

Capitolo 4

Anelli, corpi e campi

4.1 Anelli

Esempio 580 Consideriamo l'insieme Z . Sappiamo che in Z sono definite due operazioni binarie:

l'operazione di addizione $+$ e l'operazione di moltiplicazione \cdot .

Tali operazioni hanno le seguenti proprietà:

1) $(Z, +)$ è un gruppo abeliano.

2) (Z, \cdot) è un semigrupp. La moltiplicazione verifica cioè la proprietà associativa:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a \in Z \quad \forall b \in Z \quad \forall c \in Z$$

3) proprietà distributive:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a \in Z \quad \forall b \in Z \quad \forall c \in Z$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a \in Z \quad \forall b \in Z \quad \forall c \in Z$$

La prossima definizione è una generalizzazione dell'esempio precedente.

Definizione 581 Un **anello** è una terna $(A, +, \cdot)$ dove A è un insieme, $+$ e \cdot sono due operazioni binarie verificanti le seguenti condizioni:

1) $(A, +)$ è un gruppo abeliano.

2) (A, \cdot) è un semigrupp. La moltiplicazione verifica cioè la proprietà associativa:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a \in A \quad \forall b \in A \quad \forall c \in A$$

3) proprietà distributive:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a \in A \quad \forall b \in A \quad \forall c \in A$$

$$(b + c) \cdot a = b \cdot a + c \cdot a \quad \forall a \in A \quad \forall b \in A \quad \forall c \in A$$

Nota 582 Nello scrivere le proprietà distributive abbiamo la stessa convenzione usata nel caso di Z . Quando si hanno le operazioni di addizione di moltiplicazione, prima si fa la moltiplicazione e poi l'addizione.

Nel caso in cui si voglia fare prima l'addizione e poi la moltiplicazione si mettono le parentesi.

Nota 583 Sia $(A, +, \cdot)$ un anello. Abbiamo visto che ciò implica che $(A, +)$ è un gruppo abeliano. Esiste quindi l'elemento neutro rispetto all'operazione $+$. Poiché abbiamo adoperato la notazione additiva, indichiamo l'elemento neutro con il simbolo 0 . Dato poi un qualsiasi elemento $a \in A$ esiste il suo simmetrico, che chiamiamo **opposto** di a e indichiamo con il simbolo $-a$.

Definizione 584 Dato un anello $(A, +, \cdot)$, se (A, \cdot) è un monoide, cioè se l'operazione \cdot , oltre ad essere associativa, è dotata di elemento neutro, diciamo che l'anello A è dotato di **unità**. Indichiamo l'unità con il simbolo 1 . L'unità di un anello, quando esiste, ha la seguente proprietà:

$$a \cdot 1 = 1 \cdot a = a \quad \forall a \in A$$

Un anello si dice **commutativo** se l'operazione \cdot è commutativa, cioè se:

$$a \cdot b = b \cdot a \quad \forall a \in A \quad \forall b \in A$$

Esempio 585 Diamo alcuni esempi di anelli.

- 1) Abbiamo già detto che $(Z, +, \cdot)$ è un anello. Esso è commutativo e ha l'unità.
- 2) $(Q, +, \cdot)$ è un anello commutativo con unità.
- 3) $(R, +, \cdot)$ è un anello commutativo con unità.
- 4) $(C, +, \cdot)$ è un anello commutativo con unità.
- 5) $(nZ, +, \cdot)$, con $n \in N$, è un anello commutativo. Se $n \neq 1$ non vi è unità.
- 6) $(M(R, n, n), +, \cdot)$ è un anello non commutativo con unità.
- 7) $(M(Z, n, n), +, \cdot)$ è un anello non commutativo con unità.
- 8) $(M(Q, n, n), +, \cdot)$ è un anello non commutativo con unità.
- 9) $(M(C, n, n), +, \cdot)$ è un anello non commutativo con unità.
- 10) $(Z_n, +, \cdot)$, con $n \in N$, è un anello commutativo con unità.
- 11) $(R[x], +, \cdot)$, dove $R[x]$ è l'insieme dei polinomi a coefficienti in R , è un anello commutativo con unità.

Esercizio 586 Verificare le 11 affermazioni precedenti.

Esempio 587 [L'anello degli endomorfismi di un gruppo.]

Sia $(G, +)$ un gruppo abeliano. Ricordiamo che $\text{End}(G)$ è l'insieme degli endomorfismi di G . Vogliamo introdurre in $\text{End}(G)$ due operazioni in modo tale da renderlo un anello.

Introduciamo innanzitutto la prima operazione che indichiamo con $+$. Dati quindi $f \in \text{End}(G)$ e $g \in \text{End}(G)$, dobbiamo definire $f + g \in \text{End}(G)$. Dato $a \in G$, definiamo:

$$(f + g)(a) = f(a) + g(a)$$

Dobbiamo dimostrare che $f + g$ è un endomorfismo di G . Lasciamo la dimostrazione di ciò per esercizio.

Dimostriamo ora che $(\text{End}(G), +)$ è un gruppo abeliano.

Verifichiamo la proprietà associativa. Dobbiamo dimostrare che si ha:

$$f + (g + h) = (f + g) + h \quad \forall f \in \text{End}(G) \quad \forall g \in \text{End}(G) \quad \forall h \in \text{End}(G)$$

Abbiamo due funzioni $f + (g + h)$ e $(f + g) + h$. Sappiamo che due funzioni sono uguali se e solo se esse coincidono su ogni $a \in G$. Dobbiamo quindi dimostrare che si ha:

$$[f + (g + h)](a) = [(f + g) + h](a) \quad \forall a \in G$$

Svolgiamo i calcoli. Abbiamo:

$$\begin{aligned} [f + (g + h)](a) &= \text{(per definizione di addizione in } \text{End}(G)) \\ &= f(a) + (g + h)(a) = \text{(per definizione di addizione in } \text{End}(G)) \\ &= f(a) + [g(a) + h(a)] = \text{(per la proprietà associativa in } G) \\ &= [f(a) + g(a)] + h(a) = \text{(per definizione di addizione in } \text{End}(G)) \\ &= [(f + g)(a)] + h(a) = \text{(per definizione di addizione in } \text{End}(G)) \\ &= [(f + g) + h](a). \end{aligned}$$

Abbiamo dimostrato quel che volevamo.

Dobbiamo ora dimostrare che in $\text{End}(G)$ c'è l'elemento neutro.

Consideriamo l'endomorfismo nullo di G . L'endomorfismo nullo associa ad ogni elemento di G l'elemento 0 di G . Indichiamo l'omomorfismo con il simbolo 0 . Abbiamo quindi, per definizione di omomorfismo nullo:

$$0(a) = 0 \quad \forall a \in G$$

Si verifica facilmente che si ha:

$$f + 0 = 0 + f = f \quad \forall f \in \text{End}(G)$$

L'omomorfismo nullo è quindi l'elemento neutro di $(\text{End}(G), +)$. Dobbiamo ora dimostrare che per ogni $f \in \text{End}(G)$ esiste un elemento simmetrico rispetto all'addizione in $\text{End}(G)$.

Dato $f \in \text{End}(G)$, definiamo un'applicazione:

$$-f : G \longrightarrow G$$

nel modo seguente:

$$(-f)(a) = -f(a) \quad \forall a \in G$$

Lasciamo come esercizio la dimostrazione che $-f$ è un endomorfismo di G . Si verifica poi facilmente (esercizio) che si ha:

$$f + (-f) = -f + f = 0$$

Quindi $-f$ è il simmetrico di f .

Dobbiamo ora dimostrare che l'operazione $+$ in $\text{End}(G)$ è commutativa. Lasciamo la dimostrazione di ciò per esercizio.

Abbiamo finito di dimostrare che $(\text{End}(G), +)$ è un gruppo abeliano.

La seconda operazione che introduciamo in $\text{End}(G)$ è la composizione di endomorfismi. Abbiamo visto nel terzo capitolo che la composizione di endomorfismi è un endomorfismo. Abbiamo anzi visto che $(\text{End}(G), \circ)$ è un gruppoide associativo dotato di elemento neutro. L'elemento neutro è dato dall'identità di G . Dobbiamo ora dimostrare che, $\forall f \in \text{End}(G), \forall g \in \text{End}(G), \forall h \in \text{End}(G)$, sono valide le proprietà distributive:

$$f \circ (g + h) = f \circ g + f \circ h$$

$$(g + h) \circ f = g \circ f + h \circ f$$

Lasciamo la dimostrazione di ciò per esercizio.

Abbiamo quindi dimostrato che $(\text{End}(G), +, \circ)$ è un anello con unità. Questo anello non è commutativo. Sappiamo infatti che la composizione tra funzioni non è commutativa.

Teorema 588 Dato un anello $(A, +, \cdot)$ si ha:

$$1) a \cdot 0 = 0 \cdot a = 0 \quad \forall a \in A$$

$$2) a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$$

DIMOSTRAZIONE.

1) Sappiamo che si ha $0 + 0 = 0$. Da ciò segue, per ogni $a \in A$:

$$a \cdot 0 = a \cdot (0 + 0)$$

Applicando la proprietà distributiva otteniamo:

$$a \cdot 0 = a \cdot 0 + a \cdot 0$$

Sommando ad ambo i membri $-(a \cdot 0)$ otteniamo:

$$0 = a \cdot 0$$

In modo analogo si dimostra (esercizio) che si ha $0 = 0 \cdot a$.

2) Dobbiamo dimostrare che $a \cdot (-b)$ è l'opposto di $a \cdot b$. Dobbiamo cioè dimostrare che si ha:

$$a \cdot (-b) + a \cdot b = a \cdot b + a \cdot (-b) = 0$$

Applicando la proprietà distributiva otteniamo:

$$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0 = 0$$

Notiamo che nell'ultima uguaglianza abbiamo utilizzato ciò che avevamo appena dimostrato in 1).

In modo analogo si dimostra che si ha:

$$a \cdot b + a \cdot (-b) = 0$$

Si deve ora dimostrare che $(-a) \cdot b$ è l'opposto di $a \cdot b$.

Lasciamo ciò per esercizio. \square

Esempio 589 Sia A un insieme formato da un solo elemento che indichiamo con a . Definiamo in A le operazioni $+$ e \cdot ponendo:

$$a + a = a, \quad a \cdot a = a$$

Si verifica facilmente che $(A, +, \cdot)$ è un anello commutativo con unità. Si ha $a = 0 = 1$.

Teorema 590 Se $(A, +, \cdot)$ è un anello dotato di almeno due elementi e se A è dotato di unità 1 , allora $1 \neq 0$.

DIMOSTRAZIONE. Supponiamo per assurdo che si abbia $0 = 1$. Allora, per ogni $a \in A$ si ha:

$$a \cdot 0 = a \cdot 1$$

Ma in un anello si ha $a \cdot 0 = 0$. D'altronde, per definizione di unità, si ha $a \cdot 1 = a$. da tutto ciò segue $0 = a$. Quindi A è formato da un solo elemento. Assurdo. \square

Abbiamo visto nel teorema 588 che in un anello si ha:

$$a = 0 \quad \text{oppure} \quad b = 0 \implies a \cdot b = 0$$

Ci chiediamo se è vero il viceversa. Si ha cioè:

$$a \cdot b = 0 \implies a = 0 \quad \text{oppure} \quad b = 0?$$

Nel caso degli anelli dei reali o degli interi ciò è vero. Ma ciò non è vero per ogni anello.

Esempio 591 Esistono $A \in M(R, 2, 2)$ e $B \in M(R, 2, 2)$ tali che

$$A \neq 0, B \neq 0 \text{ e tali che } A \cdot B = 0$$

Si lascia la determinazione di tali matrici per esercizio.

Definizione 592 Un elemento $a \neq 0$ di un anello $(A, +, \cdot)$ si dice **divisore dello zero** se si ha esiste in A un elemento $b \neq 0$ tale che si abbia $a \cdot b = 0$ oppure $b \cdot a = 0$.

Un anello privo di divisori dello zero si dice **anello di integrità**.

Esempio 593 Gli anelli $(R, +, \cdot)$ e $(Z, +, \cdot)$ sono di integrità.

L'anello $(M(R, n, n), +, \cdot)$ con $n > 1$ non è di integrità.

Esercizio 594 Verificare che l'anello $(Z_4, +, \cdot)$ non è un anello di integrità.

Verificare che, se n è un numero non primo, l'anello $(Z_n, +, \cdot)$ non è un anello di integrità.

Definizione 595 Un anello A si dice avere le **leggi di semplificazione** se, fissato $0 \neq a \in A$, si ha:

$$a \cdot b = a \cdot c \implies b = c$$

$$b \cdot a = c \cdot a \implies b = c$$

Esempio 596 Gli anelli $(R, +, \cdot)$ e $(Z, +, \cdot)$ hanno le leggi di semplificazione. L'anello $(M(R, n, n), +, \cdot)$, con $n > 1$, non ha la legge di semplificazione. Si lascia come esercizio la dimostrazione di ciò.

Teorema 597 Un anello $(A, +, \cdot)$ con almeno due elementi ha la legge di semplificazione se e solo se è un anello di integrità.
DIMOSTRAZIONE. Lasciata per esercizio. \square

Esercizio 598 Sia $(A, +, \cdot)$ un anello con almeno due elementi dotato di unità. Verificare che 0 non è dotato di inverso.
Verificare che, se a è un divisore dello zero, allora a non è dotato di inverso.

4.2 Sottoanelli

Definizione 599 Sia $(A, +, \cdot)$ un anello e sia $H \subset A$. Si dice che H è un **sottoanello** di A se H è chiuso rispetto alle operazioni $+$ e \cdot di A e se $(H, +, \cdot)$ è un anello.

Nota 600 Se H è un sottoanello di un anello $(A, +, \cdot)$, allora $(H, +)$ è un sottogruppo del gruppo $(A, +)$.
Notiamo inoltre che, poiché $(A, +)$ è un gruppo abeliano, allora H è un suo sottogruppo normale.

Esempio 601 Diamo alcuni esempi di sottoanelli.

- 1) Z è un sottoanello di $(Q, +, \cdot)$.
- 2) Q è un sottoanello di $(R, +, \cdot)$.
- 3) R è un sottoanello di $(C, +, \cdot)$.
- 4) nZ è un sottoanello di $(Z, +, \cdot)$. Ricordiamo che nZ è dato dai multipli di n .

Teorema 602 Sia $(A, +, \cdot)$ un anello e sia $H \subset A$. Si ha che H è un sottoanello di $(A, +, \cdot)$ se e solo se sono verificate le seguenti condizioni:

- 1) $H \neq \emptyset$
- 2) $h \in H, h' \in H \implies h + h' \in H$
- 3) $h \in H \implies -h \in H$
- 4) $h \in H, h' \in H \implies h \cdot h' \in H$

DIMOSTRAZIONE. Lasciata per esercizio. \square

Teorema 603 Dato un anello $(A, +, \cdot)$, siano H e H' suoi sottoanelli. Allora $H \cap H'$ è un sottoanello di A .

DIMOSTRAZIONE. Lasciata per esercizio. \square

Esercizio 604 E' vero che l'unione di due sottoanelli di un anello $(A, +, \cdot)$ è un sottoanello di A ?

4.3 Ideali

Definizione 605 Un sottoanello H di un anello $(A, +, \cdot)$ si dice **ideale** se si ha:

$$a \in A, h \in H \implies a \cdot h \in H, h \cdot a \in H$$

Esempio 606 Il sottoanello nZ di $(Z, +, \cdot)$ è un ideale.
La verifica di ciò viene lasciata per esercizio.

Teorema 607 Se H è un ideale di un anello $(A, +, \cdot)$ dotato di unità 1 e se $1 \in H$, allora $H = A$.

DIMOSTRAZIONE. Esercizio. \square

4.4 Anelli quozienti

Definizione 608 Sia $(A, +, \cdot)$ un anello e sia \sim una relazione di equivalenza in A . La relazione di equivalenza \sim si dice **compatibile** con le operazioni di A se si ha:

$$a \sim a', b \sim b' \implies a + b \sim a' + b', a \cdot b \sim a' \cdot b'$$

Definizione 609 Dato un anello $(A, +, \cdot)$ e una relazione di equivalenza \sim compatibile con le operazioni di A , chiamiamo **operazioni su A/\sim indotte** dalle operazioni di A le seguenti operazioni:

$$[a] + [b] = [a + b]$$

$$[a] \cdot [b] = [a \cdot b]$$

Nota 610 Si verifica facilmente che le definizioni delle due operazioni sono ben poste.

Teorema 611 Sia $(A, +, \cdot)$ un anello e sia \sim una relazione di equivalenza su A compatibile con le operazioni su A . Abbiamo quindi su A/\sim le operazioni indotte dalle operazioni di A . Si ha:

- 1) $(A/\sim, +, \cdot)$ è un anello.
- 2) Se A è un anello commutativo, anche A/\sim è un anello commutativo.
- 3) Se A è un anello con unità 1, allora $[1]$ è l'unità dell'anello A/\sim .

DIMOSTRAZIONE. Lasciata per esercizio. \square

Teorema 612 Sia $(A, +, \cdot)$ un anello e sia H un ideale. Sia \sim la relazione di equivalenza di A definita da:

$$a \sim a' \iff a - a' \in H$$

Questa relazione di equivalenza è compatibile con le operazioni definite in A .

DIMOSTRAZIONE. Poiché $(A, +)$ è un gruppo abeliano, abbiamo che H è un sottogruppo normale di $(A, +)$. Dal teorema 453 segue che la relazione \sim

è compatibile con l'operazione $+$ di A . Notiamo, tra l'altro, che per avere la compatibilità di \sim con $+$ non è necessario che H sia un ideale. Basta che $(H, +)$ sia un sottogruppo di $(A, +)$.

Vogliamo ora dimostrare che \sim è compatibile con l'operazione di moltiplicazione. Sia $a \sim a'$ e $b \sim b'$. Si ha quindi $a - a' = h \in H$ e $b - b' = h' \in H$. Dobbiamo dimostrare che si ha $a \cdot b - a' \cdot b' \in H$.

Abbiamo:

$$\begin{aligned} a \cdot b - a' \cdot b' &= a \cdot b - a' \cdot b + a' \cdot b - a' \cdot b' = \\ &= (a - a') \cdot b + a' \cdot (b - b') = h \cdot b + a' \cdot h'. \end{aligned}$$

Ricordiamo che H è un ideale, quindi $h \cdot b \in H$ e $a' \cdot h' \in H$. Ma allora, poiché H è chiuso rispetto all'addizione, si ha $h \cdot b + a' \cdot h' \in H$. Abbiamo dimostrato quel che volevamo. \square

Teorema 613 Sia $(A, +, \cdot)$ un anello e sia H un suo ideale. Sia \sim la relazione definita da:

$$a \sim a' \iff a - a' \in H$$

Allora l'insieme A/\sim ha come elementi le classi laterali di A relative a H :

$$[a] = a + H$$

Indichiamo tale insieme con il simbolo A/H .

Le operazioni indotte su A/H sono date da:

$$(a + H) + (b + H) = (a + b) + H$$

$$(a + H) \cdot (b + H) = (a \cdot b) + H$$

Si ha inoltre che $(A/H, +, \cdot)$ è un anello.

DIMOSTRAZIONE. Esercizio. Vedere la definizione 454 del capitolo 3. \square

Esempio 614 Consideriamo l'anello $(Z, +, \cdot)$ e sia $n \in N$. Abbiamo visto che nZ è un ideale. Pertanto Z/nZ è un anello.

Ricordiamo peraltro che si ha $Z/nZ = Z_n$.

4.5 Omomorfismi tra anelli

Definizione 615 Siano $(A, +, \cdot)$ e $(A', +, \cdot)$ anelli.

Una funzione $f : A \longrightarrow A'$ si dice omomorfismo tra anelli se sono verificate le seguenti proprietà:

$$f(a + b) = f(a) + f(b), \quad f(a \cdot b) = f(a) \cdot f(b) \quad \forall a \in A, \quad \forall b \in A$$

Spesso, per mettere in evidenza le operazioni dei due anelli, si scrive:

$$f : (A, +, \cdot) \longrightarrow (A', +, \cdot)$$

Un **isomorfismo** tra anelli è un omomorfismo tra anelli che sia una funzione biunivoca.

Due anelli si dicono **isomorfi** se esiste un isomorfismo tra essi.

Nota 616 Un omomorfismo $f : (A, +, \cdot) \longrightarrow (A', +, \cdot)$ tra anelli è, in particolare, un omomorfismo tra i gruppi con l'operazione di addizione.

Teorema 617 Dati i seguenti omomorfismi tra anelli:

$$\begin{aligned} f : (A, +, \cdot) &\longrightarrow (A', +, \cdot) \\ g : (A', +, \cdot) &\longrightarrow (A'', +, \cdot) \end{aligned}$$

si ha che:

$$g \circ f : (A, +, \cdot) \longrightarrow (A'', +, \cdot)$$

è un omomorfismo tra anelli.

DIMOSTRAZIONE. Lasciata per esercizio. \square

Teorema 618 Dato un isomorfismo tra anelli:

$$f : (A, +, \cdot) \longrightarrow (A', +, \cdot)$$

si ha che:

$$f^{-1} : (A', +, \cdot) \longrightarrow (A, +, \cdot)$$

è un isomorfismo tra anelli.

DIMOSTRAZIONE. Lasciata per esercizio. \square

Esercizio 619 Dimostrare che la relazione di isomorfismo tra anelli è una relazione di equivalenza.

Nota 620 Un omomorfismo f tra anelli è, in particolare, un omomorfismo tra gruppi. Possiamo quindi considerare $\ker f$ e $\operatorname{Im} f$.

Teorema 621 Sia $f : (A, +, \cdot) \longrightarrow (B, +, \cdot)$ un omomorfismo tra anelli. Allora:

- 1) $\ker f$ è un ideale di A .
- 2) $\operatorname{Im} f$ è un sottoanello di B .

DIMOSTRAZIONE. Lasciata per esercizio. \square

Teorema 622 [Teorema dell'omomorfismo tra anelli] Dato un omomorfismo tra anelli:

$$f : (A, +, \cdot) \longrightarrow (B, +, \cdot)$$

si ha che:

- 1) La relazione di equivalenza in A definita da:

$$a \sim a' \iff f(a) = f(a')$$

è compatibile con le operazioni in A .

- 2) $A/\sim = A/\ker f$
- 3) $(A/\ker f, +, \cdot)$ è un anello.
- 4) La funzione:

$$\pi : (A, +, \cdot) \longrightarrow (A/\ker f, +, \cdot)$$

definita da $\pi(a) = a + \ker f$ è un omomorfismo surgettivo tra anelli.

5) La funzione:

$$g : (A/\ker f, +, \cdot) \longrightarrow (B' = \operatorname{Im} f, +, \cdot)$$

definita da $g[a + \ker f] = f(a)$ è un isomorfismo tra anelli.

6) La funzione:

$$i : (B', +, \cdot) \longrightarrow (B, +, \cdot)$$

definita da $i(b') = b'$ è un omomorfismo iniettivo tra anelli.

7) Si ha infine:

$$f = i \circ g \circ \pi$$

DIMOSTRAZIONE. Una buona parte della dimostrazione è già stata fatta nel teorema 568 del capitolo 3. Si lascia per esercizio ciò che rimane della dimostrazione. \square

4.6 Corpi e campi

Definizione 623 Un anello $(K, +, \cdot)$ si dice **corpo** se esso è dotato di unità ed ogni elemento non nullo è dotato di inverso.

Un corpo commutativo si dice **campo**.

Nota 624 Dato un corpo K , indichiamo con K^* l'insieme degli elementi non nulli. Quindi $K^* = K - \{0\}$.

Si verifica (esercizio) che si ha che (K^*, \cdot) è un gruppo.

Teorema 625 Un corpo è privo di divisori dello zero.

DIMOSTRAZIONE. Lasciata per esercizio. \square

Esempio 626 1) $(\mathbb{Z}, +, \cdot)$ è un anello commutativo con unità ma non è un campo. Infatti i soli 1 e -1 sono dotati di inverso.

2) $(\mathbb{Q}, +, \cdot)$ è un campo.

3) $(\mathbb{R}, +, \cdot)$ è un campo.

4) $(\mathbb{C}, +, \cdot)$ è un campo.

Teorema 627 L'anello $(\mathbb{Z}_n, +, \cdot)$ è un campo se e solo se n è un numero primo.

DIMOSTRAZIONE. Lasciata per esercizio. \square

Teorema 628 Se H è un ideale di un campo K . Allora $H = \{0\}$ oppure $H = K$.

DIMOSTRAZIONE. Sia $H \neq \{0\}$. Sia quindi $0 \neq a \in H$. Esiste quindi l'inverso di a . Sia a^{-1} . Si ha $a^{-1} \in K$ e $a \in H$. Da ciò segue, essendo H un ideale, che si ha $1 = a \cdot a^{-1} \in H$. Ma allora, dal teorema 607 segue $H = K$. \square

Teorema 629 Sia $f : (K, +, \cdot) \longrightarrow (B, +, \cdot)$ un omomorfismo tra anelli. Se K è un campo, allora f o è l'omomorfismo nullo o è iniettivo.

DIMOSTRAZIONE. Lasciata per esercizio. Suggerimento: considerare il nucleo dell'omomorfismo ed applicare il teorema precedente. \square

4.7 Equazioni lineari in un campo

Teorema 630 Sia $(K, +, \cdot)$ un campo. Sia $a \in K^*$ e $b \in K$. Allora l'equazione lineare nella incognita x :

$$a \cdot x = b$$

ha una ed una sola soluzione. Essa è data da:

$$x = a^{-1} \cdot b$$

DIMOSTRAZIONE. Lasciata per esercizio. \square

Nota 631 L'equazione a coefficienti in un campo K nella incognita x del tipo:

$$a \cdot x + b = c$$

si riconduce all'equazione lineare:

$$a \cdot x = b'$$

ponendo $b' = c - b$.

Nota 632 L'equazione a coefficienti in un campo K nell'incognita x :

$$0 \cdot x = b$$

non ha soluzioni se $b \neq 0$.

Se invece $b = 0$, ogni $x \in K$ è soluzione dell'equazione.

La verifica di ciò è lasciata per esercizio.

Esempio 633 Vogliamo determinare tutti i numeri interi x tali che:

$$2 \cdot x + 1 \equiv 4 \pmod{5}$$

L'equazione di congruenze è equivalente alla seguente:

$$[2 \cdot x + 1]_5 = [4]_5$$

Utilizzando le operazioni di addizione e moltiplicazione nel campo Z_5 , si nota che l'equazione precedente coincide con la seguente equazione a coefficienti nel campo Z_5 :

$$[2]_5 \cdot [x]_5 + [1]_5 = [4]_5$$

Sottraendo ad ambo i membri $[1]_5$ otteniamo:

$$[2]_5 \cdot [x]_5 = [3]_5$$

Moltiplicando ambo i membri per $[2]_5^{-1} = [3]_5$, otteniamo:

$$[x]_5 = [3]_5 \cdot [3]_5 = [9]_5 = [4]_5$$

Tornando in Z otteniamo tutte le soluzioni dell'equazione originale:

$$x = 4 + 5h \mid h \in Z$$

Esercizio 634 Determinare tutti i numeri interi x tali che:

$$2 \cdot x + 4 \equiv 3 \pmod{5}$$

Esercizio 635 Determinare tutti i numeri interi x tali che:

$$20 \cdot x + 7 \equiv 3 \pmod{71}$$

Esercizio 636 È vera la seguente affermazione:

$$a \cdot c \equiv b \cdot c \pmod{n} \iff a \equiv b \pmod{n}?$$

4.8 Sistemi di equazioni lineari

Teorema 637 Sia dato un sistema di p equazioni lineari in q incognite a coefficienti in un campo K :

$$A \cdot X = B$$

dove $A \in M(K, p, q)$ è la matrice dei coefficienti, $X \in M(K, q, 1)$ è la matrice delle incognite e $B \in M(K, p, 1)$ è la matrice dei termini noti.

Per determinarne le eventuali soluzioni si possono utilizzare gli algoritmi di Cramer, Rouché-Capelli, di Gauss e di Gauss-Jordan studiati nel corso del primo anno nel caso di sistemi di equazioni lineari a coefficienti in un campo.

DIMOSTRAZIONE. Andare a rivedere le dimostrazioni degli algoritmi citati e rendersi conto che in esse si sono sfruttate esclusivamente le proprietà di campo dei reali. \square

Diamo un esempio di applicazione dell'algoritmo di Rouché-Capelli.

Esempio 638 Vogliamo determinare le eventuali soluzioni del seguente sistema a coefficienti in R :

$$S : \begin{cases} x_1 + x_2 + x_3 + 2x_4 = 5 \\ 2x_1 + 2x_2 + x_3 + 3x_4 = 8 \\ 4x_1 + 4x_2 + 3x_3 + 7x_4 = 18 \\ x_1 + x_2 + x_4 = 3 \end{cases}$$

Determiniamo la matrice A dei coefficienti di S e la matrice completa A' di S .

$$A = \begin{pmatrix} 1 & 1 & 1 & 2 \\ 2 & 2 & 1 & 3 \\ 4 & 4 & 3 & 7 \\ 1 & 1 & 0 & 1 \end{pmatrix} \quad A' = \begin{pmatrix} 1 & 1 & 1 & 2 & 5 \\ 2 & 2 & 1 & 3 & 8 \\ 4 & 4 & 3 & 7 & 18 \\ 1 & 1 & 0 & 1 & 3 \end{pmatrix}$$

Facendo i calcoli si verifica che si ha:

$$\text{rk}(A) = \text{rk}(A') = 2$$

Dal teorema di Rouché-Capelli segue che il sistema S ha soluzioni.

Il minore C di ordine 2 di A formato dalle prime due righe e dalla seconda e

terza colonna è invertibile.

Consideriamo allora il sistema ridotto formato dalle prime due equazioni:

$$SR: \begin{cases} x_1 + x_2 + x_3 + 2x_4 = 5 \\ 2x_1 + 2x_2 + x_3 + 3x_4 = 8 \end{cases}$$

Il teorema di Rouché-Capelli ci dice che si ha:

$$Sol(S) = Sol(SR)$$

Il teorema di Rouché-Capelli ci dice che si ha:

$$Sol(SR) = X_0 + Sol(SO)$$

dove X_0 è una soluzione di SR e SO è il sistema omogeneo associato.

Il teorema di Rouché-Capelli ci dice come determinarla. In SR poniamo $x_1 = x_4 = 0$ (sono le incognite i cui coefficienti non servono a formare il minore C). Otteniamo

$$\begin{cases} x_2 + x_3 = 5 \\ 2x_2 + x_3 = 8 \end{cases}$$

Questo sistema ha come soluzione $x_2 = 3$, $x_3 = 2$. Quindi:

$$X_0 = \begin{pmatrix} 0 \\ 3 \\ 2 \\ 0 \end{pmatrix}$$

è una soluzione di SR .

Consideriamo ora il sistema omogeneo associato al sistema SR :

$$SO: \begin{cases} x_1 + x_2 + x_3 + 2x_4 = 0 \\ 2x_1 + 2x_2 + x_3 + 3x_4 = 0 \end{cases}$$

Seguendo l'algoritmo descritto nel teorema di Rouché-Capelli, determiniamo le soluzioni di SO . In SO poniamo $x_1 = 1$ e $x_4 = 0$. Otteniamo il sistema:

$$\begin{cases} x_2 + x_3 = -1 \\ 2x_2 + x_3 = -2 \end{cases}$$

Esso ha come soluzione $x_2 = -1$, $x_3 = 0$. Quindi:

$$X_1 = \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix}$$

è una soluzione di SO . In SO poniamo $x_1 = 0$, $x_4 = 1$. Otteniamo il sistema:

$$\begin{cases} x_2 + x_3 = -2 \\ 2x_2 + x_3 = -3 \end{cases}$$

Esso ha come soluzione $x_2 = -1$, $x_3 = -1$. Quindi:

$$X_2 = \begin{pmatrix} 0 \\ -1 \\ -1 \\ 1 \end{pmatrix}$$

Il teorema di Rouché-Capelli ci dice che si ha:

$$\text{Sol}(SO) = \{h_1 X_1 + h_2 X_2 \text{ con } h_1 \in R, h_2 \in R\}$$

Da tutto ciò segue che si ha:

$$\text{Sol}(S) = \{(h_1, 3 - h_1 - h_2, 2 - h_2, h_2) \mid h_1 \in R, h_2 \in R\}$$

Esempio 639 Vogliamo determinare le soluzioni del sistema di congruenze:

$$\begin{cases} 4x + y & \equiv & 98 & (\text{mod } 5) \\ 2x + y & \equiv & 2351 & (\text{mod } 5) \end{cases}$$

Trasformiamo il sistema di congruenze in un sistema di equazioni nel campo Z_5 :

$$\begin{cases} [4]_5[x]_5 + [y]_5 & = & [98]_5 & = & [3]_5 \\ [2]_5[x]_5 + [y]_5 & = & [2351]_5 & = & [1]_5 \end{cases}$$

La matrice dei coefficienti ha determinante uguale a $[2]_5$. Esiste quindi una ed una sola soluzione. Calcoliamola utilizzando l'algoritmo di Cramer. Si ha:

$$[x]_5 = [2]_5^{-1} \cdot \begin{vmatrix} [3]_5 & [1]_5 \\ [1]_5 & [1]_5 \end{vmatrix} = [3]_5 \cdot ([3]_5 \cdot [1]_5 - [1]_5 \cdot [1]_5) = [3]_5 \cdot [2]_5 = [1]_5$$

$$[y]_5 = [2]_5^{-1} \begin{vmatrix} [4]_5 & [3]_5 \\ [2]_5 & [1]_5 \end{vmatrix} = [3]_5 \cdot ([4]_5 \cdot [1]_5 - [3]_5 [2]_5) = [3]_5 \cdot [-2]_5 = [-6]_5 = [4]_5$$

Le soluzioni del nostro sistema di congruenze sono quindi:

$$\begin{cases} x = 1 + 5h \\ y = 4 + 5k \end{cases} \quad \forall h \in Z, \forall k \in Z$$

Esempio 640 Vogliamo determinare le soluzioni del sistema di congruenze:

$$\begin{cases} 13x - 51y & \equiv & 501 & (\text{mod } 5) \\ 2001x + 23y & \equiv & 77 & (\text{mod } 5) \end{cases}$$

Trasformiamo il sistema di congruenze in un sistema di equazioni nel campo Z_5 :

$$\begin{cases} [3]_5[x]_5 + [4]_5[y]_5 & = & [1]_5 \\ [1]_5[x]_5 + [3]_5[y]_5 & = & [2]_5 \end{cases}$$

La matrice dei coefficienti ha determinante uguale a $[0]_5$. È quindi necessario calcolare il rango della matrice A dei coefficienti e della matrice A' completa. Svolgendo i calcoli si nota che si ha:

$$\text{rk}(A) = \text{rk}(A') = 1$$

Il sistema ha quindi soluzioni.

Calcoliamo le soluzioni utilizzando l'algoritmo di Rouché-Capelli. Un minore invertibile della matrice A di ordine 1 è formato dalla prima riga e dalla prima colonna di A .

Consideriamo allora il sistema ridotto:

$$SR: [3]_5[x]_5 + [4]_5[y]_5 = [1]_5$$

Calcoliamo una soluzione particolare di SR . Poniamo $[y]_5 = [0]_5$ e otteniamo:

$$[3]_5[x]_5 = [1]_5$$

Da cui:

$$[x]_5 = [3]_5^{-1} = [2]_5$$

Una soluzione particolare è data quindi da:

$$([2]_5, [0]_5)$$

Consideriamo ora il sistema omogeneo associato:

$$SO: [3]_5[x]_5 + [4]_5[y]_5 = [0]_5$$

Cerchiamo $Sol(SO)$. Poniamo $[y]_5 = [1]_5$ e otteniamo:

$$[3]_5[x]_5 + [4]_5[1]_5 = [0]_5$$

cioè:

$$[3]_5[x]_5 = [-4]_5 = [1]_5$$

da cui segue:

$$[x]_5 = [3]_5^{-1} = [2]_5$$

Si ha perciò:

$$([2]_5, [1]_5) \in Sol(SO)$$

Si ha allora:

$$Sol(SO) = \{([h]_5[2]_5, [h]_5[1]_5) , \forall [h]_5 \in Z_5\}$$

Quindi le soluzioni di S sono date da:

$$Sol(S) = \{[2]_5 + [2]_5[h]_5, [0]_5 + [h]_5 , \forall [h]_5 \in Z_5\}$$

Le soluzioni di S in Z_5 dipendono da un parametro in Z_5 .

ATTENZIONE. Le soluzioni in Z_5 non sono infinite. Si possono infatti assegnare a $[h]_5$ solo 5 valori.

Tornando al sistema in Z , abbiamo:

$$Sol(S) = \{(2 + 2h + 5k, h + 5k') , \forall h = 0, 1, 2, 3, 4, \forall k \in Z, \forall k' \in Z\}$$

Esercizio 641 Determinare tutte le eventuali soluzioni dei seguenti sistemi di congruenze:

$$\begin{cases} 3x + y \equiv 1 \pmod{3} \\ x - 2y \equiv 7 \pmod{3} \end{cases}$$

$$\begin{cases} 3x + y \equiv 1 \pmod{7} \\ x - 2y \equiv 7 \pmod{7} \end{cases}$$

$$\begin{cases} x + y + z \equiv 1 \pmod{5} \\ 6x + 13y + 26z \equiv -4 \pmod{5} \\ -4x + 121y - 3z \equiv 2011 \pmod{5} \end{cases}$$

Esercizio 642 Determinare tutte le eventuali soluzioni dei seguenti sistemi di congruenze nei casi $n = 2, n = 3, n = 5, n = 7, n = 11$.

$$\begin{cases} x + y - z \equiv 2 \pmod{n} \\ x \equiv 12 \pmod{n} \\ x + y + 2z \equiv 13 \pmod{n} \end{cases}$$

$$\begin{cases} x + y + z \equiv 1 \pmod{n} \\ 2x - y - z \equiv 0 \pmod{n} \\ 3x + y - 4z \equiv 2011 \pmod{n} \end{cases}$$

Esempio 643 Vogliamo determinare le eventuali soluzioni del seguente sistema a coefficienti in R applicando l'algoritmo di Gauss:

$$\begin{cases} x + y + z = 1 \\ x + z = 1 \\ x + y = 2 \end{cases}$$

Vogliamo determinare la soluzione modificando il sistema in modo tale da ottenere una matrice dei coefficienti che sia a scalini.

Consideriamo la matrice dei coefficienti del sistema:

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

Facciamo in modo che il termine di posto (2,1) sia nullo. Sottraendo alla seconda equazione la prima equazione otteniamo il sistema equivalente:

$$\begin{cases} x + y + z = 1 \\ -y = 0 \\ x + y = 2 \end{cases}$$

La matrice dei coefficienti è diventata:

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

Per annullare il termine di posto (3,1), sottraiamo alla terza equazione la prima. Otteniamo il sistema:

$$\begin{cases} x + y + z = 1 \\ -y = 0 \\ -z = 1 \end{cases}$$

Siamo stati fortunati, oltre al termine di posto (3,1), si è annullato anche il termine di posto (3,2). La matrice dei coefficienti è:

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

E' una matrice a scalini. Dalla seconda e dalla terza equazione otteniamo $z = -1$, $y = 0$. Sostituendo nella prima equazione otteniamo $x = 2$. Il sistema ha quindi una sola soluzione:

$$(2, 0, -1)$$

Esempio 644 Vogliamo determinare le eventuali soluzioni del seguente sistema a coefficienti in R :

$$\begin{cases} x_1 + x_2 + x_3 + 2x_4 = 5 \\ 2x_1 + 2x_2 + 2x_3 + 3x_4 = 8 \\ 4x_1 + 4x_2 + 3x_3 + 7x_4 = 10 \\ -x_1 - x_2 - x_3 - 4x_4 = -9 \end{cases}$$

Vogliamo fare in modo che il termine di posto (2,1) della matrice dei coefficienti sia uguale a 0. Sottraiamo alla seconda equazione la prima moltiplicata per 2:

$$\begin{cases} x_1 + x_2 + x_3 + 2x_4 = 5 \\ -x_4 = -2 \\ 4x_1 + 4x_2 + 3x_3 + 7x_4 = 10 \\ -x_1 - x_2 - x_3 - 4x_4 = -9 \end{cases}$$

Per annullare il termine di posto (3,1) sottraiamo alla terza equazione la prima moltiplicata per 4:

$$\begin{cases} x_1 + x_2 + x_3 + 2x_4 = 5 \\ -x_4 = -2 \\ -x_3 - x_4 = -10 \\ -x_1 - x_2 - x_3 - 4x_4 = -9 \end{cases}$$

Per annullare il termine di posto (4,1) sommiamo alla quarta equazione la prima equazione:

$$\begin{cases} x_1 + x_2 + x_3 + 2x_4 = 5 \\ -x_4 = -2 \\ -x_3 - x_4 = -10 \\ -2x_4 = -4 \end{cases}$$

Ora scambiamo la seconda equazione con la terza:

$$\left\{ \begin{array}{rcl} x_1 + x_2 + x_3 + 2x_4 & = & 5 \\ -x_3 - x_4 & = & -10 \\ -x_4 & = & -2 \\ -2x_4 & = & -4 \end{array} \right.$$

Sottraiamo alla quarta equazione la terza moltiplicata per 2:

$$\left\{ \begin{array}{rcl} x_1 + x_2 + x_3 + 2x_4 & = & 5 \\ -x_3 - x_4 & = & -10 \\ -x_4 & = & -2 \\ 0 & = & 0 \end{array} \right.$$

L'ultima equazione è identicamente soddisfatta. Dalla terza ricaviamo $x_4 = 2$. Sostituendo nella seconda ricaviamo $x_3 = 8$. Sostituendo nella prima otteniamo $x_1 = -7 - x_2$.

Le soluzioni del sistema dipendono quindi da un parametro. Sono:

$$\{(-7 - h, h, 8, 2) \mid h \in R\}$$

Esempio 645 Risolviamo con il metodo di Gauss il sistema assegnato nell'esempio 639:

$$\left\{ \begin{array}{rcl} [4]_5[x]_5 + [y]_5 & = & [3]_5 \\ [2]_5[x]_5 + [y]_5 & = & [1]_5 \end{array} \right.$$

Trasformiamo la matrice dei coefficienti in una matrice a scalini. Sottraiamo alla seconda riga la prima riga moltiplicata per $[2]_5 \cdot [4]_5^{-1} = [2]_5 \cdot [4]_5 = [3]_5$. Otteniamo:

$$\left\{ \begin{array}{rcl} [4]_5[x]_5 + [y]_5 & = & [3]_5 \\ [3]_5[y]_5 & = & [2]_5 \end{array} \right.$$

Da cui:

$$\left\{ \begin{array}{rcl} [4]_5[x]_5 + [y]_5 & = & [3]_5 \\ [y]_5 & = & [3]_5^{-1}[2]_5 = [2]_5[2]_5 = [4]_5 \end{array} \right.$$

Sostituendo nella prima equazione otteniamo $[x]_5 = [1]_5$. Abbiamo quindi la soluzione:

$$([1]_5, [4]_5)$$

Esercizio 646 Determinare le soluzioni del seguente sistema di congruenze utilizzando l'algoritmo di Gauss:

$$\left\{ \begin{array}{rcl} [3]_5[x]_5 + [4]_5[y]_5 & = & [1]_5 \\ [x]_5 + [3]_5[y]_5 & = & [2]_5 \end{array} \right.$$

Abbiamo visto che l'algoritmo di Gauss per la risoluzione di un sistema consiste nel ridurre la matrice del sistema ad una matrice a scalini.

L'**algoritmo di Gauss-Jordan** è un raffinamento dell'algoritmo di Gauss.

Supponiamo che, per mezzo dell'algoritmo di Gauss, si arrivi ad una matrice a scalini del seguente tipo:

$$\left(\begin{array}{cccccc} \bullet & * & * & * & * & * \\ \hline 0 & \bullet & * & * & * & * \\ 0 & 0 & \bullet & * & * & * \\ 0 & 0 & 0 & 0 & \bullet & * \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

dove con \bullet si sono indicati numeri reali non nulli e con $*$ numeri reali qualsiasi.

Il procedimento di Gauss-Jordan consiste nell'arrivare ad una matrice del tipo:

$$\left(\begin{array}{cccccc} \bullet & 0 & 0 & * & 0 & * \\ \hline 0 & \bullet & 0 & * & 0 & * \\ 0 & 0 & \bullet & * & 0 & * \\ 0 & 0 & 0 & 0 & \bullet & * \\ \hline 0 & 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

Si vogliono matrici tali che, nelle colonne dove c'è \bullet , tutti gli altri elementi siano nulli.

Descriviamo l'algoritmo con un esempio.

Esempio 647 Supponiamo di essere arrivati per mezzo dell'algoritmo di Gauss al seguente sistema a coefficienti in R .

$$\left\{ \begin{array}{rcl} x + y + z & = & 1 \\ -y & = & 0 \\ -z & = & -1 \end{array} \right.$$

La matrice dei coefficienti è a scalini:

$$\left(\begin{array}{ccc} 1 & 1 & 1 \\ \hline 0 & -1 & 0 \\ 0 & 0 & -1 \end{array} \right)$$

Noi vogliamo ottenere una matrice del tipo

$$\left(\begin{array}{ccc} \bullet & 0 & 0 \\ \hline 0 & \bullet & 0 \\ 0 & 0 & \bullet \end{array} \right)$$

Per far ciò dobbiamo innanzitutto annullare il coefficiente della y nella prima equazione. Sommiamo allora alla prima equazione la seconda. Otteniamo:

$$\left\{ \begin{array}{rcl} x + z & = & 1 \\ -y & = & 0 \\ -z & = & -1 \end{array} \right.$$

Vogliamo ora annullare il coefficiente della z della prima equazione. Sommiamo allora alla prima equazione la terza. Otteniamo:

$$\begin{cases} x &= & 0 \\ -y &= & 0 \\ -z &= & -1 \end{cases}$$

La matrice dei coefficienti è ora del tipo voluto:

$$\left(\begin{array}{ccc|ccc} 1 & & 0 & & 0 & \\ 0 & & -1 & & 0 & \\ 0 & & 0 & & -1 & \end{array} \right)$$

Si calcola facilmente la soluzione del sistema.

Esempio 648 Vogliamo utilizzare l'algoritmo di Gauss-Jordan per determinare le soluzioni del seguente sistema a coefficienti in R :

$$\begin{cases} x_1 + x_2 + x_3 + x_4 &= & 1 \\ 2x_1 + x_2 + 3x_3 &= & 3 \\ 4x_1 + 2x_2 + 6x_3 + x_4 &= & 7 \end{cases}$$

Sommando alla seconda ed alla terza equazione la prima moltiplicata per opportuni fattori otteniamo:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 &= & 1 \\ -x_2 + x_3 - 2x_4 &= & 1 \\ -2x_2 + 2x_3 - 3x_4 &= & 3 \end{cases}$$

Vogliamo annullare i coefficienti della x_2 nella prima e nella terza equazione. Sommando alla prima e alla terza equazione la seconda equazione moltiplicata per opportuni fattori otteniamo:

$$\begin{cases} x_1 + 2x_3 - x_4 &= & 2 \\ -x_2 + x_3 - 2x_4 &= & 1 \\ x_4 &= & 1 \end{cases}$$

Notiamo che non vi è alcuna possibilità di annullare nella prima equazione il coefficiente di x_3 . Vogliamo ora annullare nelle prime due equazioni il coefficiente della x_4 . Sommando alle prime due equazioni la terza moltiplicata per opportuni fattori otteniamo:

$$\begin{cases} x_1 + 2x_3 &= & 3 \\ -x_2 + x_3 &= & 3 \\ x_4 &= & 1 \end{cases}$$

Da cui si ottengono le soluzioni dipendenti da un parametro:

$$\{(3 - 2h, -3 + h, h, 1) \mid h \in R\}$$

4.9 Operazioni elementari

Abbiamo descritto l'algoritmo di Gauss per la risoluzione di sistemi di equazioni lineari a coefficienti in un campo K . Siamo in grado, per mezzo di esso, di sostituire ad un qualsiasi sistema un altro sistema ad esso equivalente la cui matrice dei coefficienti sia a scalini.

Vediamo quali tipi di operazioni abbiamo utilizzato per far ciò.

Vi sono due tipi di operazioni. Il primo consiste nel sommare ad una equazione del sistema un'altra equazione del sistema moltiplicata per un elemento del campo K . Il secondo consiste nello scambiare tra loro due equazioni del sistema.

Vediamo a quali tipi di operazioni sulle matrici dei coefficienti essi corrispondano.

Primo tipo. Sommare alla riga r -sima di una matrice la riga s -sima, con $s \neq r$, moltiplicata per un elemento del campo K .

Secondo tipo. Scambiare tra loro due righe di una matrice.

Questi due tipi di operazioni si dicono **operazioni elementari di riga**.

Due matrici si dicono **equivalenti per riga** se è possibile passare da una all'altra per mezzo di operazioni elementari di riga.

Teorema 649 Data una matrice $A \in M(K, p, q)$, dove K è un campo, esiste una matrice A' a scalini equivalente per righe alla matrice A .

DIMOSTRAZIONE. Applicare l'algoritmo di Gauss. \square

Teorema 650 Sia I la matrice identica di ordine n e sia $I_h(r, s)$, con $r \neq s$, la matrice ottenuta da I sommando alla r -sima riga la s -sima riga moltiplicata per h .

Si ha:

$$\det(I_h(r, s)) = 1$$

Sia poi A una matrice a n righe e q colonne e sia A' la matrice ottenuta da A sommando alla r -sima riga di A la s -sima riga di A moltiplicata per h . Si ha:

$$A' = I_h(r, s) \cdot A$$

Se inoltre la matrice A è quadrata di ordine n , dal teorema di Binet segue allora:

$$\det(A) = \det(A')$$

DIMOSTRAZIONE.

Per definizione, la matrice $I_h(r, s)$ è data da:

$$I_h(r, s) = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \dots & 1 & \dots & h & \dots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \vdots & & \vdots & & \vdots & & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix}$$

Quindi:

$$I_h(r, s) = (\gamma_{ij}) \quad \text{con} \quad \gamma_{ij} = \begin{cases} 1 & \text{se } i = j \\ h & \text{se } i = r, j = s \\ 0 & \text{altrimenti} \end{cases}$$

Notiamo che, nella rappresentazione appena fatta della matrice $I_h(r, s)$, abbiamo implicitamente supposto $r < s$. In tal caso $I_h(r, s)$ è triangolare superiore. Se invece si ha $r > s$, essa è triangolare inferiore. Ad ogni modo in ambedue i casi si ha che il suo determinante è uguale al prodotto degli elementi della diagonale principale. Quindi

$$\det(I_h(r, s)) = 1$$

Dimostriamo ora che la matrice $A' = I_h(r, s) \cdot A$ è uguale alla matrice ottenuta da A sommando alla r -sima riga di A la s -sima riga moltiplicata per h . Si ha:

$$A' = \begin{pmatrix} 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & \dots & h & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \vdots & \ddots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \cdot \begin{pmatrix} a_{11} & \dots & a_{1j} & \dots & a_{1q} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{r1} & \dots & a_{rj} & \dots & a_{rq} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{s1} & \dots & a_{sj} & \dots & a_{sq} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nj} & \dots & a_{nq} \end{pmatrix}$$

Calcoliamo il generico elemento c_{ij} della matrice A' . Si ha:

$$c_{ij} = \gamma_{i1} \cdot a_{1j} + \dots + \gamma_{ii} \cdot a_{ij} + \dots + \gamma_{in} \cdot a_{nj}$$

Notando come sono gli elementi γ_{ik} , distinguiamo due casi: $i \neq r$ e $i = r$. Per $i \neq r$ abbiamo, per ogni j :

$$c_{ij} = \underbrace{\gamma_{i1}}_{=0} \cdot a_{1j} + \dots + \underbrace{\gamma_{ii}}_{=1} \cdot a_{ij} + \dots + \underbrace{\gamma_{in}}_{=0} \cdot a_{nj} = a_{ij}$$

Per $i = r$ abbiamo, per ogni j :

$$c_{rj} = \underbrace{\gamma_{r1}}_{=0} \cdot a_{1j} + \dots + \underbrace{\gamma_{rr}}_{=1} \cdot a_{rj} + \dots + \underbrace{\gamma_{rs}}_{=h} \cdot a_{sj} + \dots + \underbrace{\gamma_{rn}}_{=0} \cdot a_{nj} = a_{rj} + h a_{sj}$$

Scrivere (esercizio) l'elemento generico della matrice ottenuta da A sommando alla r -sima riga la s -sima riga moltiplicata per h . Ci si accorgerà che esso è uguale al generico elemento della matrice A' . Abbiamo dimostrato quel che volevamo.

Notiamo che nella dimostrazione appena fatta (e anche nella rappresentazione delle due matrici) abbiamo implicitamente supposto $r < s$. La dimostrazione nel caso $r > s$ sarebbe stata analoga. \square

Teorema 651 Data la matrice I identica di ordine n sia $r < s$ e sia $I(r, s)$ la matrice ottenuta da I scambiando la riga r -sima con la riga s -sima.

Si può dimostrare, noi non lo facciamo, che si ha:

$$\det(I(r, s)) = -1$$

Sia poi A una matrice a n righe e q colonne e sia A' la matrice ottenuta da A scambiando tra loro le righe r -sima e s -sima. Si ha:

$$A' = I(r, s) \cdot A$$

Se inoltre la matrice A è quadrata di ordine n , allora dal teorema di Binet segue:

$$\det(A) = -\det(A')$$

DIMOSTRAZIONE. Lasciata per esercizio. \square

Nota 652 In definitiva abbiamo visto che, se una matrice A' è ottenuta da una matrice A per mezzo di un'operazione elementare di riga, allora si ha

$$A' = K \cdot A$$

dove K è una matrice del tipo $I_h(r, s)$ oppure del tipo $I(r, s)$ a seconda se l'operazione elementare è del primo tipo (sommare ad una riga un'altra riga moltiplicata per un fattore) o del secondo tipo (scambiare due righe).

Siano ora date due matrici A e A' equivalenti per riga. Ciò implica che si può passare dalla matrice A alla matrice A' per mezzo di operazioni elementari di riga.

Da quel che abbiamo visto in precedenza segue:

$$A' = K_m \cdots K_2 \cdot K_1 \cdot A$$

dove le matrici K_1, K_2, \dots, K_m sono matrici del tipo $I_h(r, s)$ o del tipo $I(r, s)$. Ponendo $K = K_m \cdots K_2 \cdot K_1$, abbiamo:

$$A' = K \cdot A$$

e K ha determinante uguale a 1 o a -1.

Esempio 653 Consideriamo la matrice a coefficienti reali:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 5 \\ 2 & 6 & 8 \end{pmatrix}$$

Si verifica facilmente che si può trasformare la matrice A nella seguente matrice a scalini:

$$A' = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 2 \\ 0 & 0 & 5 \end{pmatrix}$$

per mezzo delle seguenti operazioni elementari di riga: prima operazione: si somma alla terza riga di A la prima riga moltiplicata per -2.

Seconda operazione: si scambiano tra loro la seconda e la terza riga.

Si ha allora:

$$A' = I(2, 3) \cdot I_{-2}(3, 1) \cdot A$$

Si ha inoltre:

$$\det(A') = \det(I(2, 3) \cdot I_{-2}(3, 1)) \cdot \det(A) = (-1) \cdot \det(A) = -\det(A)$$

Teorema 654 Siano A e A' due matrici quadrate equivalenti per riga. Ciò significa che si passa da A a A' per mezzo di un certo numero di operazioni elementari del primo tipo e di un certo numero m di operazioni elementari del secondo tipo (scambi di riga). Si ha allora:

$$\det(A') = (-1)^m \det(A)$$

DIMOSTRAZIONE. Esercizio. \square

Teorema 655 Se A e A' sono matrici (non necessariamente quadrate) equivalenti per riga, allora esse hanno ranghi uguali. In formule:

$$\text{rk}(A') = \text{rk}(A)$$

Dimostrazione omessa. \square

Nota 656 Ricapitolando, l'algoritmo di Gauss ci permette di trasformare una qualsiasi matrice A in una matrice A' ad essa equivalente per righe che sia a scalini. Quindi

$$\text{rk}(A') = \text{rk}(A)$$

Inoltre, se A è quadrata, si ha:

$$\det(A') = (-1)^m \det(A)$$

Notiamo che, se poniamo l'ulteriore ipotesi che A sia invertibile, la matrice a scalini A' ha tutti gli elementi della diagonale principale non nulli. Applicando l'algoritmo di Gauss-Jordan, possiamo trasformare la matrice A' in una matrice diagonale A'' ad essa equivalente per righe.

Esempio 657 Consideriamo la matrice a coefficienti reali:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 5 \\ 2 & 6 & 8 \end{pmatrix}$$

Abbiamo visto che, per mezzo dell'algoritmo di Gauss di riduzione a scalini, si ottiene:

$$A' = I(2, 3) \cdot I_{-2}(3, 1) \cdot A \quad \text{con} \quad A' = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 2 \\ 0 & 0 & 5 \end{pmatrix}$$

Utilizziamo ora l'algoritmo di Gauss-Jordan.

Prima operazione: sommiamo alla prima riga di A' la seconda riga moltiplicata per -1. Otteniamo:

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 2 \\ 0 & 0 & 5 \end{pmatrix}$$

Seconda operazione: sommiamo alla prima riga di A la terza riga moltiplicata per $-1/5$. Otteniamo:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 5 \end{pmatrix}$$

Terza operazione: sommiamo alla seconda riga la terza riga moltiplicata per $-2/5$. Otteniamo:

$$A'' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

Si ha quindi:

$$A'' = I_{-2/5}(2, 3) \cdot I_{-1/5}(1, 3) \cdot I_{-1}(1, 2) \cdot A'$$

Da cui segue, utilizzando la relazione tra A' e A :

$$A'' = I_{-2/5}(2, 3) \cdot I_{-1/5}(1, 3) \cdot I_{-1}(1, 2) \cdot I(2, 3) \cdot I_{-2}(3, 1) \cdot A$$

Notiamo che la matrice A'' è diagonale.

Tutto ciò può essere generalizzato.

Teorema 658 Ogni matrice invertibile A è equivalente per righe ad una matrice diagonale A'' . E quindi si ha:

$$A'' = K \cdot A$$

dove K è il prodotto di un certo numero di matrici del tipo $I_h(r, s)$ e del tipo $I(r, s)$.

DIMOSTRAZIONE. Applicare l'algoritmo di Gauss-Jordan. \square

Esercizio 659 Data la matrice a coefficienti in R :

$$A = \begin{pmatrix} 0 & 3 & 1 \\ 0 & 2 & 2 \\ 7 & 1 & 5 \end{pmatrix}$$

determinare, per mezzo dell'algoritmo di Gauss-Jordan, una matrice diagonale A'' ad essa equivalente per righe. Determinare poi una matrice K del tipo descritto sopra tale che si abbia $A'' = K \cdot A$.

Nota 660 Abbiamo visto che matrici equivalenti per riga hanno lo stesso rango.

Sappiamo poi che il metodo di Gauss permette di sostituire una qualsiasi matrice con una matrice a scalini ad essa equivalente.

Si ha poi la seguente proprietà :

il rango di una matrice a scalini è uguale al numero degli scalini (cioè il numero di righe non nulle) della matrice.

La verifica di ciò non è difficile: basta ricordare che il rango di una matrice è uguale al numero di righe linearmente indipendenti.

Tutto ciò ci suggerisce un algoritmo per il calcolo del rango di una matrice. **Algoritmo di Gauss per il calcolo del rango di una matrice.** Data una matrice A , ne calcoliamo il rango nel seguente modo:

1) Determiniamo, con l'algoritmo di Gauss, una matrice a scalini A' equivalente per righe ad A . Si ha:

$$\text{rk}(A) = \text{rk}(A')$$

2) Contiamo il numero di scalini di A' . Siano n . Si ha allora:

$$\text{rk}(A') = n$$

Da tutto ciò segue:

$$\text{rk}(A) = n$$

Nota 661 Abbiamo visto che, se A e A' sono matrici quadrate equivalenti per riga, allora:

$$\det(A') = (-1)^m \det(A)$$

dove m è il numero di scambi di riga effettuati per passare dalla matrice A alla matrice A' .

Moltiplicando ambo i membri per $(-1)^m$ otteniamo:

$$\det(A) = (-1)^m \det(A')$$

Sappiamo poi che il metodo di Gauss permette di sostituire una qualsiasi matrice quadrata con una matrice quadrata a scalini ad essa equivalente.

Sappiamo inoltre che una matrice quadrata a scalini è triangolare superiore e che il determinante di una matrice triangolare superiore è uguale al prodotto degli elementi della sua diagonale principale.

Tutto ciò ci suggerisce un algoritmo per il calcolo del determinante di una matrice quadrata.

Algoritmo di Gauss per il calcolo del determinante. Sia A una matrice quadrata di ordine n . Calcoliamo il suo determinante nel seguente modo:

1) Cerchiamo, con l'algoritmo di Gauss, una matrice a scalini A' equivalente per righe alla matrice A e contiamo il numero di scambi di riga effettuati. Sia esso m .

2) Calcoliamo il prodotto $a'_{11} \cdot a'_{22} \cdot \dots \cdot a'_{nn}$ degli elementi della diagonale principale di A' . Si ha:

$$\det(A) = (-1)^m \cdot a'_{11} \cdot a'_{22} \cdot \dots \cdot a'_{nn}$$

L'algoritmo di Gauss di riduzione ad una matrice a scalini ci ha permesso di trovare efficaci algoritmi per la determinazione del rango di una matrice qualsiasi e per la determinazione del determinante di una matrice quadrata.

Ora vediamo come l'algoritmo di Gauss-Jordan, applicato ad una matrice invertibile, ci permette di trovare un algoritmo per la determinazione della sua inversa.

Abbiamo visto con il teorema 658 come, data una matrice invertibile A , si può determinare una matrice diagonale A'' ad essa equivalente ed una matrice K che sia prodotto di matrici del tipo $I_h(r, s)$ e del tipo $I(r, s)$ e tale che si abbia:

$$A'' = K \cdot A$$

Abbiamo detto che la matrice A'' è diagonale. Se riuscissimo a trasformare la matrice A'' nella matrice identica I e se riuscissimo a trovare una matrice K' tale che:

$$I = K' \cdot A''$$

avremmo:

$$I = K' \cdot A'' = K' \cdot K \cdot A$$

Pertanto avremmo che la matrice $K' \cdot K$ sarebbe l'inversa della matrice A . In formule:

$$A^{-1} = K' \cdot K$$

Avremmo così trovato un metodo per calcolare l'inversa di una matrice.

Bene, si tratta quindi di trovare un metodo per trasformare una matrice diagonale invertibile nella matrice identica.

Teorema 662 Sia I la matrice identica di ordine n . Dato un numero reale h , sia $I_h(r)$ la matrice ottenuta da I moltiplicando per h la r -sima riga. Si ha quindi:

$$I_h(r) = \delta_{ij}^h = \begin{cases} 1 & \text{per } i = j, i \neq r \\ h & \text{per } i = j = r \\ 0 & \text{altrimenti} \end{cases}$$

Data una matrice A a n righe e q colonne, la matrice $I_h(r) \cdot A$ è uguale alla matrice ottenuta da A moltiplicando per h la r -sima riga.

DIMOSTRAZIONE. Esercizio. \square

Nota 663 Sia ora A'' una matrice invertibile diagonale di ordine n . Gli elementi a_{11}, \dots, a_{nn} della sua diagonale principale sono tutti non nulli. Moltiplichiamo la prima riga di A'' per $h_1 = a_{11}^{-1}$, la seconda riga per $h_2 = a_{22}^{-1}$ e così via fino alla n -sima riga che moltiplichiamo per $h_n = a_{nn}^{-1}$. Otteniamo la matrice I . Abbiamo perciò:

$$I = I_{h_n}(n) \cdot \dots \cdot I_{h_2}(2) \cdot I_{h_1}(1) \cdot A''$$

Tutto ciò ci permette di trasformare una qualsiasi matrice invertibile A nella matrice I . Ecco come:

Primo passo: trasformiamo con l'algoritmo di Gauss-Jordan la matrice A in una matrice diagonale A'' e determiniamo la matrice K , prodotto di matrici del tipo $I_h(r, s)$ e del tipo $I(r, s)$, tale che:

$$A'' = K \cdot A$$

Secondo passo: moltiplichiamo le righe della matrice A'' per opportuni coefficienti h_1, \dots, h_n in modo da ottenere la matrice I . Abbiamo pertanto:

$$I = I_{h_n}(n) \cdot \dots \cdot I_{h_2}(2) \cdot I_{h_1}(1) \cdot A''$$

da cui segue:

$$I = I_{h_n}(n) \cdot \dots \cdot I_{h_2}(2) \cdot I_{h_1}(1) \cdot K \cdot A$$

Esempio 664 Proviamo a trasformare la seguente matrice invertibile a coefficienti reali:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 5 \\ 2 & 6 & 8 \end{pmatrix}$$

nella matrice identica. Abbiamo visto in precedenza che si ha:

$$A'' = I_{-2/5}(2, 3) \cdot I_{-1/5}(1, 3) \cdot I_{-1}(1, 2) \cdot I(2, 3) \cdot I_{-2}(3, 1) \cdot A$$

con

$$A'' = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 5 \end{pmatrix}$$

Moltiplicando la seconda riga di A'' per $1/2$ e la terza riga per $1/5$, otteniamo la matrice I . Quindi:

$$I = I_{1/2}(2) \cdot I_{1/5}(3) \cdot A''$$

Segue:

$$I = I_{1/2}(2) \cdot I_{1/5}(3) \cdot I_{-2/5}(2, 3) \cdot I_{-1/5}(1, 3) \cdot I_{-1}(1, 2) \cdot I(2, 3) \cdot I_{-2}(3, 1) \cdot A$$

Pertanto la matrice:

$$K'' = I_{1/2}(2) \cdot I_{1/5}(3) \cdot I_{-2/5}(2, 3) \cdot I_{-1/5}(1, 3) \cdot I_{-1}(1, 2) \cdot I(2, 3) \cdot I_{-2}(3, 1)$$

è l'inversa della matrice A .

Nasce ora il problema di calcolare la matrice K'' . Certo, si potrebbero fare tutti i prodotti necessari. Richiederebbe troppo tempo. In effetti c'è un semplice metodo per calcolare questo prodotto. Notiamo che si ha:

$$K'' = K'' \cdot I = I_{1/2}(2) \cdot I_{1/5}(3) \cdot I_{-2/5}(2, 3) \cdot I_{-1/5}(1, 3) \cdot I_{-1}(1, 2) \cdot I(2, 3) \cdot I_{-2}(3, 1) \cdot I$$

Calcoliamo innanzitutto $I_{-2}(3, 1) \cdot I$. Abbiamo ovviamente $I_{-2}(3, 1)$. Chiamiamo questa matrice per semplicità B_1 . Notiamo che la matrice B_1 è stata ottenuta dalla matrice I sommando alla terza riga la prima moltiplicata per -2 . Calcoliamo ora $B_2 = I(2, 3) \cdot B_1$. Per quel che abbiamo visto in precedenza sappiamo che B_2 si ottiene da B_1 scambiando tra loro la seconda e la terza riga. Per la stessa ragione si ha che la matrice $B_3 = I_{-1}(1, 2) \cdot B_2$ è ottenuta dalla matrice B_2 sommando alla prima riga la seconda riga moltiplicata per -1 . E così via per B_4, B_5 e B_6 fino ad ottenere $K' = B_7$ da B_6 moltiplicando la seconda riga per $1/2$.

Quindi la matrice $K'' = A^{-1}$ si ottiene operando sulla matrice identica con le stesse operazioni utilizzate per passare dalla matrice A alla matrice identica.

Nota 665 Possiamo ovviamente utilizzare questo algoritmo su qualsiasi matrice invertibile. In sintesi abbiamo il seguente algoritmo.

Algoritmo per il calcolo della matrice inversa. Data una matrice invertibile A trasformiamo la matrice A nella matrice identica e, nello stesso tempo, operiamo con le stesse operazioni sulla matrice identica. La matrice identica viene così trasformata nell'inversa della matrice A .

Il prossimo esempio dovrebbe chiarire.

Esempio 666 Riconsideriamo la matrice A vista prima:

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 5 \\ 2 & 6 & 8 \end{pmatrix}$$

trasformiamola nella matrice identica. Contemporaneamente operiamo le stesse trasformazioni sulla matrice identica

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Per far ciò scriviamo le matrici A e I una accanto all'altra e separiamole con una linea verticale:

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

Ora trasformiamo la matrice a sinistra nella matrice I . Scriviamo solamente i

passaggi:

$$\begin{aligned}
 & \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 0 & 5 & 0 & 1 & 0 \\ 0 & 2 & 2 & -2 & 0 & 1 \end{array} \right) \\
 & \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 2 & 2 & -2 & 0 & 1 \\ 0 & 0 & 5 & 0 & 1 & 0 \end{array} \right) \\
 & \left(\begin{array}{ccc|ccc} 1 & 0 & 1 & 3 & 0 & -1 \\ 0 & 2 & 2 & -2 & 0 & 1 \\ 0 & 0 & 5 & 0 & 1 & 0 \end{array} \right) \\
 & \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & -1/5 & -1 \\ 0 & 2 & 2 & -2 & 0 & 1 \\ 0 & 0 & 5 & 0 & 1 & 0 \end{array} \right) \\
 & \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & -1/5 & -1 \\ 0 & 2 & 0 & -2 & -2/5 & 1 \\ 0 & 0 & 5 & 0 & 1 & 0 \end{array} \right) \\
 & \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & -1/5 & -1 \\ 0 & 2 & 0 & -2 & -2/5 & 1 \\ 0 & 0 & 1 & 0 & 1/5 & 0 \end{array} \right) \\
 & \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 3 & -1/5 & -1 \\ 0 & 1 & 0 & -1 & -1/5 & 1/2 \\ 0 & 0 & 1 & 0 & 1/5 & 0 \end{array} \right)
 \end{aligned}$$

A sinistra abbiamo ottenuto la matrice I . A destra abbiamo ottenuto l'inversa della matrice A . Cioè:

$$A^{-1} = \begin{pmatrix} 3 & -1/5 & -1 \\ -1 & -1/5 & 1/2 \\ 0 & 1/5 & 0 \end{pmatrix}$$

Esempio 667 Consideriamo la seguente matrice $A \in M(Z_7, 2, 2)$.

$$A = \begin{pmatrix} [1]_7 & [0]_7 \\ [1]_7 & [1]_7 \end{pmatrix}$$

Abbiamo $\det(A) = [1]_7$. Quindi A è invertibile. Calcoliamone l'inversa con il metodo appena descritto.

$$\left(\begin{array}{cc|cc} [1]_7 & [0]_7 & [1]_7 & [0]_7 \\ [1]_7 & [1]_7 & [0]_7 & [1]_7 \end{array} \right)$$

Trasformiamo la matrice a sinistra nella matrice identica.

$$\left(\begin{array}{cc|cc} [1]_7 & [0]_7 & [1]_7 & [0]_7 \\ [0]_7 & [1]_7 & [6]_7 & [1]_7 \end{array} \right)$$

Quindi:

$$A^{-1} = \begin{pmatrix} [1]_7 & [0]_7 \\ [6]_7 & [1]_7 \end{pmatrix}$$

4.10 Bibliografia

1) **I.Cattaneo Gasparini** *Strutture algebriche, operatori lineari*, Veschi.

Gli ultimi tre paragrafi del secondo capitolo sono dedicati agli anelli e ai campi.

2) **I.Cattaneo Gasparini, G.Selmi** *Esercizi di algebra lineare con applicazioni alle funzioni di matrici e ai sistemi differenziali*, Veschi.

Il nono paragrafo del primo capitolo contiene esercizi sugli anelli.

3) **P.Maroscia** *Problemi di geometria*, Masson editoriale Veschi.

Nel terzo capitolo vengono assegnati e svolti molti esercizi sugli anelli e sui campi.

4) **L.Childs** *algebra, un'introduzione concreta*, ETS.

L'ottavo capitolo è dedicato agli anelli e ai campi.

5) **R.Procesi Ciampi, R.Rota** *Algebra moderna. Esercizi*, Veschi.

Il quinto capitolo contiene esercizi sugli anelli.

6) **L.Lombardo Radice** *Algebra* Editori Riuniti.

Il quinto ed il sesto capitolo sono dedicati allo studio degli anelli.

7) **I.N.Herstein** *Algebra*, Editori Riuniti.

Nel terzo capitolo vengono studiati gli anelli.

