = (\mathrm{b_{ij}}) \in \mathrm{Mat_{s,n}(R)}$$

come la matrice $AB \in \mathrm{Mat_{m,n}(R)}$, la cui componente di posto (i,j) è il prodotto della riga i-esima di A per la colonna j-esima di B. In simboli:

$$AB = \left(\sum_{k=1}^{s} a_{ik} b_{kj} \right). \tag{1.3}$$

Segue facilmente che $(AB)^t = B^t A^t$.

Per semplificare le notazioni converrà scrivere 0 per 0_R e 1 per 1_R.

In $\mathrm{Mat_{s,1}(R)}$, consideriamo i vettori colonna:

$$e_1 := \begin{pmatrix} 1 \\ 0 \\ \dots \\ 0 \end{pmatrix},\ e_2 := \begin{pmatrix} 0 \\ 1 \\ \dots \\ 0 \end{pmatrix},\ \dots\ ,\ e_s := \begin{pmatrix} 0 \\ 0 \\ \dots \\ 1 \end{pmatrix}. \tag{1.4}$$

Per ogni $A \in \mathrm{Mat_{m,s}(R)}$, la sua prima colonna coincide con Ae_1, la seconda con Ae_2, ecc... Quindi, suddividendo A nelle sue colonne:

$$A = \left(\begin{array}{c|c|c} Ae_1 & \dots & Ae_s \end{array} \right).$$

Analogamente, suddividendo B nelle sue righe:

$$B = \left(\begin{array}{c} e_1^t B \\ \hline \dots \\ \hline e_s^t B \end{array} \right).$$

Si noti che le colonne di AB sono combinazione lineare di quelle di A. Precisamente:

$$AB = \left(\begin{array}{c|c|c} b_{11}\,(Ae_1) + \ \dots\dots\ + b_{s1}\,(Ae_s) & \dots & b_{1n}\ (Ae_1) + \ \dots\dots\ + b_{sn}\ (Ae_s) \end{array} \right).$$

Analogamente le righe di AB sono combinazione lineare di quelle di B. Precisamente:

$$AB = \left(\begin{array}{c} a_{11}\left(e_1^t B\right) + \dots + a_{1s}\left(e_s^t B\right) \\ \hline \dots\dots \\ \hline a_{m1}\left(e_1^t B\right) + \dots + a_{ms}\left(e_s^t B\right) \end{array} \right).$$

(1.5) Esempio

$$A = \begin{pmatrix} 3 & -1 & 0 \\ 4 & 0 & 2 \end{pmatrix},\ B = \begin{pmatrix} 2 & 2 \\ 3 & -1 \\ 4 & 6 \end{pmatrix},\ AB = \begin{pmatrix} 3 & 7 \\ 16 & 20 \end{pmatrix}.$$

$A = \left(\begin{array}{c|c|c} 3 & -1 & 0 \\ 4 & 0 & 2 \end{array}\right) = \left(\begin{array}{c|c|c} Ae_1 & Ae_2 & Ae_3 \end{array}\right)$, *infatti:*

$$A\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \end{pmatrix}, \quad A\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \quad A\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix}.$$

$$B = \left(\begin{array}{cc} 2 & 2 \\ \hline 3 & -1 \\ \hline 4 & 6 \end{array}\right) = \left(\begin{array}{c} e_1^tB \\ \hline e_2^tB \\ \hline e_3^tB \end{array}\right), \text{ infatti:}$$

$$\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} B = \begin{pmatrix} 2 & 2 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} B = \begin{pmatrix} 3 & -1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} B = \begin{pmatrix} 4 & 6 \end{pmatrix}.$$

$$AB = \left(\begin{array}{c|c} 3 & 7 \\ 16 & 20 \end{array}\right) = \left(\begin{array}{c|c} 2Ae_1 + 3Ae_2 + 4Ae_3 & 2Ae_1 - Ae_2 + 6Ae_3 \end{array}\right) =$$

$$\left(\begin{array}{cc} 3 & 7 \\ \hline 16 & 20 \end{array}\right) = \left(\begin{array}{c} 3\left(e_1^tB\right) - \left(e_2^tB\right) + 0\left(e_3^tB\right) \\ \hline 4\left(e_1^tB\right) + 0\left(e_2^tB\right) + 2\left(e_3^tB\right) \end{array}\right).$$

Infine:

$$B^tA^t = \begin{pmatrix} 2 & 3 & 4 \\ 2 & -1 & 6 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ -1 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 16 \\ 76 & 20 \end{pmatrix} = (AB)^t.$$

Spesso è utile eseguire il prodotto di matrici *a blocchi*, con le regole fornite dal

(1.6) Teorema *Date* $A \in \mathrm{Mat}_{\mathrm{m,s}}(\mathrm{R})$, $B \in \mathrm{Mat}_{\mathrm{s,n}}(\mathrm{R})$ *e fissate delle partizioni*

$$m = m_1 + m_2,\ s = s_1 + s_2,\ n = n_1 + n_2$$

si suddividano A *e* B *in blocchi*

$$A = \begin{pmatrix} A_1 & A_2 \\ A_3 & A_4 \end{pmatrix}, \quad B = \begin{pmatrix} B_1 & B_2 \\ B_3 & B_4 \end{pmatrix}$$

dove A_1, A_2, A_3 *e* A_4 *hanno rispettivamente ordini* $m_1 \times s_1$, $m_1 \times s_2$, $m_2 \times s_1$, $m_2 \times s_2$; B_1, B_2, B_3 *e* B_4 *hanno rispettivamente ordini* $s_1 \times n_1$, $s_1 \times n_2$, $s_2 \times n_1$ *e* $s_2 \times n_2$. *Allora:*

$$AB = \begin{pmatrix} A_1B_1 + A_2B_3 & A_1B_2 + A_2B_4 \\ A_3B_1 + A_4B_3 & A_3B_2 + A_4B_4 \end{pmatrix}.$$

Tale regola è utile soprattutto quando qualcuno dei blocchi A_i oppure B_i è nullo.

(1.7) Esempio

$$\begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}\begin{pmatrix} Z & 0 \\ 0 & T \end{pmatrix} = \begin{pmatrix} XZ & 0 \\ 0 & YT \end{pmatrix}$$

(1.8) Esempio

$$\begin{pmatrix} X & 0 \\ U & Y \end{pmatrix}\begin{pmatrix} Z & 0 \\ V & T \end{pmatrix} = \begin{pmatrix} XZ & 0 \\ UZ+YV & YT \end{pmatrix}.$$

(1.9) Esempio *Chiamiamo* $v_1 = Be_1, \cdots, v_n = Be_n$ *le colonne di una matrice* $B \in \mathrm{Mat_{s,n}(R)}$. *Per ogni* $A \in \mathrm{Mat_{m,s}(R)}$ *si ha* $AB = A\,(v_1|\cdots|v_n) = (Av_1|\cdots|Av_n)$.

Le proprietà delle operazioni fra matrici sono riassunte dal seguente Teorema, la cui dimostrazione è basata sul calcolo diretto.

(1.10) Teorema

1) $\mathrm{Mat_{m,n}(R)}$ *è un gruppo abeliano rispetto alla somma di matrici;*

2) $\mathrm{Mat_{n}(R)}$ *è un anello rispetto alla somma e al prodotto di matrici;*

3) *per ogni* $A, A_1,\ A_2 \in \mathrm{Mat_{m,s}(R)}$, $B, B_1,\ B_2 \in \mathrm{Mat_{s,n}(R)}$, $C \in \mathrm{Mat_{n,\ell}(R)}$*:*

- $(A_1 + A_2)\,B = A_1B + A_2B$*;*
- $A\,(B_1 + B_2) = AB_1 + AB_2$*;*
- $(AB)C = A(BC)$.

2 Il gruppo $\mathrm{GL_2(R)}$ e alcuni suoi sottogruppi

(2.1) Definizione *Data* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat_2(R)}$, *poniamo:*

$$\det A := ad - bc \quad \text{(determinante di } A\text{)}.$$

Un calcolo diretto mostra che, per ogni $A, B \in \mathrm{Mat_2(R)}$, si ha:

$$\det(AB) = (\det A)(\det B).$$

(2.2) Lemma *Il gruppo* $\mathrm{Mat_2(R)^*}$ *delle matrici che hanno inversa in* $\mathrm{Mat_2(R)}$ *è costituito dalle matrici il cui determinante appartiene a* R^**, ossia ha inverso in* R.

Dimostrazione. Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat_2(R)}$.

Se $ad - bc$ ha inverso $\rho \in R$, allora la matrice

$$\begin{pmatrix} d\rho & -b\rho \\ -c\rho & a\rho \end{pmatrix} \in \mathrm{Mat_2(R)}$$

e si verifica direttamente che è inversa di A. Viceversa, se A ha inversa, da $AA^{-1} = I$ segue $(\det A)(\det A^{-1}) = \det I = 1_R$. Si conclude che $\det(A^{-1})$ è l'inverso di $\det A$. ∎

(2.3) Definizione $\mathrm{Mat}_2(\mathrm{R})^*$ *si dice il* gruppo generale lineare *di grado* 2 *su* R *e si indica con* $\mathrm{GL}_2(\mathrm{R})$.

Analizziamo ora alcuni sottogruppi di tale gruppo.

(2.4) Lemma *L'insieme delle* matrici di permutazione*:*

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

è un sottogruppo di $\mathrm{GL}_2(\mathrm{R})$*, isomorfo al gruppo simmetrico* $\mathrm{Sym}(2)$.

(2.5) Lemma *Le matrici della forma*

$$\left\{ \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \mid r \in R \right\}$$

formano un sottogruppo di $\mathrm{GL}_2(\mathrm{R})$*, isomorfo al gruppo additivo* $(R, +, 0)$.

Dimostrazione.

L'applicazione $f : R \to \mathrm{GL}_2(\mathrm{R})$ tale che, per ogni $r \in R$:

$$r \mapsto \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

è un monomorfismo di gruppi. Infatti:

$$f(r_1 + r_2) = \begin{pmatrix} 1 & 0 \\ r_1 + r_2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ r_1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ r_2 & 1 \end{pmatrix} = f(r_1) f(r_2).$$

■

Conviene introdurre la seguente notazione:

(2.6)

$$E_{11} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad E_{12} := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad E_{21} := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad E_{22} := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

In tal modo, il sottogruppo del Teorema 2.5 si denota mediante:

$$\{I + rE_{21} \mid r \in R\}.$$

Tale sottogruppo e il suo trasposto $\{I + rE_{12} \mid r \in R\}$ è si dicono *sottogruppi radicali.*

(2.7) Lemma *Le matrici diagonali del tipo:*

$$\left\{ \begin{pmatrix} \nu_1 & 0 \\ 0 & \nu_2 \end{pmatrix} \mid \nu_i \in R^* \right\}$$

costituiscono un sottogruppo di $\mathrm{GL}_2(\mathrm{R})$*, detto* diagonale.

3 Il gruppo $\mathrm{GL_n(R)}$ e alcuni suoi sottogruppi

(3.1) Definizione *Il gruppo* $\mathrm{Mat_n(R)^*}$ *delle matrici invertibili di* $\mathrm{Mat_n(R)}$ *si dice il* gruppo generale lineare *di grado n su R. Lo si indica abitualmente con* $\mathrm{GL_n(R)}$.

Si noti che, per ogni $A, B \in \mathrm{GL_n(R)}$:

$$(AB)^{-1} = B^{-1}A^{-1}. \tag{3.2}$$

(3.3) Lemma *Sia H un sottogruppo di* $\mathrm{GL_n(R)}$. *Allora*

$$H^t := \left\{h^t \mid h \in H\right\}$$

è un sottogruppo di $\mathrm{GL_n(R)}$, *isomorfo ad H.*

Dimostrazione.

L'applicazione $h \mapsto \left(h^{-1}\right)^t$ è un isomorfismo. Infatti:
$\left((hk)^{-1}\right)^t = \left(k^{-1}h^{-1}\right)^t = \left(h^{-1}\right)^t \left(k^{-1}\right)^t$. ■

Prenderemo ora in considerazione alcuni sottogruppi notevoli di $\mathrm{GL_n(R)}$.

A tale scopo ricordiamo che il gruppo delle applicazioni bijettive dell'insieme $\{1, \cdots, n\}$ in sè si indica con Sym(n) e si chiama il gruppo *simmetrico* di grado n. Esso ha ordine $n!$ e i suoi elementi si dicono anche *permutazioni.*

(3.4) Esempio $\mathrm{Sym}(2) = \{\mathrm{id}, (12)\}$.

(3.5) Esempio $\mathrm{Sym}(3) = \{\mathrm{id}, (123), (132), (23), (13), (12)\}$.

Per ogni permutazione $\sigma \in \mathrm{Sym(n)}$, definiamo la matrice *di permutazione* π_σ le cui colonne sono, ordinatamente, i vettori $e_{\sigma(1)}, \ldots, e_{\sigma(n)}$. Per esempio, per $n = 2$, le matrici in 2.4 sono π_{id} e $\pi_{(12)}$. D'altra parte, per $n = 3$:

$$\pi_{(123)} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \quad \pi_{(12)} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Notando che $e_i^t e_j = 0_R$ se $i \neq j$ e che $e_i^t e_i = 1_R$ si ha che, per ogni σ:

$${\pi_\sigma}^t = {\pi_\sigma}^{-1}. \tag{3.6}$$

Chiaramente l'applicazione $\sigma \mapsto \pi_\sigma$ è un monomorfismo da Sym(n) a $\mathrm{GL_n(R)}$. Quindi:

(3.7) Proposizione *Le matrici di permutazione costituiscono un sottogruppo di* $\mathrm{GL_n(R)}$, *isomorfo a* $\mathrm{Sym(n)}$.

Per ogni i, j indichiamo con E_{ij} la matrice con 1_R nella posizione (i, j) e 0_R altrove.

(3.8) Proposizione *Fissati $i \neq j$, le matrici*

$$\{I + rE_{ij} \mid r \in R\}$$

formano un sottogruppo di $\mathrm{GL_n(R)}$, *detto* radicale, *isomorfo al gruppo additivo di R.*

Dimostrazione.

L'applicazione $f_{ij} : (R, +, 0) \to \mathrm{GL_n(R)}$ tale che $r \mapsto I + rE_{ij}$ è un monomorfismo di gruppi. ■

(3.9) Proposizione *Fissata una partizione $n = h + k$, le matrici della forma:*

$$\left\{ \begin{pmatrix} I_h & 0 \\ V & I_k \end{pmatrix} \mid V \in \mathrm{Mat_{k,h}(R)} \right\} \tag{3.10}$$

costituiscono un sottogruppo di $\mathrm{GL_n(R)}$.

Dimostrazione. Ricordando il prodotto di matrici a blocchi descritto nel Teorema 1.6 del capitolo precedente, si verifica subito che:

$$\begin{pmatrix} I & 0 \\ V_1 & I \end{pmatrix} \begin{pmatrix} I & 0 \\ V_2 & I \end{pmatrix} = \begin{pmatrix} I & 0 \\ V_1 + V_2 & I \end{pmatrix}$$

$$\begin{pmatrix} I & 0 \\ V & I \end{pmatrix}^{-1} = \begin{pmatrix} I & 0 \\ -V & I \end{pmatrix}. \blacksquare$$

Analogo risultato vale per l'insieme delle matrici trasposte.

Per le matrici diagonali converrà usare la seguente notazione:

$$\begin{pmatrix} \lambda_1 & & \\ & \dots & \\ & & \lambda_n \end{pmatrix} = \mathrm{diag}\,(\lambda_1, \dots, \lambda_n)\,. \tag{3.11}$$

(3.12) Proposizione *Le matrici diagonali del tipo*

$$\{\mathrm{diag}\,(\nu_1, \dots, \nu_n) \mid \nu_i \in R^*\} \tag{3.13}$$

costituiscono un sottogruppo di $\mathrm{GL_n(R)}$, *detto* diagonale.

Dimostrazione.

$\mathrm{diag}\,(\nu_1, \dots, \nu_n)\,\mathrm{diag}\,(\mu_1, \dots, \mu_n) = \mathrm{diag}\,(\mu_1\nu_1, \dots, \mu_n\nu_n)$

$\operatorname{diag}(\nu_1,\dots,\nu_n)^{-1} = \operatorname{diag}\left(\nu_1^{-1},\dots,\nu_n^{-1}\right)$. ■

Si noti infine che una matrice diagonale a blocchi è invertibile se e solo se i suoi blocchi diagonali lo sono. In tal caso

$$\begin{pmatrix} X & \\ & Y \end{pmatrix}^{-1} = \begin{pmatrix} X^{-1} & \\ & Y^{-1} \end{pmatrix}. \tag{3.14}$$

4 Esercizi

(4.1) Esercizio *Data* $A = \begin{pmatrix} 4 & 1 & 3 & -2 \\ 1 & -1 & 2 & 5 \\ 4 & 6 & -3 & 8 \end{pmatrix} \in \mathrm{Mat}_{3,4}(\mathbb{Z})$, *eseguire i prodotti:*

$$\begin{pmatrix} 1 & 0 & 0 \end{pmatrix} A, \quad \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} A, \quad \begin{pmatrix} 0 & 0 & 1 \end{pmatrix} A, \quad Ae_1,\ Ae_2,\ Ae_3,\ Ae_4.$$

I risultati ottenuti come sono correlati alle righe e alle colonne di A ?

(4.2) Esercizio *Posto*

$$A = \begin{pmatrix} 3 & -1 & 0 \\ 4 & 0 & 2 \\ 1 & 6 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 3 \\ 1 & -1 & 2 \\ 4 & 6 & -3 \end{pmatrix}$$

eseguire il prodotto AB scrivendo

1) *le righe di AB come combinazione lineare di quelle di B;*

2) *le colonne di AB come combinazione lineare di quelle di A.*

(4.3) Esercizio *Date*

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \; B = \begin{pmatrix} 1 & \frac{-5}{4} \\ 0 & 1 \end{pmatrix}$$

si scrivano

1) le righe di BA in funzione di quelle di A;

2) le colonne di AB in funzione di quelle di A.

(4.4) Esercizio *Date*

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \; P = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \; D = \begin{pmatrix} 2 & 0 & 0 \\ 0 & \frac{1}{5} & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

si scrivano

1) *le colonne di AP e quelle di AD in funzione di quelle di A;*

2) *le righe di PA e quelle di DA in funzione di quelle di A;*

(4.5) Esercizio *Effettuando i calcoli, verificare che*

$$\left(\left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)\left(\begin{array}{cccc} 4 & 1 & 3 & -2 \\ 1 & -1 & 2 & 5 \\ 4 & 6 & -3 & 8 \end{array}\right)\right)\left(\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) =$$

$$\left(\begin{array}{ccc} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{array}\right)\left(\left(\begin{array}{cccc} 4 & 1 & 3 & -2 \\ 1 & -1 & 2 & 5 \\ 4 & 6 & -3 & 8 \end{array}\right)\left(\begin{array}{cccc} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)\right)$$

(4.6) Esercizio *Nel caso $R = \mathbb{Q}$ si calcoli l'inversa delle matrici:*

$$A = \left(\begin{array}{cc} 1 & 0 \\ 5 & 1 \end{array}\right),\ B = \left(\begin{array}{cc} 1 & 7 \\ 0 & 1 \end{array}\right),\ C = \left(\begin{array}{cc} 1 & 0 \\ \frac{7}{2} & 1 \end{array}\right),\ AB,\ ABC,\ CB.$$

(4.7) Esercizio *Nel caso $R = \mathbb{Q}$ si calcoli l'inversa delle matrici:*

$$P = \left(\begin{array}{ccc} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{array}\right),\ D = \left(\begin{array}{ccc} 2 & 0 & 0 \\ 0 & \frac{1}{5} & 0 \\ 0 & 0 & 3 \end{array}\right),\ U = \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{array}\right).$$

(4.8) Esercizio *Si scriva la matrice $P \in \mathrm{GL}_2(\mathbb{Q})$ tale che*

$$AP = \left(\begin{array}{c|c} Ae_2 & Ae_1 \end{array}\right)$$

per ogni $A \in \mathrm{Mat}_2(\mathbb{Q}$.

(4.9) Esercizio *Si scriva la matrice $P \in \mathrm{GL}_2(\mathbb{Q}$ tale che*

$$AP = \left(\begin{array}{c|c} Ae_1 & 3Ae_1 + Ae_2 \end{array}\right)$$

per ogni $A \in \mathrm{Mat}_2(\mathbb{Q}$.

(4.10) Esercizio *Si dimostri che una matrice diagonale a blocchi $A = \left(\begin{array}{cc} X & \\ & Y \end{array}\right)$ è invertibile se e solo se i suoi blocchi X e Y sono invertibili.*

(4.11) Esercizio *In $\mathrm{Mat}_3(\mathbb{R})$, eseguire i seguenti prodotti a blocchi:*

$$\left(\begin{array}{c|cc} -2 & 0 & 0 \\ \hline 0 & 3 & 2 \\ 0 & 6 & -1 \end{array}\right)\left(\begin{array}{c|cc} 2 & 0 & 0 \\ \hline 0 & -1 & 4 \\ 0 & -5 & 7 \end{array}\right),\quad \left(\begin{array}{c|c|c} \pi & 0 & 0 \\ \hline 0 & \sqrt{2} & 0 \\ \hline 0 & 0 & 4 \end{array}\right)\left(\begin{array}{c|c|c} 2 & 0 & 0 \\ \hline 0 & \sqrt{2} & 0 \\ \hline 0 & 0 & -\pi \end{array}\right).$$

(4.12) Esercizio *Sia H un sottogruppo di* $\mathrm{GL_n(R)}$. *Dimostrare che anche H^t è un sottogruppo.*

(4.13) Esercizio *Date* $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$ *si verifichi direttamente che* $\det(AB) = (\det A)(\det B)$.

Capitolo IV

Forme normali delle matrici

1 Equivalenza fra matrici

(1.1) Definizione *Date* $A, B \in \mathrm{Mat_{m,n}(R)}$*, diciamo che* A *è* equivalente *a* B *e scriviamo* $A \equiv B$*, se esistono* $Q \in \mathrm{GL_m(R)}$ *e* $P \in \mathrm{GL_n(R)}$ *tali che* $A = QBP$*.*

Il fatto che $\mathrm{GL_m(R)}$ e $\mathrm{GL_n(R)}$ siano gruppi ha la seguente conseguenza.

(1.2) Lemma *L' equivalenza fra matrici è riflessiva, simmetrica e transitiva.*

Dimostrazione. Per ogni $A, B, C \in \mathrm{Mat_{m,n}(R)}$:

1) $A \equiv A$.

Infatti $A = I_m A I_n$.

2) $A \equiv B \Longrightarrow B \equiv A$.

Infatti da $A = QBP$ segue $B = Q^{-1}AP^{-1}$.

3) ($A \equiv B$ e $B \equiv C$) $\Longrightarrow A \equiv C$.

Infatti da $A = Q_1 B P_1$ e da $B = Q_2 C P_2$ segue $A = (Q_1 Q_2)\, C\, (P_2 P_1)$.

Resta da notare che se Q_1 e Q_2 appartengono a $\in \mathrm{GL_m(R)}$ anche il loro prodotto $Q_1 Q_2$ vi appartiene. Analoga considerazione per P_1 e P_2. ■

(1.3) Esempio *Tenendo presente i paragrafi* 2 *e* 3 *del Capitolo III, per ogni matrice* $A = \left(\ Ae_1 \mid Ae_2 \mid Ae_3\ \right) \in \mathrm{Mat_{2,3}(R)}$ *si ha:*

$$A \equiv \left(\ Ae_2 \mid Ae_1 \mid Ae_3\ \right), \quad A \equiv \left(\ Ae_1 \mid Ae_2 - 2Ae_3 \mid Ae_3\ \right).$$

Infatti:

$$A \ \equiv \ A\pi_{(12)} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{12} & a_{11} & a_{13} \\ a_{22} & a_{21} & a_{23} \end{pmatrix}.$$

$$A \equiv A\,(I - 2E_{32}) = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -2 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} - 2a_{13} & a_{13} \\ a_{21} & a_{22} - 2a_{23} & a_{23} \end{pmatrix}.$$

In generale:

(1.4) Lemma *Una matrice $A \in \mathrm{Mat_{m,n}(R)}$ è equivalente a qualunque matrice ottenuta con una delle seguenti operazioni sulle sue colonne:*

1) *scambio delle colonne Ae_i e Ae_j;*

2) *sostituzione della colonna Ae_j con $Ae_j + rAe_i$, per ogni $r \in R$, $i \neq j$;*

3) *moltiplicazione della colonna Ae_i per un elemento $\nu \in R^*$.*

Similmente A è equivalente a qualunque matrice da essa ottenuta con una delle analoghe operazioni sulle sue righe.

Dimostrazione.

1) La matrice *di permutazione* $\pi_{(ij)}$ appartiene a $\mathrm{GL_n(R)}$. Ne segue $A \equiv A\pi_{ij}$. Notando che $A\pi_{ij}$ si ottiene da A scambiando fra loro Ae_i e Ae_j, si ha l'asserto.

2) La matrice *elementare* $I + rE_{ij}$ appartiene a $\mathrm{GL_n(R)}$. Ne segue $A \equiv A\,(I + rE_{ij})$. Notando che $A\,(I + rE_{ij})$ si ottiene da A sostituendo Ae_j con $Ae_j + rAe_i$, si ha l'asserto.

3) La matrice diagonale $N = \mathrm{diag}\,(1_R, \ldots, \nu, \ldots, 1_R)$ che ha ν nel posto (i,i) e 1_R altrove, appartiene a $\mathrm{GL_n(R)}$. Quindi $A \equiv AN$. Notando che AN si ottiene da A moltiplicando la colonna Ae_i per ν si ha l'asserto.

L' affermazione riguardante le operazioni sulle righe si dimostra moltiplicando *a sinistra* A per le analoghe matrici. ■

(1.5) Esempio *Per ogni matrice* $A = \begin{pmatrix} e_1^t A \\ e_2^t A \end{pmatrix} \in \mathrm{Mat_{2,3}(R)}$ *si ha:*

$$A \equiv \begin{pmatrix} e_2^t A \\ e_1^t A \end{pmatrix}, \quad A \equiv \begin{pmatrix} e_1^t A + 3e_2^t A \\ e_2^t A \end{pmatrix}, \quad A \equiv \begin{pmatrix} 3\,e_1^t A + 4\,e_2^t A \\ -e_1^t A - e_2^t A \end{pmatrix}.$$

Infatti:

$$A \equiv \pi_{(12)} A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} = \begin{pmatrix} a_{21} & a_{22} & a_{23} \\ a_{11} & a_{12} & a_{13} \end{pmatrix};$$

$A \equiv (I + 3E_{12})\,A =$

$$= \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} = \begin{pmatrix} a_{11} + 3a_{21} & a_{12} + 3a_{22} & a_{13} + 3a_{23} \\ a_{21} & a_{22} & a_{23} \end{pmatrix};$$

$$A \equiv \begin{pmatrix} 3 & 4 \\ -1 & -1 \end{pmatrix} A =$$

$$\begin{pmatrix} 3 & 4 \\ -1 & -1 \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \end{pmatrix} = \begin{pmatrix} 3a_{11}+4a_{21} & 3a_{12}+4a_{22} & 3a_{13}+4a_{23} \\ -a_{11}-a_{21} & -a_{12}-a_{22} & -a_{13}-a_{23} \end{pmatrix}.$$

(1.6) Lemma *Se $A_1 \equiv B_1$ e $A_2 \equiv B_2$ allora*

$$\begin{pmatrix} A_1 & \\ & A_2 \end{pmatrix} \equiv \begin{pmatrix} B_1 & \\ & B_2 \end{pmatrix}.$$

Dimostrazione.

Siano Q_1, Q_2, P_1, P_2 matrici invertibili tali che

$$A_1 = Q_1 B_1 P_1, \quad A_2 = Q_2 B_2 P_2.$$

Allora le matrici

$$Q = \begin{pmatrix} Q_1 & \\ & Q_2 \end{pmatrix}, \quad P = \begin{pmatrix} P_1 & \\ & P_2 \end{pmatrix}$$

sono invertibili e $A = QBP$. ■

2 Forme normali nei dominii a ideali principali

Per il Lemma 1.2, l'equivalenza fra matrici ripartisce $\mathrm{Mat_{m,n}(R)}$ in classi di equivalenza. Nel caso in cui $R = D$ è un dominio a ideali principali, è possibile scegliere degli opportuni rappresentanti per tali classi, detti *forme normali*. Allo scopo di descriverli, ricordiamo che una matrice di $\mathrm{Mat_{m,n}(D)}$ è *pseudodiagonale* se gli elementi di posto (i, j) con $i \neq j$ sono tutti nulli. Quindi, se $m = n$, le matrici pseudodiagonali sono quelle diagonali. Altrimenti sono della forma:

$$\begin{pmatrix} \lambda_1 & & & 0 & \dots & 0 \\ & \lambda_2 & & 0 & \dots & 0 \\ & & \dots & 0 & \dots & 0 \\ & & \lambda_m & 0 & \dots & 0 \end{pmatrix} \text{ se } m < n, \quad \begin{pmatrix} \lambda_1 & & & \\ & \lambda_2 & & \\ & & \dots\dots & \\ & & & \lambda_n \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix} \text{ se } n < m.$$

In generale, detto s il minimo fra m e n, indicheremo tali matrici mediante

$$\mathrm{pseudodiag}\,(\lambda_1,\ \dots,\ \lambda_s)\,.$$

(2.1) Definizione *Diciamo* forma normale *ogni matrice* pseudodiag $(d_1, \ldots, d_s)$ *in cui ogni elemento diagonale* d_i *divide il successivo* d_{i+1}.

(2.2) Lemma *Se* $d \in D$ *divide tutte le componenti* a_{ij} *di una matrice* $A \in \mathrm{Mat_{m,n}(D)}$, *allora* d *divide tutte le componenti di ogni matrice equivalente ad* A.

Dimostrazione. Ogni matrice equivalente ad A è della forma QAP, con $Q \in \mathrm{GL_m(D)}$ e $P \in \mathrm{GL_n(D)}$. Le componenti di QA sono combinazioni lineari a coefficienti in D di quelle di A, e sono quindi tutte divisibili per d. Analogamente le componenti di $(QA)P$ sono combinazioni lineari di quelle di QA, e sono quindi tutte divisibili per d. ■

(2.3) Lemma *Dati* $a, b \in D$, *sia* $d := \mathrm{M.C.D}\,(a, b)$. *Allora:*

- $\begin{pmatrix} a \\ b \end{pmatrix} \equiv \begin{pmatrix} d \\ 0 \end{pmatrix}$ *in* $\mathrm{Mat_{2,1}(D)}$;
- $\begin{pmatrix} a, b \end{pmatrix} \equiv \begin{pmatrix} d, 0 \end{pmatrix}$ *in* $\mathrm{Mat_{1,2}(D)}$.

Dimostrazione. Siano $x, y \in D$ tali che $d = xa + yb$. Posto $a = d\overline{a}$, $b = d\overline{b}$, si ha

$$1 = x\overline{a} + y\overline{b}.$$

Ne segue che la matrice $\begin{pmatrix} x & y \\ -\overline{b} & \overline{a} \end{pmatrix}$ ha determinante 1, ed appartiene quindi a $\mathrm{GL_2(D)}$. pertanto:

$$\begin{pmatrix} a \\ b \end{pmatrix} \equiv \begin{pmatrix} x & y \\ -\overline{b} & \overline{a} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

Trasponendo:

$$\begin{pmatrix} a & b \end{pmatrix} \equiv \begin{pmatrix} a & b \end{pmatrix} \begin{pmatrix} x & -\overline{b} \\ y & \overline{a} \end{pmatrix} = \begin{pmatrix} d & 0 \end{pmatrix}.$$

■

Ricordiamo che, per il Corollario 2.5 del Capitolo 2, D è fattoriale. Questo fatto ci consente di definire la *lunghezza* $\lambda(a)$ di ogni elemento non nullo a di D nel modo seguente. Se $a \in D^*$, poniamo $\lambda(a) = 0$. Altrimenti, considerata una fattorizzazione $a = p_1 \ldots p_k$ in fattori irriducibili (non necessariamente distinti), poniamo $\lambda(a) = k$. Per esempio, nell'anello $\mathbb{Z}$ si ha $8 = 2 \cdot 2 \cdot 2$, quindi $\lambda(8) = 3$.

Notiamo che, per ogni divisore proprio d di a, si ha $\lambda(d) < \lambda(a)$. Infatti l'insieme dei divisori irriducibili di d è un sottoinsieme proprio di quelli di a.

(2.4) Teorema *Ogni matrice* $A = (a_{ij}) \in \mathrm{Mat_{m,n}(D)}$ *è equivalente ad una forma normale.*

Dimostrazione.

Se A è la matrice nulla, $A \equiv A$ è lei stessa una forma normale. Altrimenti scegliamo una componente $a_{ij} \neq 0$ di A tale che $\lambda(a_{ij})$ sia minima fra le componenti non nulle di A. Sostituendo eventualmente A con la matrice $\pi_{1k} A \pi_{1\ell}$, ad essa equivalente, possiamo supporre che sia $a_{k\ell} = a_{11}$.

Supponiamo che a_{11} non divida un elemento della prima riga. Dopo un eventuale scambio di colonne, possiamo supporre che a_{11} non divida a_{12}. Ne segue che $b_{11} :=$ M.C.D.(a_{11}, a_{12}) è tale che

$$\lambda(b_{11}) < \lambda(a_{11}). \tag{2.5}$$

Ora, tenendo presente il Lemma 2.3 e ponendo

$$b_{11} = a_{11}x + a_{12}y, \quad a_{11} = b_{11}\overline{a}_{11}, \quad a_{12} = b_{11}\overline{a}_{12}, \quad P = \begin{pmatrix} x & -\overline{a}_{12} \\ y & \overline{a}_{11} \end{pmatrix}$$

si ottiene:

$$A \equiv A \begin{pmatrix} P & \\ & I_{n-2} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \dots \\ a_{21} & a_{22} & \dots \\ \dots & \dots & \dots \end{pmatrix} \begin{pmatrix} x & -\overline{a}_{12} & \\ y & \overline{a}_{11} & \\ & & I_{n-2} \end{pmatrix} = \begin{pmatrix} b_{11} & \dots & \dots \\ \dots & \dots & \dots \\ \dots & \dots & \dots \end{pmatrix}.$$

Sempre per il Lemma 2.3 ottiene un risultato analogo se a_{11} non divide un elemento della prima colonna di A.

In virtù di (2.5), questo procedimento ammette solo un numero finito di iterazioni. Perveniamo quindi ad una matrice $A' = \left(a'_{ij}\right)$, equivalente ad A, in cui a'_{11} divide tutti gli elementi della prima riga e tutti gli elementi della prima colonna.

Posto $a'_{j1} = a'_{11}\,\overline{a}_{j1}$ $(1 \leq j \leq m)$, $a'_{1j} = a'_{11}\,\overline{a}_{1j}$ $(1 \leq j \leq n)$,

$$w = (\overline{a}_{21}, \dots, \overline{a}_{m1})^t, \quad v^t = (\overline{a}_{12}, \dots, \overline{a}_{1n}),$$

si ha $A' = \begin{pmatrix} a'_{11} & a'_{11}v^t \\ a'_{11}w & * \end{pmatrix}$. Pertanto

$$A' \equiv \begin{pmatrix} 1 & 0 \\ -w & I_{m-1} \end{pmatrix} A' \begin{pmatrix} 1 & -v^t \\ 0 & I_{n-1} \end{pmatrix} = \begin{pmatrix} a'_{11} & 0 \\ 0 & * \end{pmatrix} = A''$$

Se a'_{11} non divide qualche componente di A'', sommando alla prima riga di A'' la riga a cui appartiene quella componente, si ottiene una matrice equivalente ad A'', in cui un elemento della prima riga non è divisibile per a'_{11}. Iterando tutto il procedimento un numero finito di volte, si perviene una matrice equivalente ad A della forma:

$$\begin{pmatrix} d_1 & 0 \\ 0 & T \end{pmatrix}$$

in cui d_1 divide tutte le componenti di T. Per induzione, possiamo supporre

$$T \equiv \text{pseudodiag}\,(d_2, \ldots, d_m)$$

dove $d_2|d_3|\ldots|d_m$. Dal Lemma 2.2 segue che d_1 divide d_2, pertanto pseudodiag $(d_1, d_2, \ldots, d_m)$ è una forma normale. Per il Lemma 1.6 si ha la tesi. ■

(2.6) Esempio *In* $\mathrm{Mat}_2(\mathbb{Z})$ *la matrice* $A = \begin{pmatrix} 1 & 3 \\ -2 & 1 \end{pmatrix}$ *è equivalente a* $\begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}$. *Infatti*

$$A \equiv \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} A \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}.$$

(2.7) Esempio *In* $\mathrm{Mat}_2(\mathbb{Z})$ *la matrice* $A = \begin{pmatrix} 3 & 10 \\ 2 & 3 \end{pmatrix}$ *è equivalente a* $\begin{pmatrix} 1 & 0 \\ 0 & 11 \end{pmatrix}$. *Infatti:*

$$A \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} A = \begin{pmatrix} 2 & 3 \\ 3 & 10 \end{pmatrix};$$

$$\begin{pmatrix} 2 & 3 \\ 3 & 10 \end{pmatrix} \equiv \begin{pmatrix} 2 & 3 \\ 3 & 10 \end{pmatrix} \begin{pmatrix} -1 & -3 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 7 & 11 \end{pmatrix};$$

$$\begin{pmatrix} 1 & 0 \\ 7 & 11 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ -7 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 7 & 11 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 11 \end{pmatrix}.$$

3 Applicazione alla risoluzione dei sistemi lineari

Un sistema lineare di m equazioni in n indeterminate $x_1, \ldots, x_n$, a coefficienti in $\mathbb{K}$, si scrive nella forma

$$\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{m1} & \ldots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \ldots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \ldots \\ b_m \end{pmatrix}$$

o, più brevemente,

$$AX = B, \tag{3.1}$$

con $A \in \mathrm{Mat_{m,n}}(\mathbb{K})$, $B \in \mathrm{Mat_{m,1}}(\mathbb{K})$.

(3.2) Definizione *Ogni* $C \in \mathrm{Mat_{n,1}}(\mathbb{K})$ *tale che*

$$AC = B$$

si dice soluzione del sistema (3.1).

Per quanto osservato sul prodotto di matrici, il vettore $AX = x_1Ae_1 + \cdots + x_nAe_n$ è combinazione lineare delle colonne di A. Pertanto il sistema (3.1) ha (almeno una) soluzione $C \in \mathrm{Mat_{n,1}} := \mathbb{K}^n$ se e solo se B è combinazione lineare, a coefficienti in $\mathbb{K}$, delle colonne di A. (Si confronti questa osservazione con il Teorema di Rouche' Capelli, visto nel corso di Geometria).

(3.3) Lemma *Per ogni matrice $Q \in \mathrm{GL_m}(\mathbb{K})$ il sistema* (3.1) *e il sistema*

$$QAX = QB, \tag{3.4}$$

hanno le stesse soluzioni, ossia sono equivalenti.

Dimostrazione. Sia C una soluzione di (3.1). Da $AC = B$ segue $QAC = QB$, ossia C è soluzione di (3.4). Viceversa, sia $\overline{C}$ una soluzione di (3.4). Da $QA\overline{C} = QB$ segue $Q^{-1}QA\overline{C} = Q^{-1}QB$, ossia $A\overline{C} = B$, ossia $\overline{C}$ è soluzione di (3.1). ■

Il metodo di risoluzione di un sistema per graduale eliminazione delle indeterminate è fornito dal seguente:

(3.5) Teorema *(di Gauss Jordan) A meno di un riordinamento delle equazioni e delle indeterminate, il sistema* (3.1) *è equivalente a un sistema* a gradini*, ossia della forma: $A'X = B'$, dove A' ha le seguenti proprietà :*

1) è triangolare superiore;

2) per qualche $k \geq 0$, i primi k elementi sulla diagonale principale sono 1*, e gli eventuali rimanenti sono* 0*.*

Dimostrazione.

Se A è non nulla, riordinando eventualmente le viariabili e le equazioni possiamo supporre che sia $a_{11} \neq 0$. Posto

$$v = \begin{pmatrix} -a_{21} \\ \dots \\ -a_{m1} \end{pmatrix}, \quad Q_1 = \begin{pmatrix} 1 & 0 \\ v & I_{m-1} \end{pmatrix}, \quad Q_2 = \mathrm{diag}\left(a_{11}^{-1}, 1, \dots, 1\right)$$

il sistema (3.1) è equivalente al sistema:

$$Q_1Q_2AX = Q_1Q_2B$$

in cui x_1 compare soltanto nella prima equazione, e ha coefficiente 1. La tesi segue per induzione sul numero n delle indeterminate. ■

(3.6) Esempio *Sul campo razionale Q, il sistema*

$$\begin{cases} x_1 + 3x_2 - x_3 = 5 \\ 4x_1 + 7x_2 + 2x_3 = 0 \end{cases}$$

è equivalente al sistema a gradini:

$$\begin{cases} x_1 & +3x_2 & -x_3 & = & 5 \\ & x_2 & -\frac{6}{5}x_3 & = & 4 \end{cases}.$$

Ricavando x_2 dalla seconda equazione e sostituendolo tale valore nella prima:

$$x_2 = \tfrac{6}{5}x_3 + 4$$
$$x_1 = \tfrac{-13}{5}x_3 - 7.$$

Capitolo V

Determinanti

In questo capitolo R indica un anello commutativo.

1 Definizione e proprietà

Ricordiamo che una permutazione si dice *pari* se è prodotto di un numero pari di scambi. Si dice *dispari* in caso contrario. Non è difficile verificare la consistenza di questa definizione, nonostante non sia unico il modo di scrivere una permutazione come prodotto di scambi. Chiaramente la permutazione identica è pari (prodotto di 0 scambi) e ogni scambio (ij) è dispari.

(1.1) Esempio *Le permutazioni* $(123),\ (12345)$ *sono pari. Infatti*
$(123) = (13)(12),\ (12345) = (15)(14)(13)(12)$.
Le permutazioni $(1234),\ (123456)$ *sono dispari. Infatti*
$(1234) = (14)(13)(12),\ (123456) = (16)(15)(14)(13)(12)$

Per ogni $\sigma \in \mathrm{Sym(n)}$, poniamo $\mathrm{sg}\,(\sigma) := 1$ se σ è pari, $\mathrm{sg}\,(\sigma) := -1$ se σ è dispari. Notiamo che:

$$\mathrm{sg}\,(\sigma_1\sigma_2) = \mathrm{sg}\,(\sigma_1)\,\mathrm{sg}\,(\sigma_2)\,. \tag{1.2}$$

$$\mathrm{sg}\,(\sigma) = \mathrm{sg}\left(\sigma^{-1}\right). \tag{1.3}$$

Ne segue che l'insieme $\mathrm{Alt}(n)$ delle permutazioni pari è un sottogruppo di $\mathrm{Sym(n)}$. Esso ha ordine $\frac{n!}{2}$ ed è detto il gruppo *alterno* di grado n.

(1.4) Lemma *Per ogni matrice* $A = (a_{ij}) \in \mathrm{Mat_n(R)}$, *si ha*

$$\sum_{\sigma\in\mathrm{Sym(n)}} \mathrm{sg}\,(\sigma) \prod_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{a_{k\,\sigma(k)}} \;=\; \sum_{\sigma\in\mathrm{Sym(n)}} \mathrm{sg}\,(\sigma) \prod_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{a_{\sigma(k)\,k}}. \tag{1.5}$$

Dimostrazione.

Fissata σ, poniamo $h = \sigma(k)$. Per la commutatività del prodotto in R risulta

$$\prod_{k=1}^{n} a_{k\,\sigma(k)} = \prod_{h=1}^{n} a_{\sigma^{-1}(h)\,h}$$

da cui, tenendo presente 1.3

$$\sum_{\sigma\in \mathrm{Sym(n)}} \mathrm{sg}\,(\sigma) \prod_{\mathrm{k=1}}^{\mathrm{n}} \mathrm{a_{k\,\sigma(k)}} = \sum_{\sigma\in \mathrm{Sym(n)}} \mathrm{sg}\,\left(\sigma^{-1}\right) \prod_{\mathrm{h=1}}^{\mathrm{n}} \mathrm{a_{\sigma^{-1}(h)\,h}} =$$

$$\sum_{\sigma^{-1}\in \mathrm{Sym(n)}} \mathrm{sg}\,\left(\sigma^{-1}\right) \prod_{\mathrm{h=1}}^{\mathrm{n}} \mathrm{a_{\sigma^{-1}(h)\,h}} = \sum_{\sigma\in \mathrm{Sym(n)}} \mathrm{sg}\,(\sigma) \prod_{\mathrm{k=1}}^{\mathrm{n}} \mathrm{a_{\sigma(k)\,k}}.$$

■

(1.6) Definizione *L'elemento di R fornito da* (1.5) *si chiama* determinante *di A e si indica con* $\det A$.

(1.7) Esempio *La matrice* $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ *ha determinante:*

$$a_{11}\,a_{22} \;-\; a_{12}\,a_{21}.$$

(1.8) Esempio *La matrice* $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ *ha determinante:*

$$a_{11}\,a_{22}\,a_{33} \;+\; a_{12}\,a_{23}\,a_{31} \;+\; a_{13}\,a_{21}\,a_{32} \;-\; a_{11}\,a_{23}\,a_{32} \;-\; a_{13}\,a_{22}\,a_{31} \;-\; a_{12}\,a_{21}\,a_{33}.$$

Notiamo che, per ogni i, j, ciascun addendo dello sviluppo di $\det A$ ha un unico fattore il cui primo indice è i (ossia che si trova nella riga i-esima di A) e un unico fattore il cui secondo indice è j (ossia che si trova nella colonna j-esima di A).

(1.9) Teorema *Il determinante di* $A \in \mathrm{Mat_n(R)}$ *ha le seguenti proprietà :*

1) $\det A = \det A^t$*;*

2) *per* $\rho \in \mathrm{Sym(n)}$*, detta* A' *la matrice le cui colonne sono* $Ae_{\rho(1)}, \ldots, Ae_{\rho(n)}$*,*

$$\det A' = \mathrm{sg}\,(\rho) \det \mathrm{A};$$

3) *se A ha due colonne uguali,* $\det A = 0_R$*;*

4) *se A ha una colonna nulla,* $\det A = 0_R$*;*

5) $\det A$ *è lineare nelle colonne, ossia da*

$$Ae_i = \lambda b + \mu c$$

con $\lambda, \mu \in R$, $b, c \in R^n$, *segue :*

$$\det A = \lambda \det B + \mu \det C,$$

dove B *e* C *sono le matrici ottenute da* A *sostituendo* Ae_i *rispettivamente con* b *e* c.

In virtù di 1), analoghe proprietà valgono per le righe di A.

Dimostrazione.

1) Segue da (1.5).

2) Notando che $\mathrm{Sym(n)} = \{\sigma\rho \mid \sigma \in \mathrm{Sym(n)}\}$ e ricordando 1.2 e 1.3:

$$\det A' = \sum_{\sigma \in \mathrm{Sym(n)}} \mathrm{sg}\,(\sigma) \prod_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{a}_{\mathrm{k}\,\sigma\rho(\mathrm{k})} =$$

$$\mathrm{sg}\,(\rho)^{-1} \sum_{\sigma \in \mathrm{Sym(n)}} \mathrm{sg}\,(\sigma\rho) \prod_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{a}_{\mathrm{k}\,\sigma\rho(\mathrm{k})} = \mathrm{sg}\,(\rho) \det \mathrm{A}.$$

3) Supponiamo $Ae_i = Ae_j$, con $i \neq j$. Detta A' la matrice ottenuta da A scambiando la colonna i-esima con la j-esima, si ha $A = A'$ e, per il punto 2), $\det A = -\det A$. Quindi, se tutti gli elementi di R hanno caratteristica $\neq 2$, il punto 3) segue dal precedente. Tuttavia esso vale in generale. A tale scopo, consideriamo lo scambio $\tau = (i, j)$. Possiamo ripartire $\mathrm{Sym(n)}$ in $\mathrm{Alt(n)}$ e $\mathrm{Alt(n)}\tau$. Pertanto

$$\det A = \sum_{\sigma \in \mathrm{Sym(n)}} \mathrm{sg}\,(\sigma) \prod_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{a}_{\sigma(\mathrm{k})\,\mathrm{k}} = \sum_{\sigma \in \mathrm{Alt(n)}} \left(\prod_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{a}_{\sigma(\mathrm{k})\,\mathrm{k}} - \prod_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{a}_{\sigma\tau(\mathrm{k})\,\mathrm{k}} \right).$$

Notando che, per tutti gli indici $k \notin \{i, j\}$, si ha $\sigma(k) = \sigma\tau(k)$, risulta:

$$\det A = \sum_{\sigma \in \mathrm{Alt(n)}} \left(a_{\sigma(i)\,i}\; a_{\sigma(j)\,j} - a_{\sigma(j)\,i}\; a_{\sigma(i)\,j} \right) \prod_{k \neq i,j} a_{\sigma(k)\,k}.$$

Da $Ae_i = Ae_j$ segue $a_{\sigma(i)\,i}\; a_{\sigma(j)\,j} = a_{\sigma(i)\,j} a_{\sigma(j)\,i} =$ (per la commutatività del prodotto) $= a_{\sigma(j)\,i} a_{\sigma(i)\,j}$. Pertanto, in ogni addendo di $\det A$, il coefficiente $a_{\sigma(i)\,i}\; a_{\sigma(j)\,j} - a_{\sigma(j)\,i}\; a_{\sigma(i)\,j}$ è nullo. Si conclude che $\det A = 0$.

4) Ogni addendo dello sviluppo di $\det A$ ha un fattore che appartiene a quella colonna, ed è quindi nullo.

5) Possiamo supporre:

$$b = \begin{pmatrix} b_1 \\ \dots \\ b_n \end{pmatrix},\ c = \begin{pmatrix} c_1 \\ \dots \\ c_n \end{pmatrix}, \quad Ae_i = \begin{pmatrix} \lambda b_1 + \mu c_1 \\ \dots \\ \lambda b_n + \mu c_n \end{pmatrix}.$$

Ne segue:

$\det A = \sum_{\sigma\in \mathrm{Sym(n)}} \mathrm{sg}\,(\sigma) \prod_{\mathrm{k=1}}^{\mathrm{n}} \mathrm{a}_{\sigma(\mathrm{k})\,\mathrm{k}} =$

$$\sum_{\sigma\in \mathrm{Sym(n)}} (\mathrm{sg}\ \sigma)\left(\lambda b_{\sigma(i)} + \mu c_{\sigma(i)}\right) \prod_{k\neq i} a_{\sigma(k)\,k} =$$

$$\lambda \sum_{\sigma\in \mathrm{Sym(n)}} (\mathrm{sg}\ \sigma)\, b_{\sigma(i)} \prod_{k\neq i} a_{\sigma(k)\,k} \ +\ \mu \sum_{\sigma\in \mathrm{Sym(n)}} (\mathrm{sg}\ \sigma)\, c_{\sigma(i)} \prod_{k\neq i} a_{\sigma(k)\,k} =$$

$\lambda \det B + \mu \det C.$ ■

(1.10) Corollario *Sia $A \in \mathrm{Mat_n}(\mathbb{R})$. Se una colonna (riga) di A è combinazione lineare delle altre colonne (righe), allora det$(A) = 0$.*

Dimostrazione. Supponiamo, ad esempio, $Ae_1 = \lambda_2 Ae_2 + \cdots + \lambda_n Ae_n$. Per ogni $i \geq 2$, sia B_i la matrice ottenuta da A sostituendo Ae_1 mediante Ae_i. La matrice B_i ha la prima e l'i-esima colonna uguali, quindi il suo determinante è 0. Ne segue $\det A = \lambda_2 \det B_2 + \cdots + \lambda_n \det B_n = 0$. ■

(1.11) Teorema *(di Binet) Per ogni $A, B \in \mathrm{Mat_n(R)}$ si ha*

$$\det(AB) = (\det A)(\det B).$$

Dimostrazione.

Le colonne di AB sono combinazione lineare delle colonne di A, i.e.,

$$AB = \left(\ \textstyle\sum_{j=1}^{n} b_{j1} Ae_j \ \middle|\ \dots \ \middle|\ \sum_{j=1}^{n} b_{jn} Ae_j\ \right).$$

Applicando iteratamente il punto 5) del Teorema precedente si ha:

$$\det(AB) = \sum_{i_1,\dots i_n} b_{i_1 1} \dots b_{i_n n} \det\left(\ Ae_{i_1} \ \middle|\ \dots \ \middle|\ Ae_{i_n}\ \right)$$

dove la sommatoria è estesa a tutte le n-ple $(i_1,\ \dots,\ i_n)$ con $1 \leq i_j \leq n$ per ogni j. Tenendo presente che per le n-ple con (almeno) due indici uguali si ha

$$\det\left(\ Ae_{i_1} \ \middle|\ \dots \ \middle|\ Ae_{i_n}\ \right) = 0,$$

che le rimanenti n-ple sono quelle dell'insieme $\{(\sigma(1),\dots,\sigma(n)) \mid \sigma \in \mathrm{Sym(n)}\}$ e che, per ciascuna di esse,

$$\det\left(\ Ae_{\sigma(1)} \ \middle|\ \dots \ \middle|\ Ae_{\sigma(n)}\ \right) = \mathrm{sg}(\sigma)\det \mathrm{A}$$

si ottiene

$$\det(AB) = \left(\sum_{\sigma\in \mathrm{Sym(n)}} \mathrm{sg}\,(\sigma)\prod_{\mathrm{k}=1}^{\mathrm{n}} \mathrm{b}_{\sigma(\mathrm{k})\,\mathrm{k}}\right)\det A = \det B\det A = \det A\det B.$$

■

2 Il Teorema di Laplace

(2.1) Definizione *Data $A = (a_{hk}) \in \mathrm{Mat_n(R)}$, fissati $i, j \le n$ sia Δ_{ij}^A il determinante della sottomatrice ottenuta da A sopprimendone la i-esima riga e la j-esima colonna.*

1) *Il* cofattore A_{ij} *di* a_{ij} *è definito mediante:*

$$A_{ij} := (-1)^{i+j}\Delta_{ij}^A.$$

2) *La* aggiunta ad A *di A è definita mediante:*

$$\mathrm{ad\ A} := (\mathrm{A_{ij}})^{\mathrm{t}} \ = \ \begin{pmatrix} A_{11} & \dots & A_{n1} \\ \dots & \dots & \dots \\ A_{1n} & \dots & A_{nn} \end{pmatrix}.$$

(2.2) Esempio $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $\mathrm{ad\ A} = \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$.

(2.3) Esempio $A = \begin{pmatrix} 1 & 0 & -1 \\ 4 & 2 & 3 \\ 0 & 1 & 1 \end{pmatrix}$, $\mathrm{ad\ A} = \begin{pmatrix} -1 & -1 & 2 \\ -4 & 1 & -7 \\ 4 & -1 & 2 \end{pmatrix}$.

(2.4) Teorema *(di Laplace) Per ogni matrice $A \in \mathrm{Mat_n(R)}$ si ha:*

$$A\,(\mathrm{ad\ A}) \ = \ (\mathrm{ad\ A})\,\mathrm{A} \ = \ (\det \mathrm{A})\,\mathrm{I}.$$

Tale Teorema fornisce, in particolare, lo sviluppo di $\det A$ secondo una sua qualunque riga o colonna. Alla sua dimostrazione dobbiamo premettere alcune considerazioni.

Fissato $i \in \{1,\dots,n\}$, si consideri il sottogruppo G_i del gruppo simmetrico $\mathrm{Sym}(n)$ costituito dalle permutazioni che fissano i. Chiaramente $G_i \sim \mathrm{Sym(n-1)}$. In simboli:

$$G_i := \{\sigma \in \mathrm{Sym(n)} \mid \sigma(\mathrm{i}) = \mathrm{i}\}\,. \tag{2.5}$$

I suoi laterali sinistri danno luogo alla seguente *partizione* di Sym(n):

$$\text{Sym(n)} \;=\; \text{(i1)G}_\text{i} \,\dot\cup\, \text{(i2)G}_\text{i} \,\dot\cup\, \ldots \,\dot\cup\, \text{(in)G}_\text{i}. \tag{2.6}$$

Infatti:

$$\begin{array}{rcl} (i1)G_i & = & \{\sigma \in \text{Sym(n)} \mid \sigma(\text{i}) = 1\} \\ (i2)G_i & = & \{\sigma \in \text{Sym(n)} | \sigma(\text{i}) = 2\} \\ \ldots & & \\ (in)G_i & = & \{\sigma \in \text{Sym(n)} | \sigma(\text{i}) = \text{n}\} \end{array} .$$

Per esempio, per $n = 3$, $j = 1$, si ha:

$$\text{Sym(3)} \;=\; \text{G}_1 \,\dot\cup\, (12)\text{G}_1 \,\dot\cup\, (13)\text{G}_1 \;=\; \{\text{id},\ (23)\} \,\dot\cup\, \{(12), (123)\} \,\dot\cup\, \{(13), (132)\}\,.$$

(2.7) Lemma *Per ogni $A = (a_{k\,h}) \in \text{Mat}_\text{n}(\text{R})$ e per ogni $i, j \in \{1, \ldots, n\}$ si ha:*

$$A_{ij} = \sum_{\tau \in (ij)G_i} \text{sg}(\tau) \prod_{\text{k}\neq\text{i}} \text{a}_{\text{k}\,\tau(\text{k})}. \tag{2.8}$$

Dimostrazione.

Se $i = j$ si ha evidentemente $A_{ii} = \Delta^A_{ii} = \sum_{\sigma\in G_i} sg(\sigma) \prod_{k\neq i} a_{k\,\sigma(k)}$.

Se $i \neq j$ supponiamo, per fissare le idee, $i < j$. Posto $j = i + r$ consideriamo la permutazione ciclica $\rho = (i, i+1, \ldots, i+r)$ e la matrice $B = (b_{k\,h})$ ottenuta da A applicando ρ alle sue colonne. Le entrate di B sono quindi cosí definite: $b_{k\,h} := a_{k\,\rho^{-1}(h)}$. Si ha allora:

$$\Delta^A_{ij} = \Delta^B_{ii} = \sum_{\sigma\in G_i} sg(\sigma) \prod_{k\neq i} b_{k\,\sigma(k)} = \sum_{\sigma\in G_i} sg(\sigma) \prod_{k\neq i} a_{k\,\rho^{-1}\sigma(k)}.$$

Poniamo $\tau := \rho^{-1}\sigma$. Si ha $\rho^{-1}G_i = (ij)G_i$, infatti $(ij)\rho^{-1} = (ij)(i, j, \ldots)$ fissa i. Inoltre

$$sg(\sigma) = sg(\rho\tau) = (-1)^{j-i} sg(\tau) = (-1)^{i+j} sg(\tau).$$

Si conclude

$$\Delta^A_{ij} = \sum_{\tau\in(ij)G_i} (-1)^{i+j} sg(\tau) \prod_{k\neq i} a_{k\,\tau(k)}$$

da cui l'asserto, moltiplicando per $(-1)^{i+j}$. ∎

Dimostrazione. (del Teorema di Laplace)

$\det A$ è l'elemento di posto (ii) del prodotto $A\,(\text{ad A})$, per ogni $i \leq n$. Infatti:

$$\det A := \sum_{\sigma \in \mathrm{Sym(n)}} \mathrm{sg}\,(\sigma) \prod_{\mathrm{k=1}}^{\mathrm{n}} \mathrm{a_{k\,\sigma(k)}} =$$

(considerando la partizione di Sym(n) fornita da (2.6))

$$\begin{array}{ll} a_{i1} \ \sum_{\sigma \in (i1)G_i} \mathrm{sg}(\sigma) \prod_{\mathrm{k} \neq \mathrm{i}} \mathrm{a_{k\,\sigma(k)}} & + \\ a_{i2} \ \sum_{\sigma \in (i2)G_i} \mathrm{sg}(\sigma) \prod_{\mathrm{k} \neq \mathrm{i}} \mathrm{a_{k\,\sigma(k)}} & + \\ \ldots & + \\ a_{in} \ \sum_{\sigma \in (in)G_i} \mathrm{sg}(\sigma) \prod_{\mathrm{k} \neq \mathrm{i}} \mathrm{a_{k\,\sigma(k)}} & = \end{array}$$

$$a_{i1}A_{i1} + \cdots + a_{in}A_{in} \ = \ \sum_{h=1}^{n} a_{ih}A_{ih}.$$

Abbiamo così ottenuto, in particolare, lo sviluppo di $\det A$ secondo la i-esima riga di A.

Resta da dimostrare che, per $i \neq j$, l'elemento di posto (ij) del prodotto $A\,(\text{ad A})$ è 0. A tale scopo consideriamo la matrice A' ottenuta da A sostituendo la j-esima riga con la i-esima riga. A' ha due righe uguali, quindi $\det A' = 0$. D' altra parte, sviluppando $\det A'$ secondo la j-esima riga, si ha:

$$0 \ = \ \det A' \ = \ \sum_{h=1}^{n} a_{ih}A_{jh}.$$

Abbiamo così dimostrato che $A\,(\text{ad A}) \ = \ (\det \mathrm{A})\,\mathrm{I}$.

Poichè tale relazione vale per ogni matrice, possiamo applicarla ad A^t, ottenendo $A^t\,(\text{ad } \mathrm{A^t}) = (\det \mathrm{A})\,\mathrm{I}$. Trasponendo, e notando che $\text{ad } \mathrm{A^t} = (\text{ad A})^{\mathrm{t}}$ si ha la relazione $(\text{ad A})\,\mathrm{A} = (\det \mathrm{A})\,\mathrm{I}$. ■

(2.9) Corollario $A \in \mathrm{Mat_n}(\mathbb{R})^* = \mathrm{GL_n(R)}$ *se e solo se* $\det A \in R^*$.

Dimostrazione.

Se $\det(A) \in R^*$, per il Teorema di Laplace la matrice A ha inversa

$$A^{-1} = \det(A)^{-1}\text{ad (A)}.$$

Viceversa, se A ha inversa, da $AA^{-1} = I$ segue, per il Teorema di Binet,

$$\det(A)\det(A)^{-1} = \det(I) = 1_R.$$

Si conclude che $\det A \in R^*$. ■

3 Fattori invarianti

Sia $A \in \mathrm{Mat_{m,n}(R)}$.

(3.1) Definizione *Per ogni $k \leq min\ (m,n)$:*

1*) un minore di ordine k di A è il determinante di una sottomatrice $k \times k$ di A;*

2) *$J_k(A)$ è l'ideale generato dai minori di ordine k di A.*

(3.2) Lemma *Siano $X \in \mathrm{Mat_m(R)}$, $Y \in \mathrm{Mat_n(R)}$. Per ogni $k \leq min\ (m,n)$.*

1) *$J_k(XA) \leq J_k(A)$;*

2) *$J_k(AY) \leq J_k(A)$;*

3) *se A è equivalente ad A', allora $J_k(A) = J_k(A')$.*

Dimostrazione.

1) Detti $a_1,\ \ldots,\ a_s$ i minori di ordine k di A e $b_1,\ \ldots,\ b_s$ quelli di XA, si ha:

$$J_k(A) = Ra_1 +,\ \ldots,\ +Ra_s, \quad J_k(XA) = Rb_1 +,\ \ldots,\ +Rb_s.$$

Ogni riga di XA è combinazione lineare, a coefficienti in R, delle righe di A. Quindi anche ogni sottoriga di XA è combinazione lineare di sottorighe di A. Poichè i determinanti sono lineari nelle righe, ne segue che ogni b_j è combinazione lineare degli a_j. Pertanto $J_k(XA) \leq J_k(A)$.

2) Idem, osservando che le colonne di AY sono combinazioni lineari di quelle di A.

3) Posto $A' = QAP$, con Q, P invertibili, si ha:

$$J_k(A') = J_k\left(Q(AP)\right) \leq J_k(AP) \leq J_k(A).$$

Reciprocamente, da $A = Q^{-1}A'P^{-1}$, segue $J_k(A) \leq J_k(A')$ e si conclude $J_k(A) = J_k(A')$.

■

Come abbiamo visto nel capitolo III, se $\lambda_1, \ldots, \lambda_s$ sono elementi di D^*, la matrice $\mathrm{diag}\,(\lambda_1, \ldots, \lambda_s)$ ha inversa. Ne segue la seguente equivalenza tra forme normali:

$$\mathrm{pseudodiag}\,(d_1,\ \ldots,\ d_s) \sim \mathrm{pseudodiag}\,(\lambda_1 d_1,\ \ldots,\ \lambda_s d_s)\,.$$

Viceversa, vale il seguente:

(3.3) Teorema *In $\mathrm{Mat_{m,n}(D)}$, si considerino due forme normali:*

$$N = \mathrm{pseudodiag}\,(d_1,\ \ldots,\ d_s)\,, \quad N' = \mathrm{pseudodiag}\left(d_1{}',\ \ldots,\ d_s{}'\right),$$

con $s = \min\{m, n\}$. *Se* N *è equivalente ad* N', *allora:*

$$d'_k = \lambda_k d_k, \quad \lambda_k \in D^* \quad (1 \leq k \leq s). \tag{3.4}$$

Dimostrazione.

Ricordando che, per definizione di forma normale

$$d_i | d_{i+1}, \quad d'_i | d'_{i+1} \qquad (1 \leq i \leq s-1) \tag{3.5}$$

si ha:

$$J_1(N) = Dd_1, \quad J_2(N) = Dd_1d_2, \quad \ldots, \quad J_s(N) = D\prod_{i=1}^{s} d_i.$$

$$J_1(N') = Dd'_1, \quad J_2(N') = Dd'_1d'_2, \quad \ldots, \quad J_s(N') = D\prod_{i=1}^{s} d'_i.$$

Per il Lemma precedente:

$$Dd_1 = Dd'_1, \quad Dd_1d_2 = Dd'_1d'_2, \quad \ldots, \quad D\prod_{i=1}^{s} d_i = D\prod_{i=1}^{s} d'_i. \tag{3.6}$$

L'asserto è evidente se N è la matrice nulla. Possiamo quindi supporre che t sia il massimo indice per cui $d_t \neq 0_{\mathbb{K}}$. Da (3.6) segue $d'_t \neq 0_{\mathbb{K}}$.

Dimostriamo innanzitutto che vale (3.4) per ogni $k \leq t$.

Per il punto 2) del Lemma 1.2, Capitolo 2, da (3.6) segue:

$$d'_1 = \lambda_1 d_1, \ \lambda_1 \in D^*, \quad \ldots, \quad \prod_{i=1}^{t} d'_i = \mu \prod_{i=1}^{t} d_i, \quad \lambda_i, \ \mu \in D^*.$$

In particolare (3.4) vale per $t = 1$. Se $t > 1$, induttivamente possiamo supporre che (3.4) valga per ogni $k \leq t-1$. Abbiamo quindi:

$$\left(\prod_{i=1}^{t-1} \lambda_i d_i\right) d'_t \ = \ \mu \left(\prod_{i=1}^{t-1} d_i\right) d_t, \quad \mu \in D^*.$$

Semplificando per $\prod_{i=1}^{t-1} d_i$ si ottiene $d'_t = \prod_{i=1}^{t-1} \lambda_i^{-1} \mu d_t$ dove $\lambda_t := \prod_{i=1}^{t-1} \lambda_i^{-1} \mu \in D^*$.

Infine, se $t < s$, da $d_{t+1} = 0_{\mathbb{K}}$ segue $d'_{t+1} = 0_{\mathbb{K}}$ in virtù di (3.6). E, per la condizione (3.5) si ha $d_k = d'_k = 0_{\mathbb{K}}$, per ogni $k \geq t+1$.

■

Per il Teorema 2.4 del Capitolo IV, ogni matrice A è equivalente a qualche forma normale, detta *forma normale* di A.

(3.7) Definizione *La matrice* $A \in \mathrm{Mat_{m,n}(D)}$ *sia equivalente alla forma normale*

$$\mathrm{pseudodiag}\,(d_1,\ \ldots,\ d_s)\,.$$

1) *La sequenza* $d_1,\ \ldots,\ d_s$ *si dice la sequenza dei* fattori invarianti *di* A *su* D*;*

2) *se* $d_t \neq 0_D$ *e* $d_{t+1} = 0_D$ *si dice che* A *ha* rango t*.*

In altre parole il rango di A è il numero dei suoi fattori invarianti non nulli.

Per quanto visto, due matrici A, B *sono equivalenti se e solo se hanno la stessa sequenza di fattori invarianti*, a meno di fattori unitari.

Il punto 3) del Lemma 3.2 dà un metodo per calcolarli. Infatti

- d_1 è il M.C.D. degli elementi di A;
- $d_1 d_2$ è il M.C.D. dei minori di ordine 2;
- $d_1 d_2 d_3$ è il M.C.D. dei minori di ordine 3, ecc...

(3.8) Teorema *La matrice* A *e la sua trasposta* A^t *hanno la stessa sequenza di fattori invarianti. In particolare:*

$$\text{rango di } A \ = \ \text{rango di } A^t.$$

Dimostrazione. Sia A' una forma normale di A. Poichè A' è equivalente ad A, esistono due matrici invertibili Q, P tali che $A = QA'P$. Ne segue $A^t = P^t(A')^t Q^t$, ossia $(A')^t$ è equivalente ad A^t. Poichè la trasposta di una forma normale è , a sua volta, una forma normale, si ha che $(A')^t$ è una forma normale di A^t. Chiaramente A' e $(A')^t$ hanno gli stessi fattori invarianti, da cui l'asserto. ■

Il fatto che gli unici ideali di un campo $\mathbb{K}$ siano $\mathbb{K}$ e $\{0_K\}$ ha la seguente conseguenza.

(3.9) Osservazione *La sequenza dei fattori invarianti di una matrice* $A \in \mathrm{Mat_{m,n}}(\mathbb{K})$ *è del tipo:* $\mathbb{K},\ \ldots,\ \mathbb{K}, \{0_K\},\ \ldots,\ \{0_K\}$*, ossia*

$$1_{\mathbb{K}},\ \ldots,\ 1_{\mathbb{K}}, 0_K,\ \ldots,\ 0_K.$$

Ne segue che A *è equivalente a una e una sola matrice di uno dei seguenti tipi:*

$$I_r,\ \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix},\ \begin{pmatrix} I_r & 0 \end{pmatrix},\ \begin{pmatrix} I_r \\ 0 \end{pmatrix}$$

dove r *è il rango di* A*.*

(3.10) Corollario *Sia* $\mathbb{K}$ *è un campo. Il gruppo* $\mathrm{GL_n}(\mathbb{K})$ *delle matrici invertibili di* $\mathrm{Mat_n}(\mathbb{K})$ *è costituito dalle matrici di rango* n*.*

Dimostrazione.

Sia $A \in \mathrm{GL_n}(\mathbb{K})$. Ne segue che A è equivalente ad $IAA^{-1} = I$. Pertanto I è una forma normale di A. Si conclude che A ha rango n. Viceversa, se A ha rango n, una sua forma normale è I. Pertanto esistono P, Q invertibili tali che $QAP = I$. Si conclude che $A = Q^{-1}P^{-1}$ ha inversa. ■

(3.11) Esempio *In* $\mathrm{Mat}_2(\mathbb{Z})$ *la matrice* $A = \begin{pmatrix} 1 & 3 \\ -2 & 1 \end{pmatrix}$ *ha forma normale*

$$\begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}.$$

Infatti $J_1(A) = M.C.D.(1, 3, -2)=1$. $J_2(A) = \det(A) = 7$.

Le forme normali di A sono:

$$\begin{pmatrix} 1 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -7 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -7 \end{pmatrix}.$$

La sequenza dei fattori invarianti di A è $1, 7$. *Il suo rango è 2.*

(3.12) Esempio *In* $\mathrm{Mat}_2(\mathbb{Q})$ *la matrice* $A = \begin{pmatrix} 1 & 3 \\ -2 & 1 \end{pmatrix}$ *ha forma normale*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Le forme normali di A sono:

$$\begin{pmatrix} q_1 & 0 \\ 0 & q_2 \end{pmatrix}, \ q_1 q_2 \neq 0.$$

La sequenza dei fattori invarianti di A è $1, 1$. *Il rango è 2.*

Elenco dei simboli

Indice analitico

Bibliografia

[1] B.Hartley, T.O.Hawkes, Rings, Modules and Linear Algebra, Chapman and Hall, 1970.

[2] N.Jacobson, Basic Algebra I, W.H.Freeman and company, San Francisco,1974.

[3] M.C. Tamburini, Appunti di Algebra, Pubblicazioni dell' I.S.U. Iniversità Cattolica (2000).

[4] M.C. Tamburini, Algebra I unità .