Eserciziario – Gruppi e loro proprietà

TESTO DEGLI ESERCIZI

Esercizio A1

Verificare se è un gruppo $(\{1,-1, i, -i\}, \times)$

Esercizio A2

Verificare se è un gruppo l'insieme dei polinomi di grado non superiore a 2, nella indeterminata x, a coefficienti in $\mathbb{Z}$ rispetto alla somma (usualmente indicato con $(\mathbb{Z}^2[x],+)$).

Esercizio A3

Verificare se è un gruppo $(\{4n\ (n\in\mathbb{Z})\},\times)$

Esercizio A4

Verificare se è un gruppo $(\mathbb{Z}_7, \times)$

Esercizio A5

Verificare se è un gruppo $(\mathbb{Z}_5,+)$

Esercizio A6

Verificare se è un sottogruppo di $(\mathbb{Q}_0, \times)$ il sottoinsieme dei numeri decimali non periodici.

Esercizio A7

Verificare se è un sottogruppo di $(\mathbb{Z},+)$ il sottoinsieme dei numeri primi.

Esercizio A8

Verificare se è un sottogruppo di $(\mathbb{Z}^2[x],+)$ il sottoinsieme dei polinomi che hanno una radice uguale a 1.

Esercizio A9

Verificare se è un sottogruppo di $(\mathbb{Q},+)$ il sottoinsieme delle frazioni con denominatore 10.

Esercizio A10

Verificare se è un sottogruppo di $(\mathbb{Q}_0,\times)$ il sottoinsieme delle frazioni che sono potenze di $\frac{1}{2}$, ad esponente in $\mathbb{Z}$.

SOLUZIONE DEGLI ESERCIZI

Esercizio 1

Essendo gli elementi solo 4, possiamo costruire la tabella moltiplicativa per vedere se l'operazione è interna, se ammette neutro e se ammette inverso per ogni elemento; essendo gli elementi numeri complessi ed essendo il prodotto di numeri complessi associativo (e commutativo) tali proprietà non sono da verificare in quanto note. Se risulta gruppo, è un gruppo commutativo:

$\times$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

Dalla tabella si vede che:

- l'operazione è interna (gli elementi della tabella sono sempre i quattro elementi);
- esiste neutro (1);
- esiste inverso per ogni elemento: $1^{-1}=1$; $(-1)^{-1}=-1$; $i^{-1}=-i$; $(-i)^{-1}=i$.

Esercizio 2

- La somma di due polinomi di grado non superiore a 2, a coefficienti in $\mathbb{Z}$, è ancora di grado non superiore a 2 e i suoi coefficienti sono interi.
- La somma di polinomi qualsiasi è associativa.
- Il polinomio con tutti i coefficienti 0 ha grado 0, e quindi non superiore a 2 e sommato a un polinomio dà il polinomio stesso.
- L'inverso rispetto alla somma (opposto) è il polinomio con i coefficienti opposti di quelli del polinomio di partenza, quindi ancora del tipo detto.
- La somma è commutativa.

Esercizio 3

- L'operazione è interna: $4n \times 4m = 4p$ ove $p = 4mn$.
- Il prodotto è associativo: $(4n\times4m)\times4r = 16nm\times4r = 64nmr$ e $4n\times(4m\times4r) = 4n\times16mr = 64nmr$.
- Il prodotto è commutativo (anche se questa proprietà non è necessaria per la definizione di gruppo)
- Cerchiamo il neutro rispetto al prodotto: chiamiamolo $4x$ e deve essere $4x\times4m=4m$ per ogni m. Ma $4x\times4m = 16m$ e $16m=4m$ solo se $m=0$, mentre è richiesto che il neutro valga per ogni m, quindi non esiste neutro.

Di conseguenza non ha senso cercare l'inverso, e l'insieme non è gruppo.

Esercizio 4

L'insieme dato non può essere gruppo perché contiene l'elemento 0, che è un elemento assorbente rispetto al prodotto. Lo 0 non ha inverso, quindi non si può trattare di un gruppo. È un gruppo, invece l'insieme $(Z_7 - \{0\}, \times)$ e la sua tabella moltiplicativa è la seguente:

×	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

In tale tabella si vede che la legge di composizione è interna, ammette neutro che è 1 e ammette inverso per ogni elemento, che si determina cercando l'elemento 1 su ogni riga e colonna. L'associatività vale perché vale per gli elementi di Z, di cui gli elementi dati sono classi di equivalenza.

Esercizio 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

La tabella della operazione scritta mostra che la legge di composizione è interna, ammette neutro (che è 0) e ammette inverso per ogni elemento, che si determina cercando l'elemento 0 su ogni riga e colonna.

L'associatività vale perché vale per gli elementi di Z, di cui gli elementi dati sono classi di equivalenza.

Esercizio 6

La condizione assegnata significa che ogni frazione dell'insieme, ridotta ai minimi termini, deve avere un denominatore che ha come soli fattori primi 2 e 5.

La condizione necessaria è soddisfatta, dato che il neutro del gruppo, che è 1, si può pensare come $\frac{1}{2^0 \times 5^0}$ (e che comunque 1, essendo intero, ha una rappresentazione decimale non periodica).

Bisogna quindi usare il criterio: poiché l'insieme è infinito, bisogna mostrare che per ogni coppia di elementi a e b che appartengono all'insieme, $a \times b^{-1}$ è ancora un elemento dell'insieme.

La condizione però è falsa; se ad esempio $b = \frac{3}{10}$, $b^{-1} = \frac{10}{3}$ e il prodotto $a \times b^{-1}$ ha in generale a denominatore un fattore primo 3, quindi non è del tipo richiesto.

Esercizio 7

Già la condizione necessaria non è soddisfatta dato che 0 non è primo, comunque la proprietà è sicuramente falsa; ad esempio 3+5=8 e 8 non è primo.
Un polinomio di $\mathbb{Z}^2[x]$ con la condizione indicata si può scrivere come $(x-1)(ax+b)$.

Esercizio 8

Un polinomio di $\mathbb{Z}^2[x]$ con la condizione indicata si può scrivere come $(x-1)(ax+b)$.
La condizione necessaria è soddisfatta, basta porre $a=b=0$.
Per il criterio, siano $p(x)= (x-1)(ax+b)$ e $q(x)= (x-1)(cx+d)$.
Allora $p(x) + q(x)^{-1}= p(x) - q(x) = (x-1)[(a-c)x+(b-d)]$ che è un polinomio con una radice 1.

Esercizio 9

La condizione necessaria è soddisfatta, visto che $0 = \frac{0}{10}$.
Per il criterio, sia $a = \frac{m}{10}$ e $b=\frac{n}{10}$. Allora $a+(-b)=\frac{m-n}{10}$, che è ancora del tipo voluto.

Esercizio 10

La condizione necessaria è soddisfatta, visto che $1 = \frac{1}{2^0}$.
Per il criterio, siano $a = \frac{1}{2^m}$ e $b = \frac{1}{2^n}$. Allora risulta $a \times b^{-1} = \frac{2^n}{2^m} = \frac{1}{2^{m-n}}$ che è ancora una potenza di $\frac{1}{2}$, purché, come è infatti richiesto, gli esponenti possano anche essere negativi.
Da osservare che tale sottogruppo coincide con quello delle potenze di 2.
Se invece gli esponenti fossero in $\mathbb{N}$, non è sottogruppo né il sottoinsieme delle potenze di 2 né quello delle potenze di $\frac{1}{2}$.

Eserciziario – Gruppo simmetrico su *n* oggetti

TIPOLOGIA A - TESTO DEGLI ESERCIZI

Esercizio A1

Calcolare il prodotto delle seguenti permutazioni di S_8:

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\2&6&4&3&1&8&5&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&1&6&8&5&7\end{pmatrix}$$

Esercizio A2

Calcolare il prodotto delle seguenti permutazioni di S_8:

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\5&6&4&8&1&3&2&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\7&3&4&6&1&8&5&2\end{pmatrix}$$

Esercizio A3

Calcolare il prodotto delle seguenti permutazioni di S_7:

$$\begin{pmatrix}1&2&3&4&5&6&7\\4&7&6&1&3&2&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\2&7&5&3&4&1&6\end{pmatrix}$$

Esercizio A4

Calcolare il prodotto delle seguenti permutazioni di S_6:

$$\begin{pmatrix}1&2&3&4&5&6\\3&6&4&1&2&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\2&4&6&1&3&5\end{pmatrix}$$

TIPOLOGIA B - TESTO DEGLI ESERCIZI

Esercizio B1

Trasformare in prodotto di cicli disgiunti la seguente permutazione:

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\2&6&4&7&3&8&5&1\end{pmatrix}$$

Esercizio B2

Trasformare in prodotto di cicli disgiunti la seguente permutazione:

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\2&6&4&3&1&8&5&7\end{pmatrix}$$

Esercizio B3

Trasformare in prodotto di cicli disgiunti la seguente permutazione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 6 & 1 & 2 & 3 & 5 \end{pmatrix}$$

Esercizio B4

Trasformare in prodotto di cicli disgiunti la seguente permutazione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 5 & 3 & 4 & 1 & 6 \end{pmatrix}$$

Esercizio B5

Trasformare in prodotto di cicli disgiunti la seguente permutazione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 9 & 5 & 1 & 8 & 6 & 7 & 3 \end{pmatrix}$$

Esercizio B6

Trasformare in prodotto di cicli disgiunti la seguente permutazione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 4 & 5 & 3 & 7 & 6 & 2 & 1 \end{pmatrix}$$

TIPOLOGIA C - TESTO DEGLI ESERCIZI

Esercizio C1

Trasformare in prodotto di cicli disgiunti la seguente permutazione, scritta come prodotto di cicli non disgiunti:

(2 4 3 1)(1 6 4 2 7)(3 5 4)(1 2 6 7 4)

Esercizio C2

Trasformare in prodotto di cicli disgiunti la seguente permutazione, scritta come prodotti di cicli non disgiunti:

(1 7 2 5 4)(3 6 4 2)(4 7 3 5)(7 5)

Esercizio C3

Trasformare in prodotto di cicli disgiunti la seguente permutazione, scritta come prodotti di cicli non disgiunti:

(2 5 3 7)(8 4 3 6)(1 2 6 4 5)

Esercizio C4

Trasformare in prodotto di cicli disgiunti la seguente permutazione, scritta come prodotti di cicli non disgiunti:

$$(2\ 5\ 4\ 7)(8\ 5\ 3\ 6)(1\ 2\ 3\ 6\ 4\ 5)$$

Esercizio C5

Trasformare in prodotto di cicli disgiunti la seguente permutazione, scritta come prodotti di cicli non disgiunti:

$$(1\ 5\ 3\ 7\ 9)(8\ 9\ 3\ 2\ 6)(1\ 3\ 6\ 4\ 5\ 9)$$

Esercizio C6

Trasformare in prodotto di cicli disgiunti la seguente permutazione, scritta come prodotti di cicli non disgiunti:

$$(1\ 3\ 6\ 2)(4\ 6\ 2\ 5)(3\ 6\ 5\ 2)(1\ 5)$$

Esercizio C7

Trasformare in prodotto di cicli disgiunti la seguente permutazione, scritta come prodotti di cicli non disgiunti:

$$(1\ 2\ 6\ 8)(4\ 6\ 2\ 5)(3\ 6\ 5\ 2)(1\ 5\ 8\ 3\ 4)$$

TIPOLOGIA D - TESTO DEGLI ESERCIZI

Esercizio D1

Calcolare tutte le potenze distinte del ciclo seguente:

$$c = (1\ 4\ 3\ 2)$$

Esercizio D2

Calcolare tutte le potenze distinte del ciclo seguente:

$$c = (1\ 7\ 4\ 5\ 3\ 6\ 2)$$

TIPOLOGIA E - TESTO DEGLI ESERCIZI

Esercizio E1

Calcolare tutte le potenze distinte della permutazione seguente:

$$p = (1\ 7\ 5\ 6)\ (2\ 3\ 4)$$

Esercizio E2

Calcolare tutte le potenze distinte della permutazione seguente:

$$p = (1\ 5)\ (3\ 8\ 6\ 4\ 2)$$

Esercizio E3

Calcolare tutte le potenze distinte della permutazione seguente:

$$p = (1\ 4\ 8\ 6\ 2\ 9)(0\ 3\ 7\ 5)$$

TIPOLOGIA A – SOLUZIONE DEGLI ESERCIZI

Esercizio A1

Bisogna ricordare che si usa la scrittura funzionale, quindi si esegue prima la permutazione scritta a destra. Seguendo i vari elementi si ha:

$1 \to 2 \to 6$
$2 \to 3 \to 4$
$3 \to 4 \to 3$
$4 \to 1 \to 2$
$5 \to 6 \to 8$
$6 \to 8 \to 7$
$7 \to 5 \to 1$
$8 \to 7 \to 5$

Quindi in conclusione:

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\2&6&4&3&1&8&5&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\2&3&4&1&6&8&5&7\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7&8\\6&4&3&2&8&7&1&5\end{pmatrix}$$

Esercizio A2

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\5&6&4&8&1&3&2&7\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7&8\\7&3&4&6&1&8&5&2\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7&8\\2&4&8&3&5&7&1&6\end{pmatrix}$$

Esercizio A3

$$\begin{pmatrix}1&2&3&4&5&6&7\\4&7&6&1&3&2&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6&7\\2&7&5&3&4&1&6\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7\\7&5&3&6&1&4&2\end{pmatrix}$$

Esercizio A4

$$\begin{pmatrix}1&2&3&4&5&6\\3&6&4&1&2&5\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\2&4&6&1&3&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\6&1&5&3&4&2\end{pmatrix}$$

TIPOLOGIA B – SOLUZIONE DEGLI ESERCIZI

Esercizio B1

Si parte da 1 e si segue il percorso dei vari elementi:

$1 \rightarrow 2 \rightarrow 6 \rightarrow 8 \rightarrow 1$

Poiché si è tornati a 1, il ciclo si chiude, quindi il primo ciclo è (1 2 6 8).
Ora si cerca il primo elemento non ancora usato: 3.

$3 \rightarrow 4 \rightarrow 7 \rightarrow 5 \rightarrow 3$ e si è tornati al primo elemento.

Allora in conclusione:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 4 & 7 & 3 & 8 & 5 & 1 \end{pmatrix} = (1\ 2\ 6\ 8)(3\ 4\ 7\ 5).$$

Osservazione: è indifferente quale sia il primo elemento da cui si parte, cioè ad esempio (3 4 7 5)=(4 7 5 3)=(5 3 4 7) ecc; basta che l'ordine, ciclicamente, sia lo stesso, cioè quando si arriva in fondo al ciclo si ricomincia dal primo, come se i numeri fossero scritti su una circonferenza.

Esercizio B2

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 6 & 4 & 3 & 1 & 8 & 5 & 7 \end{pmatrix} = (1\ 2\ 6\ 8\ 7\ 5)(3\ 4).$$

Esercizio B3

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 6 & 1 & 2 & 3 & 5 \end{pmatrix} = (1\ 4)(2\ 7\ 5)(3\ 6)$$

Esercizio B4

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 5 & 3 & 4 & 1 & 6 \end{pmatrix} = (1\ 2\ 7\ 6)(3\ 5\ 4)$$

Esercizio B5

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 9 & 5 & 1 & 8 & 6 & 7 & 3 \end{pmatrix} = (1\ 2\ 4\ 5)(3\ 9)(6\ 8\ 7)$$

Esercizio B6

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 4 & 5 & 3 & 7 & 6 & 2 & 1 \end{pmatrix} = (1\ 8\ 2\ 9)(3\ 4\ 5)(6\ 7)$$

TIPOLOGIA C – SOLUZIONE DEGLI ESERCIZI

Esercizio C1

Si parte dal primo elemento, 1, ricordando che si usa la scrittura funzionale, quindi si esegue prima il ciclo scritto più a destra. Se in un ciclo un elemento non compare, vuol dire che sta fermo.

$1 \to 2 \to 2 \to 7 \to 7$
$7 \to 4 \to 3 \to 3 \to 1$ il ciclo si è chiuso.

Ricominciamo dal primo elemento non usato:

$2 \to 6 \to 6 \to 4 \to 3$
$3 \to 5 \to 5 \to 5 \to 5$
$5 \to 5 \to 4 \to 2 \to 4$
$4 \to 1 \to 1 \to 6 \to 6$
$6 \to 7 \to 7 \to 1 \to 2$ il ciclo si è chiuso.

Quindi in definitiva (2 4 3 1)(1 6 4 2 7)(3 5 4)(1 2 6 7 4) =(1 7)(2 3 5 4 6)

Esercizio C2

(1 7 2 5 4)(2 3 6 4)(4 7 3 5)(7 5) = (1 7 5 6) (2 3 4)

Esercizio C3

(2 5 3 7)(8 4 3 6)(1 2 6 4 5)= (2 8 4 3 6 7) (1 5)

Esercizio C4

(2 5 4 7)(8 5 3 6)(1 2 3 6 4 5)= (2 6 7) (1 5) (8 4 3)

Esercizio C5

(1 5 3 7 9)(8 9 3 2 6)(1 3 6 4 5 9)= (1 2 6 4 3 8) (7 9 5)

Esercizio C6

(1 3 6 2)(4 6 2 5)(3 6 5 2)(1 5)= (1 5 3) (4 2 6)

Esercizio C7

(1 2 6 8)(4 6 2 5)(3 6 5 2)(1 5 8 3 4)= (1 5) (3 8 6 4 2)

TIPOLOGIA D – SOLUZIONE DEGLI ESERCIZI

Esercizio D1

$c = (1\ 4\ 3\ 2)$
$c^2 = (1\ 4\ 3\ 2)\ (1\ 4\ 3\ 2) = (1\ \ 3)(2\ \ 4)$
$c^3 = (1\ \ 3)(2\ \ 4)\ (1\ 4\ 3\ 2) = (1\ 2\ \ 3\ \ 4)$
$c^4 = (1\ 4\ 3\ 2)\ (1\ 2\ \ 3\ \ 4) = \mathrm{id}$

Osservazioni:

- Il periodo del ciclo (cioè il più piccolo esponente a cui deve venir elevato per avere il neutro) è uguale al numero degli elementi che lo compongono.
- Poiché $c \times c^3 = c^4 = \mathrm{id}$, c^3 è l'inverso di c (e viceversa) e c^3 si ottiene da c iniziando dal primo elemento e poi percorrendo il ciclo in senso inverso.
- Se gli elementi non fossero solo quattro, lo stesso discorso varrebbe per tutti gli elementi: se fossero 7, p^6 sarebbe l'inverso di p, p^5 sarebbe l'inverso di p^2 e p^4 sarebbe l'inverso di p^3; questa osservazione semplifica molto i conti, consentendo di calcolarne effettivamente solo la metà.

Esercizio D2

$c = (1\ \ 7\ 4\ \ 5\ \ 3\ \ 6\ \ 2)$
$c^2 = (1\ \ 4\ \ 3\ \ 2\ \ 7\ \ 5\ \ 6)$
$c^3 = (1\ \ 5\ \ 2\ \ 4\ \ 6\ \ 7\ \ 3)$
$c^4 = (1\ \ 3\ \ 7\ \ 6\ \ 4\ \ 2\ \ 5)$
$c^5 = (1\ \ 6\ \ 5\ \ 7\ \ 2\ \ 3\ \ 4)$
$c^6 = (1\ \ 2\ \ 6\ \ 3\ \ 5\ \ 4\ \ 7)$
$c^7 = \mathrm{id}$

TIPOLOGIA E – SOLUZIONE DEGLI ESERCIZI

Esercizio E1

La permutazione è composta da due cicli disgiunti, che quindi commutano:

$$(1\ 7\ 5\ 6)(2\ 3\ 4)=(2\ 3\ 4)(1\ 7\ 5\ 6).$$

Allora, posto $x = (2\ 3\ 4)$ e $y = (1\ 7\ 5\ 6)$,L risulta $p^2=(xy)^2=x^2y^2$.

Quindi:

$p = (1\ 7\ 5\ 6)(2\ 3\ 4)$	$p^2 = (1\ 5)(7\ 6)(2\ 4\ 3)$	$p^3 = (1\ 6\ 5\ 7)$	$p^4 = (2\ 3\ 4)$
$p^5 = (1\ 7\ 5\ 6)(2\ 4\ 3)$	$p^6 = (1\ 5)(7\ 6)$	$p^7 = (1\ 6\ 5\ 7)(2\ 3\ 4)$	$p^8 = (2\ 4\ 3)$
$p^9 = (1\ 7\ 5\ 6)$	$p^{10} = (1\ 5)(7\ 6)(2\ 3\ 4)$	$p^{11} = (1\ 6\ 5\ 7)(2\ 4\ 3)$	$p^{12} = \mathrm{id}$

Osservazioni:

- Il periodo del prodotto di due cicli disgiunti è il mcm dei due periodi; in questo caso, siccome sono primi tra loro, è il loro prodotto.
- incolonnando opportunamente le potenze, si vede bene che le potenze dei due fattori si ripetono, anche se con un "ritmo" diverso tra di loro.

Esercizio E2

Il periodo di p è 10=mcm(2,5)

$p = (1\ 5)\ (3\ 8\ 6\ 4\ 2)$	$p^2 = (3\ 6\ 2\ 8\ 4)$	$p^3 = (1\ 5)(3\ 4\ 8\ 2\ 6)$	$p^4 = (3\ 2\ 4\ 6\ 8)$	$p^5=(1\ 5)$
$p^6 = (3\ 8\ 6\ 4\ 2)$	$p^7 = (1\ 5)(3\ 6\ 2\ 8\ 4)$	$p^8 = (3\ 4\ 8\ 2\ 6)$	$p^9=(1\ 5)(3\ 2\ 4\ 6\ 8)$	$p^{10}=\mathrm{id}$

Esercizio E3

Il periodo di p è il mcm(6,4)=12.

$p = (1\ 4\ 8\ 6\ 2\ 9)(0\ 3\ 7\ 5)$	$p^2 = (1\ 8\ 2)(4\ 6\ 9)(0\ 7)(3\ 5)$	$p^3 = (1\ 6)(4\ 2)(8\ 9)(0\ 5\ 7\ 3)$
$p^4 = (1\ 2\ 8)(4\ 9\ 6)$	$p^5=(1\ 9\ 2\ 6\ 8\ 4)(0\ 3\ 7\ 5)$	$p^6 = (0\ 7)(3\ 5)$
$p^7 = (1\ 4\ 8\ 6\ 2\ 9)(0\ 5\ 7\ 3)$	$p^8 = (1\ 8\ 2)(4\ 6\ 9)$	$p^9=(1\ 6)(4\ 2)(8\ 9)\ (0\ 3\ 7\ 5)$
$p^{10}=(1\ 2\ 8)(4\ 9\ 6)\ (0\ 7)(3\ 5)$	$p^{11}=(1\ 9\ 2\ 6\ 8\ 4)\ (0\ 5\ 7\ 3)$	$p^{12}=\mathrm{id}$

Eserciziario – Gruppi ciclici

TESTO DEGLI ESERCIZI

Esercizio 1

Stabilire se il gruppo $(\mathbb{Z}^*_7,\times)$ è ciclico, determinandone un generatore.

Esercizio 2

Stabilire se il gruppo $(\mathbb{Z}^*_9,\times)$ è ciclico, determinandone un generatore.

Esercizio 3

Stabilire se il gruppo $(\mathbb{Z}_7,+)$ è ciclico, determinandone un generatore.

Esercizio 4

Stabilire se il gruppo $(\mathbb{Z}^*_{10},\times)$ è ciclico, determinandone un generatore.

Esercizio 5

Determinare tutti i possibili generatori del gruppo ciclico $(\mathbb{Z}_9,+)$.

Esercizio 6

Determinare tutti i possibili generatori del gruppo ciclico $(\mathbb{Z}^*_7,\times)$.

Esercizio 7

Determinare tutti i possibili generatori del gruppo ciclico $(\mathbb{Z}^*_{11},\times)$.

Esercizio 8

Dato un gruppo $(G, \circ)$ ciclico di ordine 12, di cui un generatore sia g, stabilire quale elemento di G genera:

- il sottogruppo di ordine 2;
- il sottogruppo di ordine 3,
- il sottogruppo di ordine 4;
- il sottogruppo di ordine 6.

Determinare quali sono invece i generatori.

Esercizio 9

Dato un gruppo $(G, \circ)$ ciclico di ordine 15, di cui un generatore sia g, stabilire quale elemento di G genera:

- il sottogruppo di ordine 3
- il sottogruppo di ordine 5

Determinare quali sono invece i generatori.

Esercizio 10

Mostrare che in un qualsiasi gruppo $(\mathbb{Z}^*_n,\times)$:

- l'elemento $n-1$ appartiene al gruppo;
- l'elemento $n-1$ ha sempre periodo 2.

SOLUZIONE DEGLI ESERCIZI

Esercizio 1

Generatore per un gruppo ciclico è ogni elemento che abbia come periodo l'ordine del gruppo.

Poiché $\mathbb{Z}^*_7=\{1, 2, 3, 4, 5, 6\}$ e quindi ha ordine 6, bisogna trovare un elemento di periodo 6.

Cerchiamo i periodi degli elementi:

- 1, il neutro, ha sempre periodo 1.
- 2 ; $2^2=4$; $2^3=8\equiv 1$ 2 ha periodo 3
- 3 ; $3^2=9\equiv 2$; $3^3=3^2\times 3\equiv 2\times 3=6$; $3^4=3^2\times 3^2\equiv 2\times 2=4$; $3^5=3\times 3^4\equiv 3\times 4=12\equiv 5$; $3^6=3\times 3^5\equiv 3\times 5=15\equiv 1$, quindi 3 è un generatore.

Osservazione: una volta scoperto che 32 e 33 non sono congrui a 1, il calcolo successivo è inutile: infatti ogni elemento di un gruppo genera un sottogruppo ciclico del gruppo stesso e i sottogruppi propri di un gruppo di ordine 6, per il teorema di Lagrange, possono avere ordine solo 2 o 3; se il sottogruppo generato da 3 ha un ordine maggiore di 3, è sicuramente tutto il gruppo, e quindi 3 è generatore.

Esercizio 2

Risulta $\mathbb{Z}^*_9=\{1, 2, 4, 5, 7, 8\}$ (gli elementi più piccoli di 9 e primi con 9); quindi $\mathbb{Z}^*_9$ ha ordine 6, per cui un generatore deve essere un elemento di periodo 6.

1 genera solo se stesso.

2 ; $2^2=4$; $2^3=8$; possiamo già dire che 2 è generatore, dal momento che il sottogruppo ciclico generato da 2 ha ordine maggiore di 3 e quindi ordine 6, cioè è tutto il gruppo,che quindi risulta ciclico.

Esercizio 3

Bisogna fare attenzione al fatto che si tratta di un gruppo additivo, e che quindi le potenze sono in realtà i multipli degli elementi: dato k, $k^2= k+ k= 2k$; $k^3= k+k+k= 3k$ ecc.

Il gruppo in questione ha ordine 7, infatti $\mathbb{Z}_7=\{0, 1, 2 , 3, 4, 5, 6\}$.

Allora deve necessariamente essere ciclico, dal momento che non può avere sottogruppi propri; a parte il neutro, 0, che genera solo se stesso, e quindi il sottogruppo di ordine 1, ogni altro elemento genera un sottogruppo di ordine 7 (l'unico altro divisore di 7), cioè è un generatore.

Esercizio 4

Risulta $\mathbb{Z}^*_{10}=\{1, 3, 7, 9\}$ (elementi più piccoli di 10 e primi con 10} e quindi ha ordine 4.

Vediamo il periodo dei suoi elementi:

- 1 ha periodo 1
- 3; $3^2=9$; 3^3 non c'è bisogno di calcolarlo, dato che abbiamo già passato il periodo 2, che è il massimo possibile per un elemento che non generi tutto lo spazio: 3 è generatore, quindi il gruppo è ciclico.

Esercizio 5

È noto dalla teoria che ogni $(\mathbb{Z}_n,+)$ è ciclico e un suo generatore è 1.

Ricordiamo che si tratta di un gruppo additivo, e che quindi le potenze sono in realtà i multipli degli elementi: dato k, $k^2 = k+k = 2k$; $k^3 = k+k+k = 3k$ ecc.

Allora con le convenzioni di scrittura che abbiamo posto è:

$$1=1^1,\ 2=1^2,\ 3=1^3,\ 4=1^4,\ 5=1^5,\ 6=1^6,\ 7=1^7,\ 8=1^8,\ 0=1^9$$

Sappiamo che un elemento è generatore di questo gruppo (che ha ordine 9) se ha periodo 9, cioè se il più piccolo esponente a cui deve essere elevato per avere il neutro è 9.

Dal momento che gli elementi sono già potenze di un generatore e sappiamo che la potenza di una potenza ha per esponente il prodotto degli esponenti, dobbiamo trovare le "potenze" di 1 il cui esponente, moltiplicato per l'incognito periodo p dia un multiplo di 9 solo se $p=9$.

Gli esponenti che interessano sono quindi i numeri primi con 9, e quindi 1, 2, 4, 5, 7, 8 e poiché $1^k=k$ questi elementi 1, 2, 4, 5, 7, 8 sono i generatori di $(\mathbb{Z}_9,+)$.

Esercizio 6

Abbiamo visto in un esercizio precedente che $(\mathbb{Z}^*_7,\times)$ è un gruppo ciclico e che 3 è un suo generatore; più precisamente:

$$3^1=3;\ 3^2=2;\ 3^3=6;\ 3^4=4;\ 3^5=5;\ 3^6=1.$$

Di tali esponenti, solo 1 e 5 sono primi con l'ordine 6 del gruppo, quindi solo 3 e $3^5=5$ sono i generatori di $(\mathbb{Z}^*_7,\times)$.

Degli altri elementi:

- $3^2=2$ e $3^4=4$ hanno periodo 3, infatti $(3^2)^3=3^6=1$ e $(3^4)^3=3^{12}=1$, quindi generano il sottogruppo di ordine 3 $\{1, 2, 4\}$;
- $3^3=6$ ha periodo 2, infatti $(3^3)^2=3^6=1$ e genera il sottogruppo di ordine 2 $\{1, 6\}$;
- 1 genera solo se stesso: $\{1\}$ sottogruppo improprio di ordine 1.

Esercizio 7

Essendo 11 un numero primo,sappiamo dalla teoria che $(\mathbb{Z}^*_{11},\times)$ è sicuramente un gruppo ciclico. $(\mathbb{Z}^*_{11},\times)$ ha ordine 10, infatti $\mathbb{Z}^*_{11}=\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, cerchiamone un generatore.

I suoi due sottogruppi propri hanno ordine 2 e 5.

$2^1=2$; $2^2=4$; $2^3=8$; $2^4=16\equiv 5$; $2^5=2^1\times 2^4\equiv 2\times 5=10$; $2^6=2\times 2^5\equiv 2\times 10\equiv 9$: $2^7=2\times 2^6=2\times 9\equiv 7$; $2^8=2\times 2^7\equiv 2\times 7\equiv 3$; $2^9=2\times 2^8=2\times 3\equiv 6$; $2^{10}=2\times 2^9\equiv 2\times 6\equiv 1$

2 è quindi un generatore e gli altri generatori hanno esponenti primi con 10, quindi 3, 7, 9 quindi i generatori sono 2, 8, 7, 6.

Degli altri elementi:

- $2^2=4$, $2^4=5$, $2^6=9$, $2^8=3$ e $2^{10}=1$ appartengono anche al sottogruppo di ordine 5;
- $2^5=10$ e $2^{10}=1$ appartengono anche al sottogruppo di ordine 2.

Esercizio 8

Risulta $(G, ¤) = \{g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}=n\}$ (ove n è il neutro dell'operazione ¤).

- Genera il sottogruppo di ordine 2 quell'elemento il cui quadrato è n, quindi g^6, dato che $(g^6)^2=g^{12}=n$.
- Genera il sottogruppo di ordine 3 quell'elemento il cui cubo è n, quindi g^4; dato che $(g^4)^3=g^{12}=n$. Al sottogruppo appartengono $\{g^4, g^8, n\}$ e anche g^8 genera lo stesso sottogruppo.
- Genera il sottogruppo di ordine 4 l'elemento g^3 infatti $(g^3)^4=g^{12}=n$. Al sottogruppo appartengono $\{g^3, g^6, g^9, n\}$ e anche g^9 genera lo stesso sottogruppo, mentre g^6 abbiamo visto che genera il sottogruppo di ordine 2 (=4/2)
- Genera il sottogruppo di ordine 6 l'elemento g^2 infatti $(g^2)^6=g^{12}=n$. Al sottogruppo appartengono $\{g^2, g^4, g^6, g^8, g^{10}, n\}$; anche g^{10} genera lo stesso sottogruppo, mentre gli altri 3 elementi abbiamo già trovato cosa generano.
- Sono rimasti esclusi da questo elenco g, g^5, g^7, g^{11} che sono i generatori del gruppo.

Esercizio 9

Il discorso è analogo a quello dell'esercizio precedente.

Risulta $(G, ¤) = \{g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}, g^{13}, g^{14}, g^{15}=n\}$ (ove n è il neutro dell'operazione ¤).

- Il sottogruppo di ordine 3 è generato da g^5, infatti $(g^5)^3 = g^{15} = n$. Al sottogruppo appartengono $\{g^5, g^{10}, g^{15}, n\}$ e anche g^{10} genera lo stesso sottogruppo.
- Il sottogruppo di ordine 5 è generato da g^3, infatti $(g^3)^5 = g^{15} = n$. Al sottogruppo appartengono $\{g^3, g^6, g^9, g^{12}, g^{15}, n\}$ e anche gli altri elementi (a parte n) generano lo stesso sottogruppo, dal momento che un sottogruppo di ordine 5 non può a sua volta avere sottogruppi, visto che 5 è primo.
- Sono generatori tutti gli elementi il cui esponente è primo con 15, cioè: $g, g^2, g^4, g^7, g^8, g^{11}, g^{13}$ e g^{14}.

Esercizio 10

- Poiché $\mathbb{Z}^*_n$ è costituito da tutti gli elementi più piccoli di n e primi con n, $n-1$ appartiene perché è sempre primo con n, per ogni n. Infatti $n \equiv 1 \bmod n-1$, per ogni n, per cui non possono avere divisori comuni.
- Risulta $(n-1)^2 = n^2 - 2n + 1 = n(n-2)+1$ e $n(n-2) \equiv 0 \bmod n$ per cui $(n-1)^2 \equiv 1$ quindi $n-1$ ha periodo 2.

Eserciziario – Omomorfismi di gruppi

TESTO DEGLI ESERCIZI

Esercizio 1

Sia $(G, \circ)$ un gruppo ciclico di ordine 6 e sia g un suo generatore.

- Stabilire quanti e quali omomorfismi f esistono tra $(Z_6,+)$ e $(G, \circ)$.
- Stabilire quanti e quali omomorfismi j esistono tra $(G, \circ)$ e $(Z_6,+)$.

Esercizio 2

Sia $(G, \circ)$ un gruppo ciclico di ordine 12 e sia g un suo generatore. Stabilire quanti e quali omomorfismi f: $(Z_8,+) \rightarrow (G,\circ)$ esistono.

Esercizio 3

Sia $(G, \circ)$ un gruppo ciclico di ordine 12 e sia g un suo generatore. Stabilire quanti e quali omomorfismi f: $(Z_8^*,\times) \rightarrow (G,\circ)$ esistono.

Esercizio 4

- Determinare, se esiste, un omomorfismo $(Z_{10},+) \rightarrow (Z^*_{10},\times)$ diverso da quello banale.
- Determinare, se esiste, un omomorfismo $(Z^*_{10},\times) \rightarrow (Z_{10},+)$ diverso da quello banale.

Esercizio 5

Determinare tutti i possibili omomorfismi f :$(Z_6,+) \rightarrow (Z^*_9,\times)$, dopo aver studiato per quanto possibile i due gruppi.

Esercizio 6

Determinare tutti i possibili omomorfismi f : $(Z^*_8,\times) \rightarrow (Z_8,+)$ dopo aver studiato per quanto possibile i due gruppi.

Esercizio 7

- Determinare tutti i possibili omomorfismi del gruppo del triangolo in $(Z_6,+)$.
- Determinare tutti i possibili omomorfismi di $(Z_6,+)$ nel gruppo del triangolo.
- Esistono isomorfismi?

Esercizio 8

Si consideri il gruppo S_7 delle permutazioni sugli elementi 1, 2, ... ,7.

- Scrivere la permutazione $\alpha = (2\ 3\ 5)(4\ 3\ 7)(3\ 7\ 6)(1\ 5\ 2)$ come prodotto di cicli disgiunti.
- Determinare l'ordine e gli elementi del sottogruppo $\boldsymbol{G}$ di di S_7 generato da α.
- Determinare tutti i possibili omomorfismo di $\boldsymbol{G}$ in $(Z_6,+)$ e di $(Z_9,+)$ in $\boldsymbol{G}$.

Esercizio 9

Si consideri il gruppo $(P_1[x],+)$ dei polinomi di grado non superiore a 1, con coefficienti in Z_3.

- Stabilire l'ordine di $P_1[x]$ ed elencarne gli elementi.
- Stabilire se $P_1[x]$ è un gruppo ciclico.
- Individuare tutti i sottogruppi di $P_1[x]$.
- Stabilire se esistono omomorfismi tra il gruppo $(P_1[x],+)$ e il gruppo $(Z_9,+)$ e in caso positivo, indicarli.

Esercizio 10

Si consideri il gruppo $(P_2[x],+)$ dei polinomi di grado non superiore a 2, con coefficienti in Z_2.

- Stabilire l'ordine di $P_2[x]$ ed elencarne gli elementi.
- Stabilire se $P_2[x]$ è un gruppo ciclico.
- Individuare tutti i sottogruppi di $P_2[x]$.
- Stabilire se esistono omomorfismi tra il gruppo $(P_2[x],+)$ e il gruppo $(Z_6,+)$ e indicarli.
- Stabilire se esistono omomorfismi tra il gruppo$(Z_6,+)$ e il gruppo $(P_2[x],+)$ e indicarli.
- Stabilire se esistono omomorfismi tra il gruppo $(P_2[x],+)$ e il gruppo $(Z_8,+)$ e indicarli.

SOLUZIONE DEGLI ESERCIZI

Esercizio 1

Risulta $(\boldsymbol{G}, \circ) = \{g, g^2, g^3, g^4, g^5, g^6=n\}$.

Anche $(Z_6,+)=\{0, 1, 2, 3, 4, 5\}$ ha ordine 6 ed è ciclico (1 è un suo generatore).

Essendo i due gruppi entrambi ciclici, si può costruire sia per individuare gli f che per individuare i j una tabella mettendo nella prima colonna gli elementi del dominio, partendo da un generatore e successivamente dalle sue potenze, e nella prima riga gli elementi del codominio.

j	1	2	3	4	5	0
g	1	2	3	4	5	0
g^2	2	4	0	2	4	0
g^3	3	0	3	0	3	0
g^4	4	2	0	4	2	0
g^5	5	4	3	2	1	0
$g^6=n$	0	0	0	0	0	0
	iso	sì	sì	sì	iso	sì

f	g	g^2	g^3	g^4	g^5	n
1	g	g^2	g^3	g^4	g^5	n
2	g^2	g^4	n	g^2	g^4	n
3	g^3	n	g^3	n	g^3	n
4	g^4	g^2	n	g^4	g^2	n
5	g^5	g^4	g^3	g^2	g	n
0	n	n	n	n	n	n
	iso	sì	sì	sì	iso	sì

Dopo aver mandato il generatore scelto nell'elemento caratterizzante la colonna, si completa la colonna rispettando l'operazione, che è sempre la potenza, ma nel caso dei gruppi additivi risulta coincidere col multiplo.

Se dopo aver compilato la colonna il trasformato del neutro risulta essere il neutro si tratta di un omomorfismo; tale omomorfismo, se gli elementi che compaiono nella colonna sono tutti quelli del codominio è addirittura un isomorfismo, cosa in questo caso possibile perché i due gruppi hanno lo stesso ordine.

Osservazione: gli isomorfismi, quando esistono, si hanno nel caso di un generatore che viene trasformato in un generatore.

Esercizio 2

Risulta $(\boldsymbol{G}, \circ) = \{g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}=n\}$.

Anche $(Z_8,+)=\{0, 1, 2, 3, 4, 5, 6, 7\}$ è ciclico (1 è un suo generatore) ed ha ordine 8.

Gli omomorfismi di tipo f si possono costruire con la tabella, essendo il dominio ciclico.

Dato che gli elementi del codominio sono molti, scriviamo solo quelli che danno luogo ad un omomorfismo. Poiché il dominio ha ordine 8, si avranno degli omomorfismi solo quando il generatore del dominio, che ha periodo 8, viene trasformato in un elemento la cui ottava potenza sia il neutro, cioè che abbia periodo 8, o 4 o 2. Nessun elemento di un gruppo di ordine 12 ha periodo 8 (altrimenti genererebbe un sottogruppo di ordine 8 che non può esistere per il teorema di Lagrange).

g^6 ha periodo 2 e g^3 e g^9 periodo 4; quindi gli omomorfismi possibili sono:

f	g^3	g^6	g^9	n
1	g^3	g^6	g^9	n
2	g^6	n	g^6	n
3	g^9	g^6	g^3	n
4	n	n	n	n
5	g^3	g^6	g^9	n
6	g^6	n	g^6	n
7	g^9	g^6	g^3	n
0	n	n	n	n

Ovviamente nessuno di essi è un isomorfismo, poiché dominio e codominio hanno ordini diversi.

Il primo e il terzo hanno per nucleo {0, 4} e per immagine $\{g^3, g^6, g^9, n\}$, il secondo ha per nucleo {0, 2, 4, 6} e per immagine $\{ g^6, n\}$, l'ultimo è l'omomorfismo banale, che ha per nucleo tutto il dominio.

Esercizio 3

Risulta $(\boldsymbol{G}, \circ) = \{g, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9, g^{10}, g^{11}, g^{12}=n\}$.

$(Z_8^*, \times)=\{1, 3, 5, 7\}$, quindi ha ordine 4.

Per vedere se è ciclico cerchiamo un generatore. Risulta $3^2=9\equiv1$; $5^2=25\equiv1$ e $7^2=49\equiv1$ quindi tutti gli elementi diversi dal neutro hanno periodo 2. Quindi non è ciclico, ma ha tre sottogruppi di ordine 2.

Prima di cercare gli omomorfismi, qualche osservazione: anche se 4 è un divisore di 12, non può esistere un omomorfismo che abbia il nucleo ridotto al solo neutro, altrimenti il dominio sarebbe isomorfo all'immagine, cosa non possibile, dal momento che il dominio non è ciclico mentre tutti i sottogruppi del codominio lo sono. Quindi gli unici omomorfismi esistenti (oltre a quello banale) hanno un nucleo e una immagine di ordine 2. L'unica immagine possibile è quindi $\{n, g^6\}$. Il nucleo può essere {1, 3} o {1, 5} o {1, 7}.

Allora gli omomorfismi mandano ordinatamente gli elementi della prima riga in quelli sottostanti:

nucleo	1	3	5	7
{1, 3}	n	n	g^6	g^6
{1, 5}	n	g^6	n	g^6
{1, 7}	n	g^6	g^6	n
{1, 3, 5, 7}	n	n	n	n

Quelli che abbiamo ottenuto sono tutti omomorfismi, cioè godono della relazione:

per ogni coppia di elementi x e y del dominio è $f(x\times y) = f(x) \circ f(y)$

Infatti sia gli elementi del dominio che i trasformati (a parte il neutro) hanno periodo 2.

Esercizio 4

$(Z_{10}, +) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ è ciclico (1 è un suo generatore) ed ha ordine 10, quindi ha un sottogruppo (ciclico) per ogni divisore dell'ordine, cioè 1, 2, 5, 10.

Il sottogruppo di ordine 5 è {0, 2, 4, 6, 8}; quello di ordine 2 {0, 5}.

$(Z^*_{10},\times) = \{1, 3, 7, 9\}$ ha ordine 4. Per vedere se è ciclico cerchiamo un generatore. $3^2=9\neq1$, quindi 3 è generatore (infatti genera un sottogruppo di ordine maggiore di 2, e quindi di ordine 4).

Anche 7 è generatore (infatti $7^2=49\neq1$) mentre non lo è 9, infatti $9^2=81\equiv1$, e quindi il sottogruppo di ordine 2 è $\{1, 9\}$.

Per il teorema sugli ordini di nucleo e immagine in un omomorfismo, per il quale:

ordine nucleo × ordine immagine = ordine dominio

- nel caso del primo punto l'unica possibilità è 10(dominio) = 5 (nucleo) × 2 (immagine);
- nel caso del secondo punto l'unica possibilità è 4 (dominio) = 2 (nucleo) × 2 (immagine).

$(Z_{10},+) \rightarrow (Z^*_{10},\times)$

nucleo	0	1	2	3	4	5	6	7	8	9
{0, 2, 4, 6, 8}	1	9	1	9	1	9	1	9	1	9

$(Z^*_{10},\times) \rightarrow (Z_{10},+)$

nucleo	1	3	7	9
{1, 9}	0	5	5	0

Quelli che abbiamo ottenuto sono tutti omomorfismi, per ogni coppia di elementi *x* e *y* del dominio è:

$$f(x+y) = f(x) \times f(y).$$

Esercizio 5

$(Z_6,+) = \{0, 1, 2, 3, 4, 5\}$ è un gruppo ciclico di ordine 6 generato da 1.

$(Z^*_9,\times) = \{1, 2, 4, 5, 7, 8\}$ ha anch'esso ordine 6. Per vedere se è ciclico vediamo se ha un generatore. $2^2=4$, $2^3=8 \neq 1$, quindi 2 è generatore (il massimo ordine di un sottogruppo proprio può essere 3…). Essendo ciclico avrà un sottogruppo di ordine 2 e uno di ordine 3.

Essendo 2 un generatore del gruppo:

- $2^2=4$ genera il sottogruppo di ordine 3, che è $\{2^2=4, 2^4=16\equiv7, 1\}$;
- $2^3=8$ genera il sottogruppo di ordine 2 $\{8, 1\}$.

I due gruppi sono quindi entrambi ciclici e dello stesso ordine, quindi sono isomorfi.

Gli omomorfismi tra i due gruppi sono:

f	1	2	4	5	7	8
1	1	2	4	5	7	8
2	1	4	7	7	4	1
3	1	8	1	8	1	8
4	1	7	4	4	7	1
5	1	5	7	2	4	8
0	1	1	1	1	1	1
	banale	iso	sì	iso	sì	sì

Esercizio 6

$(\mathbb{Z}_8,+) = \{0, 1, 2, 3, 4, 5, 6, 7\}$ sappiamo essere un gruppo ciclico di ordine 8 generato da 1.

$(\mathbb{Z}^*_8,\times) = \{1, 3, 5, 7\}$, ha ordine 4. Abbiamo già visto che non è ciclico, poiché risulta $3^2=9\equiv1$; $5^2=25\equiv1$ e $7^2=49\equiv1$ quindi tutti gli elementi diversi dal neutro hanno periodo 2 e dunque ha tre sottogruppi di ordine 2.

Non si può quindi costruire la tabella dei corrispondenti di un generatore, visto che non esiste.

Per la condizione:

$$\text{ordine nucleo} \times \text{ordine immagine} = \text{ordine dominio}$$

a parte l'omomorfismo banale, ci possono essere tre omomorfismi che hanno per nuclei i tre sottogruppi di ordine 2 $\{1, 3\}$, $\{1, 5\}$ e $\{1, 7\}$ e per immagine il sottogruppo di ordine 2 del codominio, cioè $\{0, 4\}$, mentre non c'è un omomorfismo di nucleo $\{1\}$ e immagine il sottogruppo di ordine 4 $\{0, 2, 4, 6\}$ poiché sarebbe un isomorfismo con l'immagine, cosa impossibile dato che uno non è ciclico mentre l'altro lo è.

Allora gli omomorfismi sono:

Nucleo	1	3	5	7
{1, 3}	0	0	4	4
{1, 5}	0	4	0	4
{1, 7}	0	4	4	0
{1, 3, 5, 7}	0	0	0	0

La condizione che caratterizza gli omomorfismi è sicuramente soddisfatta.

Esercizio 7

Il gruppo $(\mathbb{Z}_6,+)$ è notoriamente un gruppo ciclico di ordine è generato da 1; ha un sottogruppo proprio di ordine 3: $\{0, 2, 4\}$ e uno di ordine 2: $\{0, 3\}$.

Il gruppo del triangolo ricordiamo che ha ordine 6, non è ciclico, e ammette come sottogruppi

- il sottogruppo di ordine 3 delle rotazioni $\{R_1, R_2, I\}$,
- tre sottogruppi di ordine 2 delle simmetrie assiali rispetto ai tre assi passanti per i vertici *A*, *B*, *C*: $\{S_A, I\}$; $\{S_B, I\}$;$\{S_C, I\}$.

Allora non può esistere un isomorfismo, dato che i due gruppi hanno natura diversa.

Per gli omomorfismi del gruppo del triangolo in $(\mathbb{Z}_6,+)$, quello che ha per nucleo $\{R_1, R_2, I\}$ e per immagine $\{0, 3\}$e facilmente determinabile:

Nucleo	I	R_1	R_2	S_A	S_B	S_C
$\{R_1, R_2, I\}$	0	0	0	3	3	3

Se il nucleo è $\{S_A, I\}$ sappiamo che: $I \to 0$ e $S_A \to 0$ per definizione di nucleo.

∘	I	R_1	R_2	S_A	S_B	S_C
I	I	R_1	R_2	S_A	S_B	S_C
R_1	R_1	R_2	I	S_C	S_A	S_B
R_2	R_2	I	R_1	S_B	S_C	S_A
S_A	S_A	S_B	S_C	I	R_1	R_2
S_B	S_B	S_C	S_A	R_2	I	R_1
S_C	S_C	S_A	S_B	R_1	R_2	I

Per gli altri elementi possiamo ragionare in due modi (la tabella moltiplicativa è riportata a fianco):

- se $R_1 \to 2$, $R_2 = R_1 \circ R_1 \to 2+2=4$; $S_B = S_A \circ R_1 \to 0+2=2$, $S_C = S_A \circ R_2 \to 0+4=4$ e poi provare cosa succede se invece $R_1 \to 4$, con tutto quel che segue;
- costruire i laterali del nucleo $\{S_A, I\} \circ R_1 = \{S_B, R_1\}$ e $\{S_A, I\} \circ R_2 = \{S_C, R_2\}$; se $R_1 \to 2$ anche tutto il laterale è trasformato nello stesso elemento, e quindi l'altro laterale in 4 e viceversa.

Ne viene lo schema:

Nucleo	I	R_1	R_2	S_A	S_B	S_C
$\{R_1, R_2, I\}$	0	0	0	3	3	3
$\{S_A, I\}$	0	2	4	0	2	4
……	…	…	…	…	…	…

In tutti i casi, verifichiamo ora di aver ottenuto veramente un omomorfismo, cioè che per ogni coppia di elementi x e y del dominio sia $f(x \circ y) = f(x) + f(y)$. La cosa è vera per il primo omomorfismo (per esempio $f(S_A \circ S_A) = f(I) = 0 = 3+3$ (infatti l'elemento S_A e l'elemento 3 hanno lo stesso periodo), ma non per gli altri: nel secondo $f(S_B \circ S_B) = f(I) = 0 \neq 2+2$ quindi NON è un omomorfismo, e così per gli altri: un elemento di periodo 2 non può essere trasformato in uno di periodo 3.

Per quello che riguarda gli omomorfismi di $(Z_6,+)$ nel gruppo del triangolo, essendo il dominio ciclico basta costruire la tabella:

	I	R_1	R_2	S_A	S_B	S_C
1	I	R_1	R_2	S_A	S_B	S_C
2	I	R_2	R_1	I	I	I
3	I	I	I	S_A	S_B	S_C
4	I	R_1	R_2	I	I	I
5	I	R_2	R_1	S_A	S_B	S_C
0	I	I	I	I	I	I
	sì	sì	sì	sì	sì	sì

Esercizio 8

- Risulta $\alpha = (1\ 2)(3\ 4\ 5)(6\ 7)$.
- α è costituita da tre cicli di lunghezze 2 o 3, quindi mcm(2,3,2)=6 e dunque $\boldsymbol{G}$ ha ordine 6. Risulta:
- $\boldsymbol{G} = \{\alpha=(1\ 2)(3\ 4\ 5)(6\ 7), \alpha^2=(3\ 5\ 4), \alpha^3=(1\ 2)(6\ 7), \alpha^4=(3\ 4\ 5), \alpha^5=(1\ 2)(3\ 5\ 4)(6\ 7), \alpha^6=n\}$
- Essendo ciclico, ha solo due sottogruppi propri, $\{\alpha^2, \alpha^4, n\}$ di ordine 3 e $\{\alpha^3, n\}$ di ordine 2.
- Essendo $\boldsymbol{G}$ ciclico, la tabella degli omomorfismi $f: \boldsymbol{G} \to (Z_6,+)$ è:

f	1	2	3	4	5	0
α	1	2	3	4	5	0
α^2	2	4	0	2	4	0
α^3	3	0	3	0	3	0
α^4	4	2	0	4	2	0
α^5	5	4	3	2	1	0
$\alpha^6=n$	0	0	0	0	0	0
	iso	sì	sì	sì	iso	sì

- Viceversa, anche $(Z_9,+)$ è ciclico, generato da 1, ma di ordine 9. La tabella degli omomorfismi è:

f	α	α^2	α^3	α^4	α^5	$g^6=n$
1	α	α^2	α^3	α^4	α^5	n
2	α^2	α^4	n	α^2	α^4	n
3	α^3	n	α^3	n	α^3	n
4	α^4	α^2	n	α^4	α^2	n
5	α^5	α^4	α^3	α^2	α	n
6	n	n	n	n	n	n
7	α	α^2	α^3	α^4	α^5	n
8	α^2	α^4	n	α^2	α^4	n
0	α^3	n	α^3	n	α^3	n
	no	*sì*	*no*	*sì*	*no*	*sì*
nuclei		{3,6,0}		{3,6,0}		Z_9
immag.		$\{\alpha^2, \alpha^4, n\}$		$\{\alpha^2, \alpha^4, n\}$		$\{n\}$

Esercizio 9

Gli elementi di Z_3 sono $\{0, 1, 2\}$.

- Gli elementi di $P_1[x]$ sono quindi: $\{0, 1, 2, x, 2x, x+1, 2x+1, x+2, 2x+2\}$ e dunque l'ordine è 9.
- Per vedere se $P_1[x]$ è ciclico dobbiamo vedere se esiste un elemento di periodo 9:
  - 0 ha periodo 1, come sempre il neutro;
  - 1, $1^2=1+1=2$; $1^3=1+2=3\equiv 0$, quindi 1 e 2 hanno periodo 3;
  - x, $x^2=2x$, $x^3=0$, quindi x e $2x$ hanno periodo 3;
  - $x+1$, $(x+1)^2=(x+1)+(x+1)=2x+2$; $(x+1)^3=(x+1)+(2x+2)=0$, quindi $x+1$ e $2x+2$ hanno periodo 3;
  - $2x+1$, $(2x+1)^2=(2x+1)+(2x+1)=x+2$, $(2x+1)^3=0$, quindi anche $2x+1$ e $x+2$ hanno periodo 3.
- Allora ogni elemento ha periodo3, e il gruppo non è ciclico;
- Ha 4 sottogruppi di ordine 3, generati da 1, x, $x+1$, $2x+1$ e che hanno rispettivamente elementi:
- $A=\{0, 1, 2\}$; $B=\{0, x, 2x\}$; $C=\{0, x+1, 2x+2\}$; $D=\{0, 2x+1, x+2\}$ e i due sottogruppi impropri: $\{0\}$ e $P_1[x]$.

- Sicuramente non esistono isomorfismi, visto che sono un gruppo ciclico e uno no.

  Oltre all'omomorfismo banale possono però esistere omomorfismi non banali con nucleo di ordine 3 e immagine di ordine 3; l'immagine è l'unico sottogruppo non banale di Z_9, $\{0, 3, 6\}$. I due gruppi sono costituiti entrambi da elementi di periodo 3 (a parte il neutro) quindi le trasformazioni che si otterranno sono omomorfismi, pur di costruire i laterali con gli elementi di un medesimo sottogruppo.

  - $A=\{0, 1, 2\}$ Nucleo; i laterali sono $A+x=\{x, x+1, x+2\}$ e $A+2x=\{2x, 2x+1, 2x+2\}$
  - $B=\{0, x, 2x\}$ Nucleo; i laterali sono $B+1=(1, x+1, 2x+1\}$ e $B+2=\{2, x+2, 2x+2\}$
  - $C=\{0, x+1, 2x+2\}$ Nucleo; i laterali sono $C+1=\{1, x+2, 2x\}$ e $C+2=\{2, x, 2x+1\}$
  - $D=\{0, 2x+1, x+2\}$ Nucleo; i laterali sono $D+1=\{1, 2x+2, x\}$ e $D+2=\{2, 2x, x+1\}$

  Si trovano 8 omomorfismi mandando gli elementi del nucleo in 0, quelli di un laterale in 3 e quelli dell'altro in 6, cioè:

$\{0, 1, 2\} \to 0$;	$\{x, x+1, x+2\} \to 3$;	$\{2x, 2x+1, 2x+2\} \to 6$
$\{0, 1, 2\} \to 0$;	$\{x, x+1, x+2\} \to 6$;	$\{2x, 2x+1, 2x+2\} \to 3$
$\{0, x, 2x\} \to 0$;	$\{1, x+1, 2x+1\} \to 3$;	$\{2, x+2, 2x+2\} \to 6$
$\{0, x, 2x\} \to 0$;	$\{1, x+1, 2x+1\} \to 6$;	$\{2, x+2, 2x+2\} \to 3$
$\{0, x+1, 2x+2\} \to 0$;	$\{1, x+2, 2x\} \to 3$;	$\{2, x, 2x+1\} \to 6$
$\{0, x+1, 2x+2\} \to 0$;	$\{1, x+2, 2x\} \to 6$;	$\{2, x, 2x+1\} \to 3$
$\{0, 2x+1, x+2\} \to 0$;	$\{1, 2x+2, x\} \to 3$;	$\{2, 2x, x+1\} \to 6$
$\{0, 2x+1, x+2\} \to 0$;	$\{1, 2x+2, x\} \to 6$;	$\{2, 2x, x+1\} \to 3$

Esercizio 10

Z_2 ha due soli elementi: $\{0,1\}$.

- Gli elementi di $P_2[x]$ sono quindi: $P_2[x]=\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$ quindi ha ordine 8
- Cerchiamo un generatore; individueremo contemporaneamente anche i sottogruppi.
  - 0 ha periodo 1
  - 1 ha periodo 2: $1+1\equiv 0$
  - x ha periodo 2: $x+x \equiv 0$ è chiaro che questo succede per ogni elemento: TUTTI gli elementi hanno periodo 2.

  I sottogruppi propri, di ordine 2, sono:

  $A=\{0, 1\}$; $B=\{0, x\}$; $C=\{0, x+1\}$; $D=\{0, x^2\}$; $E=\{0, x^2+1\}$; $F=\{0, x^2+x\}$; $G=\{0, x^2+x+1\}$
- A parte l'omomorfismo banale, gli eventuali omomorfismi hanno come nucleo uno dei sottogruppi di ordine 2. Poiché il prodotto dell'ordine del nucleo per quello dell'immagine deve dare 8, l'immagine non esiste, visto che $(Z_6,+)$ non può avere sottogruppi di ordine 4, quindi non ci sono omomorfismi.

- Il viceversa invece è possibile, ed essendo $(Z_6,+)$ ciclico si può usare il metodo della tabella, ottenendo gli 8 omomorfismi:

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
2	0	0	0	0	0	0	0	0
3	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
4	0	0	0	0	0	0	0	0
5	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
	sì	sì	sì	sì	sì	sì	sì	sì

- $(Z_8,+)$ ha invece ordine 8, quindi il ragionamento fatto precedentemente porta a qualche altra conseguenza possibile, forse.

  I "candidati nuclei" sono A, B, C, D, E, F, G e l'immagine potrebbe essere il sottogruppo di ordine 4 $\{0, 2, 4, 6\}$. Di questi elementi, però, solo 4 ha periodo 2; se supponiamo che il nucleo sia A, gli elementi di uno dei laterali di A ad esempio di $A+x=\{x, x+1\}$ devono essere trasformati in un elemento di periodo 2, ma questo allora non è possibile anche per gli altri laterali di A.

  In sostanza il discorso è: se il trasformato di un elemento ha periodo h, l'elemento deve avere periodo h o in generale un multiplo di h, altrimenti non si ha un omomorfismo

Eserciziario – Anelli di polinomi

TESTO DEGLI ESERCIZI

Esercizio 1

Determinare il resto della divisione del polinomio x^3-4x^2+3x+3 a coefficienti in $\mathbb{Z}$ o in $\mathbb{Z}_7$ per $x-4$.

Esercizio 2

Determinare il resto della divisione del polinomio $2x^3+4x^2+5x+10$ a coefficienti in $\mathbb{Z}_{11}$ per $x+5$.

Esercizio 3

Determinare le radici intere del polinomio x^3-3x^2+3x+9 a coefficienti in $\mathbb{Z}$.

Esercizio 4

Determinare le radici del polinomio x^3+3x^2+3x+9 a coefficienti in $\mathbb{Z}_7$.

Esercizio 5

Si considerino i due polinomi $p(x) = x^2-5x$ e $q(x) = x^3+38x^2-4x+16$ a coefficienti in $\mathbb{Z}_7$. Trovare quoziente e resto della divisione di $q(x)$ per $p(x)$.

Esercizio 6

Si considerino i due polinomi $p(x) = 2x^2-4x$ e $q(x) = x^4+5x^2-7x$ a coefficienti in $\mathbb{Z}_{11}$. Trovare quoziente e resto della divisione di $q(x)$ per $p(x)$.

Esercizio 7

Si considerino i due polinomi $p(x) = x^2-4x$ e $q(x) = x^4+5x^2-7x$ a coefficienti in $\mathbb{Z}_{11}$. Trovare quoziente e resto della divisione di $q(x)$ per $p(x)$.

Esercizio 8

Scomporre in fattori irriducibili il seguente polinomio (a coefficienti in $\mathbb{Z}_5$):

$$p(x) = 2x^4+3x^3-3x^2-6x+2$$

Esercizio 9

Scomporre in fattori irriducibili il seguente polinomio (a coefficienti in $\mathbb{Z}_5$ o in $\mathbb{Z}_7$):

$$p(x) = 2x^4+5x^3-2x^2-10x-4$$

SOLUZIONE DEGLI ESERCIZI

Esercizio 1

Basta usare il teorema del resto.

In $\mathbb{Z}$

	1	–4	3	3
4		4	0	12
	1	0	3	15

In $\mathbb{Z}_7$

	1	3	3	3
4		4	0	5
	1	0	3	1

Nel primo caso il resto è 15, nel secondo 1. Si osservi che $15 \equiv 1 \bmod 7$, quindi bastava farlo una volta e poi ridurre il resto ottenuto mod 7.

Esercizio 2

Basta usare il teorema del resto. Risulta $-5 \equiv 6$, quindi:

	2	4	5	10
6		1	8	1
	2	5	2	0

Quindi $x+5$ divide esattamente il polinomio dato.

Esercizio 3

Poiché siamo in $\mathbb{Z}$, e vogliamo radici intere, gli unici valori che possono essere radici sono 1, –1, 3, –3, 9, –9.

Per 1 e –1 il conto è immediato:

- $1-3+3+9=10 \neq 0$ quindi 1 non è radice;
- $-1-3-3+9=2 \neq 0$, quindi anche –1 non è radice;

Per 3 e –3 si può ancora usare lo stesso metodo:

- $27-27+9+9=18$, quindi 3 non è radice;
- $-27-27-9+9=-54$ quindi –3 non è radice.

Per 9 e –9 conviene usare il teorema del resto o la formula di Ruffini Corner, per avere calcoli un po' più semplici.

	1	–3	3	9	
9		9	54	513	
	1	6	57	522	$\neq 0$

	1	–3	3	9	
–9		–9	108	–999	
	1	–12	111	–990	$\neq 0$

Quindi nessuno dei valori possibili è una radice del polinomio.

Esercizio 4

Nel caso di coefficienti in $\mathbb{Z}_7$, il polinomio, che in realtà si può scrivere come x^3+3x^2+3x+2 può avere qualsiasi dei valori {1, 2, 3, 4, 5, 6} come radice (lo 0 no perché ha il termine noto).

Conviene utilizzare il teorema del resto: se si trova una radice, poi si può controllare direttamente un polinomio di grado minore.

Per 1:

	1	3	3	2
1		1	4	0
	1	4	0	2

Per 2:

	1	3	3	2
2		2	3	5
	1	5	6	0

2 è radice. Il polinomio residuo è x^2+5x+6 ; 2 potrebbe essere ancora radice (1 no, visto che non lo era di quello globale).

	1	5	6
2		2	0
	1	0	6

Non lo è. Proviamo 3:

	1	5	6
3		3	3
	1	1	9

Non lo è. Proviamo 4:

	1	5	6
4		4	8
	1	2	0

4 è radice; l'altra radice è –2, cioè 5.

Esercizio 5

Usiamo l'algoritmo di divisione, dopo aver trasformato i coefficienti in $\mathbb{Z}_7$.

$x^3 + 3x^2 + 3x + 2$ $\qquad$ x^2+2x $\quad$ quoziente $x+1$

$x^3 + 2x^2$

$x^2 + 3x + 2$

$x^2 + 2x$

$x + 2$ $\qquad$ resto.

Esercizio 6

Usiamo l'algoritmo di divisione, dopo aver trasformato i coefficienti in $\mathbb{Z}_{11}$.
Ricordiamo che l'inverso del coefficiente direttivo 2 del polinomio divisore è 6, quindi se in $\mathbb{Q}$ bisognava dividere per 2, in $\mathbb{Z}_{11}$ bisogna moltiplicare per 6.

$x^4 + 5x^2 + 4x$ $\quad 2x^2 + 7x$ $\quad$ quoziente: $6x^2 + x + 10$

$x^4 + 9x^3$
$2x^3 + 5x^2 + 4x$
$2x^3 + 7x^2$
$9x^2 + 4x$
$9x^2 + 4x$
0

Il polinomio $q(x)$ dato è divisibile per $p(x)$.

Esercizio 7

Usiamo l'algoritmo di divisione, dopo aver trasformato i coefficienti in $\mathbb{Z}_{11}$.

$x^4 + 5x^2 + 4x$ $\quad x^2 + 7x$ $\quad$ quoziente: $x^2 + 4x + 10$

$x^4 + 7x^3$
$4x^3 + 5x^2 + 4x$
$4x^3 + 6x^2$
$10x^2 + 4x$
$10x^2 + 4x$
0

Il polinomio $q(x)$ dato è divisibile per $p(x)$.

Esercizio 8

Dopo aver trasformato i coefficienti in $\mathbb{Z}_5$, cerchiamo le eventuali radici, col teorema di Ruffini, in modo da scomporre man mano il polinomio

$$p(x) = 2x^4+3x^3+2x^2+4x+2$$

Cerchiamo se 1 è radice:

	2	3	2	4	2
1		2	0	2	1
	2	0	2	1	3

No. Proviamo 2:

	2	3	2	4	2
2		4	4	2	2
	2	2	1	1	4

No. Proviamo 3:

	2	3	2	4	2
3		1	2	2	3
	2	4	4	1	0

3 è radice quindi è $p(x) = (x-3)(2x^3+4x^2+4x+1) = (x+2)(2x^3+4x^2+4x+1)$. Proviamo ancora 3:

	2	4	4	1
3		1	0	2
	2	0	4	3

Non è radice doppia. Proviamo ora il 4:

	2	4	4	1
4		3	3	3
	2	2	2	4

4 non è radice. Ora osserviamo che un polinomio di terzo grado, se è riducibile, si scompone in un polinomio di secondo grado e in uno di primo, quindi dovrebbe avere una radice. Siccome non ci sono altre radici, quella ottenuta è la massima scomposizione possibile.

Esercizio 9

Poiché il problema prevede due possibili campi diversi, possiamo risolverlo come se fossero due problemi diversi, e quindi due volte, oppure tenere i coefficienti in $\mathbb{Z}$ e tirare le conclusioni in fondo, riportando il problema nei vari campi. È conveniente usare questo metodo, ma cercheremo le radici 5 e 6 solo in $\mathbb{Z}_7$.

Radice 1:

	2	5	–2	–10	–4
1		2	7	5	–5
	2	7	5	–5	–9

In nessuno dei campi 1 è radice. Proviamo 2:

	2	5	–2	–10	–4
2		4	18	32	44
	2	9	16	22	40

2 è radice in $\mathbb{Z}_5$ ma non in $\mathbb{Z}_7$; a questo punto conviene proprio dividere i 2 casi:

$\mathbb{Z}_5$

$$p(x) = (x+3)(2x^3+4x^2+x+2)$$

Proviamo 3:

	2	4	1	2
3		1	0	3
	2	0	1	0

$$p(x) = (x+3)(x+2)(2x^2+1)$$

Proviamo ancora 3:

	2	0	1
3		1	3
	2	1	4

Proviamo ora il 4:

	2	0	1
4		3	2
	2	3	3

Non ci sono altre radici, quindi:

$$p(x) = (x+3)(x+2)(2x^2+1)$$

$\mathbb{Z}_7$

Proviamo 3:

	2	5	–2	–10	–4
3		6	5	2	4
	2	4	3	6	0

Dunque:

$$p(x) = (x+4)(2x^3+4x^2+3x+6)$$

Proviamo ancora 3:

	2	4	3	6
3		6	2	1
	2	3	5	0

Allora:

$$p(x) = (x+4)^2(2x^2+3x^2+5)$$

Proviamo ancora 3:

	2	3	5
3		6	6
	2	2	4

Proviamo ora il 4:

	2	3	5
4		1	2
	2	4	0

Allora abbiamo:

$$p(x) = (x+4)^2(x+3)(2x+4) = 2(x+4)^2(x+3)(x+2)$$

Eserciziario – Anello delle matrici

TESTO DEGLI ESERCIZI

Esercizio 1

Date le due matrici **A** e **B** seguenti, calcolare **A**+**B**, **A**–**B**, 2**B**, 3**A** – 5**B**:

$$\mathbf{A}=\begin{bmatrix}2 & 3 & 5\\ 2 & 0 & -1\end{bmatrix}\ \mathbf{B}=\begin{bmatrix}1 & -1 & 1\\ 1 & -2 & 2\end{bmatrix}$$

Esercizio 2

Date le seguenti due matrici, **A** e **B** calcolare **AB** e **BA**:

$$\mathbf{A}=\begin{bmatrix}2 & 1\\ 5 & 6\end{bmatrix},\qquad \mathbf{B}=\begin{bmatrix}1 & -2\\ 4 & 7\end{bmatrix}$$

Esercizio 3

Date le due seguenti matrici **A** e **B**, calcolare **AB** e **BA**:

$$\mathbf{A}=\begin{bmatrix}2 & 3 & 5\\ 2 & 0 & -1\end{bmatrix}\qquad \mathbf{B}=\begin{bmatrix}1 & 2\\ -1 & 3\\ -2 & 0\end{bmatrix}$$

Esercizio 4

Si consideri la matrice ad elementi in $\mathbb{Z}_9$ $\mathbf{A}=\begin{bmatrix}2 & 1\\ h & 82\end{bmatrix}$ ove h è un parametro di $\mathbb{Z}_9$.

Determinare tutti i valori di h per cui **A** è invertibile.

Esercizio 5

Calcolare l'inversa della matrice $\begin{bmatrix}2 & 5\\ 4 & 4\end{bmatrix}$ ad elementi in $\mathbb{Z}_7$.

Esercizio 6

Si consideri la matrice ad elementi in $\mathbb{Z}_8$ $\mathbf{A}=\begin{bmatrix}2 & 1\\ h & 4\end{bmatrix}$ ove h è un parametro di $\mathbb{Z}_8$.

Determinare tutti i valori di h per cui **A** è invertibile e per il più piccolo $h>0$ per cui è invertibile, determinare l'inversa.

Esercizio 7

Si consideri la matrice ad elementi in $\mathbb{Z}_{10}$ $\mathbf{A}=\begin{bmatrix} 2 & 3 \\ h & 7 \end{bmatrix}$ ove h è un parametro di $\mathbb{Z}_{10}$.

Determinare tutti i valori di h per cui **A** è invertibile e per il più piccolo $h>0$ per cui è invertibile, determinare l'inversa.

Esercizio 8

Si consideri la matrice $\mathbf{A}=\begin{bmatrix} 2 & 4 \\ 1 & 7 \end{bmatrix}$ a coefficienti in $\mathbb{Z}_h$.

Determinare tutti i valori di h, con $1< h <10$ per cui **A** è invertibile e determinare l'inversa.

Esercizio 9

Si consideri la corrispondenza che segue tra le lettere dell'alfabeto e $\mathbb{Z}_{27}$.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Determinare l'inversa della matrice $A=\begin{bmatrix} 5 & 1 \\ 1 & 1 \end{bmatrix}$ a coefficienti in $\mathbb{Z}_{27}$.

Scrivere le prime 4 lettere del proprio nome a gruppi di 2 e trasformarli in vettori numerici mediante la corrispondenza data. Usare A per crittografare le prime 4 lettere del proprio nome e successivamente A^{-1} decrittografare le lettere ottenute.

Esercizio 10

Si consideri la corrispondenza che segue tra le lettere dell'alfabeto e $\mathbb{Z}_{27}$.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Determinare l'inversa della matrice $A=\begin{bmatrix} 5 & 1 \\ 1 & 3 \end{bmatrix}$ a coefficienti in $\mathbb{Z}_{27}$.

Scrivere le prime 4 lettere del proprio nome a gruppi di 2 e trasformarli in vettori numerici mediante la corrispondenza data. Usare A per crittografare tali lettre e successivamente A^{-1} decrittografare le lettere ottenute. L'algoritmo di crittografia è il prodotto della matrice per il vettore.

Esercizio 11

Si consideri la corrispondenza che segue tra le lettere dell'alfabeto e $\mathbb{Z}_{27}$.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Determinare il più piccolo $h \geq 0$ per cui la matrice $\begin{bmatrix} 2 & 3+2t \\ 1 & h+t \end{bmatrix}$ è invertibile per qualsiasi valore di t (parametro in $\mathbb{Z}_{27}$). Per tale valore determinarne l'inversa.

Scrivere le prime 4 lettere del proprio nome a gruppi di 2 e trasformarli in vettori numerici mediante la corrispondenza data. Usare le due matrici per crittografare "parola" usando in successione al posto di t le tre cifre 275.

Esercizio 12

Si consideri la corrispondenza che segue tra le lettere dell'alfabeto e $\mathbb{Z}_{27}$.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Determinare una matrice **B** che moltiplicata a destra per **A=** $\begin{bmatrix} 2 & 3 & 1 \\ 9 & 1 & 0 \end{bmatrix}$ dia la matrice identica (**AB**=**I**). Usare le due matrici per cifrare "parola" e successivamente decifrare le lettere ottenute.

SOLUZIONE DEGLI ESERCIZI

Esercizio 1

$$\mathbf{A}+\mathbf{B}=\begin{bmatrix}3 & 2 & 6\\ 3 & -2 & 1\end{bmatrix}$$

$$\mathbf{A}-\mathbf{B}=\begin{bmatrix}1 & 4 & 4\\ 1 & 2 & -3\end{bmatrix}$$

$$2\mathbf{B}=\begin{bmatrix}2 & -2 & 2\\ 2 & -4 & 4\end{bmatrix}$$

$$3\mathbf{A}-5\mathbf{B}=\begin{bmatrix}6 & 9 & 15\\ 6 & 0 & -3\end{bmatrix}-\begin{bmatrix}5 & -5 & 5\\ 5 & -10 & 10\end{bmatrix}=\begin{bmatrix}1 & 14 & 10\\ 1 & 10 & -13\end{bmatrix}$$

Esercizio 2

Risulta:

$$\mathbf{AB}=\begin{bmatrix}2 & 1\\ 5 & 6\end{bmatrix}\begin{bmatrix}1 & -2\\ 4 & 7\end{bmatrix}=\begin{bmatrix}2\cdot 1+1\cdot 4 & 2\cdot(-2)+1\cdot 7\\ 5\cdot 1+6\cdot 4 & 5\cdot(-2)+6\cdot 7\end{bmatrix}=\begin{bmatrix}6 & 3\\ 29 & 32\end{bmatrix}$$

Mentre:

$$\mathbf{BA}=\begin{bmatrix}1 & -2\\ 4 & 7\end{bmatrix}\begin{bmatrix}2 & 1\\ 5 & 6\end{bmatrix}=\begin{bmatrix}1\cdot 2+(-2)\cdot 5 & 1\cdot 1+(-2)\cdot 6\\ 4\cdot 2+7\cdot 5 & 4\cdot 1+7\cdot 6\end{bmatrix}=\begin{bmatrix}-8 & -11\\ 43 & 46\end{bmatrix}$$

Esercizio 3

Risulta:

$$\mathbf{AB}=\begin{bmatrix}-11 & 13\\ 4 & 4\end{bmatrix}$$

$$\mathbf{BA}=\begin{bmatrix}6 & 3 & 3\\ 4 & -3 & -8\\ -4 & -6 & -10\end{bmatrix}$$

Esercizio 4

Risulta $\mathbf{A}=\begin{bmatrix} 2 & 1 \\ h & 1 \end{bmatrix}$, e quindi det $\mathbf{A}= 2-h$. La matrice è invertibile se il suo determinante è un elemento invertibile di Z_9, cioè un elemento di $(Z^*_9,\times)=\{1, 2, 4, 5, 7, 8\}$, il che significa che deve essere:

- $2-h=1 \quad \Rightarrow \quad \boldsymbol{h=1}$,
- $2-h=2 \quad \Rightarrow \quad \boldsymbol{h=0}$;
- $2-h=4 \quad \Rightarrow \quad \boldsymbol{h=7}$;
- $2-h=5 \quad \Rightarrow \quad \boldsymbol{h=6}$;
- $2-h=5 \quad \Rightarrow \quad \boldsymbol{h=4}$;
- $2-h=8 \quad \Rightarrow \quad \boldsymbol{h=3}$.

Esercizio 5

Risulta $\det\begin{bmatrix} 2 & 5 \\ 4 & 4 \end{bmatrix}=8-20=-12\equiv 2 \bmod 7$.

L'inverso di 2 in $(Z^*_7,\times)$ è 4 ($4\times2=8\equiv 1$).

Allora:

$$\begin{bmatrix} 2 & 5 \\ 4 & 4 \end{bmatrix}^{-1}=\begin{bmatrix} 4\times4 & -5\times4 \\ -4\times4 & 2\times4 \end{bmatrix}=\begin{bmatrix} 16 & -20 \\ -16 & 8 \end{bmatrix}\equiv\begin{bmatrix} 2 & 1 \\ 5 & 1 \end{bmatrix}$$

Esercizio 6

In Z_8 sono invertibili 1, 3, 5, 7.

$\Delta=\det A=\det\begin{bmatrix} 2 & 1 \\ h & 4 \end{bmatrix}\equiv 8-h$ risulta invertibile se :

$\Delta=8-h=1 \Rightarrow \boldsymbol{h=7}$; $\Delta=8-h=3 \Rightarrow \boldsymbol{h=5}$; $\Delta=8-h=5 \Rightarrow \boldsymbol{h=3}$; $\Delta=8-h=7 \Rightarrow \boldsymbol{h=1}$.

In $(Z^*_8,\times)$ ogni elemento è inverso di se stesso, quindi, posto $\Delta = \det M=\det\begin{bmatrix} x & y \\ z & w \end{bmatrix}$, dalla formula

$M^{-1}=\begin{bmatrix} x & y \\ z & w \end{bmatrix}^{-1}=\Delta^{-1}\times\begin{bmatrix} w & -y \\ -z & x \end{bmatrix}$ ricaviamo, se $h=1$, quindi $\Delta^{-1}=7$, $\begin{bmatrix} 2 & 1 \\ 1 & 4 \end{bmatrix}^{-1}=\begin{bmatrix} 4 & 1 \\ 1 & 6 \end{bmatrix}$.

Per gli altri valori di h, non richiesti dall'esercizio, risulta comunque:

se $h=3$, quindi $\Delta^{-1}=5$, $\begin{bmatrix} 2 & 1 \\ 3 & 4 \end{bmatrix}^{-1}=\begin{bmatrix} 4 & 3 \\ 1 & 2 \end{bmatrix}$;

se $h=5$, quindi $\Delta^{-1}=3$, $\begin{bmatrix} 2 & 1 \\ 5 & 4 \end{bmatrix}^{-1}=\begin{bmatrix} 4 & 5 \\ 1 & 6 \end{bmatrix}$;

se $h=7$, quindi $\Delta^{-1}=1$, $\begin{bmatrix} 2 & 1 \\ 7 & 4 \end{bmatrix}^{-1}=\begin{bmatrix} 4 & 7 \\ 1 & 2 \end{bmatrix}$.

Esercizio 7

In $\mathbb{Z}_{10}$ sono invertibili 1, 3, 7, 9.

$\Delta = \det A = \det \begin{bmatrix} 2 & 3 \\ h & 7 \end{bmatrix} \equiv 4-3h$ risulta invertibile se:

$$4-3h=1 \Rightarrow \boldsymbol{h=1};\quad \Delta^{-1}=1$$
$$4-3h=3 \Rightarrow \boldsymbol{h=7};\quad \Delta^{-1}=7$$
$$4-3h=7 \Rightarrow \boldsymbol{h=9};\quad \Delta^{-1}=3$$
$$4-3h=9 \Rightarrow \boldsymbol{h=5};\quad \Delta^{-1}=9$$

$M^{-1}=\begin{bmatrix} x & y \\ z & w \end{bmatrix}^{-1} = \Delta^{-1} \times \begin{bmatrix} w & -y \\ -z & x \end{bmatrix}$ ricaviamo, se $\boldsymbol{h=1}$ che è il valore richiesto: $\begin{bmatrix} 2 & 3 \\ 1 & 7 \end{bmatrix}^{-1} = \begin{bmatrix} 7 & 7 \\ 9 & 2 \end{bmatrix}$.

Per gli altri valori di h, non richiesti dall'esercizio, risulta comunque:

$$\begin{bmatrix} 2 & 3 \\ 7 & 7 \end{bmatrix}^{-1} = \begin{bmatrix} 9 & 9 \\ 1 & 4 \end{bmatrix} \text{ se } \boldsymbol{h=7};$$
$$\begin{bmatrix} 2 & 3 \\ 9 & 7 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 1 \\ 3 & 6 \end{bmatrix} \text{ se } \boldsymbol{h=9};$$
$$\begin{bmatrix} 2 & 3 \\ 5 & 7 \end{bmatrix}^{-1} = \begin{bmatrix} 3 & 3 \\ 5 & 8 \end{bmatrix} \text{ se } \boldsymbol{h=5}$$

Esercizio 8

Risulta $\Delta = \det \mathbf{A} = 10$.

10 è un elemento invertibile in:

- $\mathbb{Z}_3$ (in cui vale 1) e $\Delta^{-1}=1$,
- $\mathbb{Z}_7$ (in cui vale 3) e $\Delta^{-1}=5$,
- $\mathbb{Z}_9$ (in cui vale 1) e $\Delta^{-1}=1$.

Da $\begin{bmatrix} x & y \\ z & w \end{bmatrix}^{-1} = \Delta^{-1} \times \begin{bmatrix} w & -y \\ -z & x \end{bmatrix}$ ricaviamo in:

$$\mathbb{Z}_3 \Rightarrow \mathbf{A}^{-1}=\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & 2 \\ 2 & 2 \end{bmatrix},$$
$$\mathbb{Z}_7 \Rightarrow \mathbf{A}^{-1}=\begin{bmatrix} 2 & 4 \\ 1 & 0 \end{bmatrix}^{-1} = \begin{bmatrix} 0 & 1 \\ 2 & 3 \end{bmatrix},$$
$$\mathbb{Z}_9 \Rightarrow \mathbf{A}^{-1}=\begin{bmatrix} 2 & 4 \\ 1 & 7 \end{bmatrix}^{-1} = \begin{bmatrix} 7 & 5 \\ 8 & 2 \end{bmatrix}.$$

Esercizio 9

Risulta detA=4, che è un elemento invertibile di Z_{27}, in quanto primo con 27. Risulta $4^{-1}=7$.

Allora $A^{-1}=\begin{bmatrix} 1\times 4^{-1} & -1\times 4^{-1} \\ -1\times 4^{-1} & 5\times 4^{-1} \end{bmatrix}=\begin{bmatrix} 7 & 20 \\ 20 & 8 \end{bmatrix}$

Usiamo "nome" come nome proprio. L'algoritmo da usare è:

$$\begin{bmatrix} 5 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 14 \\ 15 \end{bmatrix}=\begin{bmatrix} 85 \\ 29 \end{bmatrix}\equiv\begin{bmatrix} 4 \\ 2 \end{bmatrix}=\begin{bmatrix} D \\ B \end{bmatrix} \text{ e } \begin{bmatrix} 5 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 13 \\ 5 \end{bmatrix}=\begin{bmatrix} 70 \\ 18 \end{bmatrix}\equiv\begin{bmatrix} 16 \\ 18 \end{bmatrix}=\begin{bmatrix} P \\ R \end{bmatrix}$$

E analogamente per decrittografare:

$$\begin{bmatrix} 7 & 20 \\ 20 & 8 \end{bmatrix}\begin{bmatrix} 4 \\ 2 \end{bmatrix}\equiv\begin{bmatrix} 14 \\ 15 \end{bmatrix}=\begin{bmatrix} N \\ O \end{bmatrix} \text{ e } \begin{bmatrix} 7 & 20 \\ 20 & 8 \end{bmatrix}\begin{bmatrix} 16 \\ 18 \end{bmatrix}=\begin{bmatrix} 13 \\ 5 \end{bmatrix}=\begin{bmatrix} M \\ E \end{bmatrix}$$

Esercizio 10

Risulta detA=14, che è un elemento invertibile di Z_{27}, in quanto primo con 27. Risulta $14^{-1}=2$.

Allora $A^{-1}=\begin{bmatrix} 3\times 14^{-1} & -1\times 14^{-1} \\ -1\times 14^{-1} & 5\times 14^{-1} \end{bmatrix}=\begin{bmatrix} 6 & 25 \\ 25 & 10 \end{bmatrix}$

Usiamo "nome" come nome proprio. L'algoritmo da usare è:

$$\begin{bmatrix} 5 & 1 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 14 \\ 15 \end{bmatrix}=\begin{bmatrix} 85 \\ 59 \end{bmatrix}\equiv\begin{bmatrix} 4 \\ 5 \end{bmatrix}=\begin{bmatrix} D \\ E \end{bmatrix} \text{ e } \begin{bmatrix} 5 & 1 \\ 1 & 3 \end{bmatrix}\begin{bmatrix} 13 \\ 5 \end{bmatrix}=\begin{bmatrix} 70 \\ 28 \end{bmatrix}\equiv\begin{bmatrix} 16 \\ 1 \end{bmatrix}=\begin{bmatrix} P \\ A \end{bmatrix}$$

E analogamente per decrittografare :

$$\begin{bmatrix} 6 & 25 \\ 25 & 10 \end{bmatrix}\begin{bmatrix} 4 \\ 5 \end{bmatrix}\equiv\begin{bmatrix} 14 \\ 15 \end{bmatrix}=\begin{bmatrix} N \\ O \end{bmatrix} \text{ e } \begin{bmatrix} 6 & 25 \\ 25 & 10 \end{bmatrix}\begin{bmatrix} 16 \\ 1 \end{bmatrix}=\begin{bmatrix} 13 \\ 5 \end{bmatrix}=\begin{bmatrix} M \\ E \end{bmatrix}$$

Esercizio 11

La matrice data ha determinante $2h+2t-3-2t=2h-3$ e non dipende da t; quindi è invertibile purché non sia multiplo di 3. Per $h=0$ non è invertibile, ma per $h=1$ sì, poiché vale $-1\equiv 26$. L'inverso di 26 è ancora 26, quindi la matrice inversa è:

$$\begin{bmatrix} 26(1+t) & -26(3+2t) \\ -26 & 52 \end{bmatrix}\equiv\begin{bmatrix} -(1+t) & 3+2t \\ 1 & -2 \end{bmatrix}$$

Allora risulta:

$$\begin{bmatrix} -(1+2) & 3+4 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 16 \\ 1 \end{bmatrix}=\begin{bmatrix} -3 & 7 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 16 \\ 1 \end{bmatrix}=\begin{bmatrix} 13 \\ 14 \end{bmatrix}=\begin{bmatrix} M \\ N \end{bmatrix}$$

$$\begin{bmatrix} -(1+7) & 3+14 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 18 \\ 15 \end{bmatrix}=\begin{bmatrix} -8 & 17 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 18 \\ 15 \end{bmatrix}=\begin{bmatrix} 3 \\ 15 \end{bmatrix}=\begin{bmatrix} C \\ O \end{bmatrix}$$

$$\begin{bmatrix} -(1+5) & 3+10 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 12 \\ 1 \end{bmatrix}=\begin{bmatrix} -6 & 13 \\ 1 & -2 \end{bmatrix}\begin{bmatrix} 12 \\ 1 \end{bmatrix}=\begin{bmatrix} 22 \\ 10 \end{bmatrix}=\begin{bmatrix} V \\ J \end{bmatrix}$$

Esercizio 12

La matrice **B** deve avere tre righe, perché deve essere possibile moltiplicarla per la matrice **A** e deve avere due colonne perché si deve avere come risultato una matrice quadrata, con tante righe quante ne ha **A** e quindi di ordine 2.
Risulta quindi:

$$\begin{bmatrix}2 & 3 & 1\\ 9 & 1 & 0\end{bmatrix}\begin{bmatrix}a & b\\ c & d\\ e & f\end{bmatrix}=\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\Rightarrow\begin{cases}2a+3c+e=1\\ 2b+3d+f=0\\ 9a+c=0\\ 9b+d=1\end{cases}\Rightarrow\begin{cases}c=-9a\\ e=1+25a\\ d=1-9b\\ f=25b-3\end{cases}$$

Scelti allora per esempio $a = b = 1$, la matrice B risulta:

$$\begin{bmatrix}1 & 1\\ -9 & -8\\ 26 & 22\end{bmatrix},$$

ma si potrebbero anche scegliere a=1 e b=0, o viceversa, ottenendo una matrice più semplice.

Bisogna ora decidere se bisogna usare **A** per crittografare e **B** per decrittografare o viceversa.

La matrice **A** trasforma un vettore a tre componenti in un vettore a due componenti, quindi non dà luogo ad un omomorfismo iniettivo. Se l'omomorfismo non è iniettivo, e quindi vettori diversi possono essere trasformati nello stesso vettore, sicuramente non sarà possibile decrittografare quanto ottenuto, quindi si deve usare **B** per crittografare e poi **A** per decrittografare.

$$\begin{bmatrix}P\\ A\end{bmatrix}\rightarrow\begin{bmatrix}16\\ 1\end{bmatrix};\begin{bmatrix}R\\ O\end{bmatrix}\rightarrow\begin{bmatrix}18\\ 15\end{bmatrix};\begin{bmatrix}L\\ A\end{bmatrix}\rightarrow\begin{bmatrix}12\\ 1\end{bmatrix};$$

Allora:

$$\begin{bmatrix}1 & 1\\ -9 & -8\\ 26 & 22\end{bmatrix}\begin{bmatrix}16\\ 1\end{bmatrix}=\begin{bmatrix}17\\ 10\\ 6\end{bmatrix}=\begin{bmatrix}Q\\ J\\ F\end{bmatrix};\ \begin{bmatrix}1 & 1\\ -9 & -8\\ 26 & 22\end{bmatrix}\begin{bmatrix}18\\ 15\end{bmatrix}=\begin{bmatrix}6\\ 15\\ 15\end{bmatrix}=\begin{bmatrix}F\\ O\\ O\end{bmatrix};\begin{bmatrix}1 & 1\\ -9 & -8\\ 26 & 22\end{bmatrix}\begin{bmatrix}12\\ 1\end{bmatrix}=\begin{bmatrix}13\\ 23\\ 10\end{bmatrix}=\begin{bmatrix}M\\ W\\ J\end{bmatrix}.$$

Moltiplicando i tre vettori ottenuti per **A**, sulla sinistra, poiché **AB**=**I**, si riottene "parola".

Eserciziario – Matrice inversa

TESTO DEGLI ESERCIZI

Esercizio 1

Sia data la matrice $M=\begin{bmatrix}1 & -1 & 2\\ 0 & 1 & 1\\ 3 & 0 & -1\end{bmatrix}$.

Usare il metodo di Gauss Jordan per trovarne la matrice inversa.

Esercizio 2

Determinare la matrice inversa della matrice $\begin{bmatrix}4 & 2 & 3\\ 6 & -1 & 1\\ 2 & 1 & 2\end{bmatrix}$ pensando che in suoi coefficienti siano in $\mathbb{Q}$, in $\mathbb{Z}_5$, in $\mathbb{Z}_7$, in $\mathbb{Z}_{11}$.

Esercizio 3

Determinare la matrice inversa della matrice $M=\begin{bmatrix}4 & 2 & 1\\ 1 & -2 & 2\\ 3 & 4 & -1\end{bmatrix}$ pensando che in suoi coefficienti siano in $\mathbb{Q}$, in $\mathbb{Z}_5$, in $\mathbb{Z}_7$, in $\mathbb{Z}_{11}$.

Esercizio 4

Determinare la matrice inversa della matrice $M=\begin{bmatrix}3 & -1 & 2\\ 1 & -2 & 2\\ 3 & 4 & -1\end{bmatrix}$ pensando che in suoi coefficienti siano in $\mathbb{Q}$, in $\mathbb{Z}_5$, in $\mathbb{Z}_7$, in $\mathbb{Z}_{11}$.

SOLUZIONE DEGLI ESERCIZI

Esercizio 1

Il metodo richiesto prevede di accostare sulla destra la matrice identica alla matrice assegnata, e di applicare alla matrice ottenuta il metodo usato per i sistemi lineari.

Si parte quindi dalla matrice:

$$\begin{bmatrix} 1 & -1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 3 & 0 & -1 & 0 & 0 & 1 \end{bmatrix} : 3° \Leftrightarrow 3°-3\times 1° \Rightarrow$$

$$\begin{bmatrix} 1 & -1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 3 & -7 & -3 & 0 & 1 \end{bmatrix} : 3° \Leftrightarrow 3°-3\times 2° \text{ e } 1° \Leftrightarrow 1° + 2° \Rightarrow$$

$$\begin{bmatrix} 1 & 0 & 3 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & -10 & -3 & -3 & 1 \end{bmatrix} \Rightarrow \begin{bmatrix} 1 & 0 & 3 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & \frac{3}{10} & \frac{3}{10} & -\frac{1}{10} \end{bmatrix} : 2° \Leftrightarrow 2°-3° \text{ e } 1° \Leftrightarrow 1° -3\times 3° \Rightarrow$$

$$\begin{bmatrix} 1 & 0 & 0 & \frac{1}{10} & \frac{1}{10} & \frac{3}{10} \\ 0 & 1 & 0 & -\frac{3}{10} & \frac{7}{10} & \frac{1}{10} \\ 0 & 0 & 1 & \frac{3}{10} & \frac{3}{10} & -\frac{1}{10} \end{bmatrix}$$ la matrice sulla destra è quella richiesta.

Controllo:

$$\begin{bmatrix} \frac{1}{10} & \frac{1}{10} & \frac{3}{10} \\ -\frac{3}{10} & \frac{7}{10} & \frac{1}{10} \\ \frac{3}{10} & \frac{3}{10} & -\frac{1}{10} \end{bmatrix} \begin{bmatrix} 1 & -1 & 2 \\ 0 & 1 & 1 \\ 3 & 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Esercizio 2

La matrice da modificare per ottenere la matrice inversa è: $\begin{bmatrix} 4 & 2 & 3 & 1 & 0 & 0 \\ 6 & -1 & 1 & 0 & 1 & 0 \\ 2 & 1 & 2 & 0 & 0 & 1 \end{bmatrix}$.

Col metodo di GaussJordan si ottiene, nei vari casi:

- in $\mathbb{Q}$:

$$\begin{bmatrix} 1 & 0 & 0 & \frac{3}{8} & \frac{1}{8} & \frac{-5}{8} \\ 0 & 1 & 0 & \frac{5}{4} & \frac{-1}{4} & \frac{-7}{4} \\ 0 & 0 & 1 & -1 & 0 & 2 \end{bmatrix}$$

- in $\mathbb{Z}_5$:

$$\begin{bmatrix} 1 & 0 & 0 & 1 & 2 & 0 \\ 0 & 1 & 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 4 & 0 & 2 \end{bmatrix}$$

- in $\mathbb{Z}_7$:

$$\begin{bmatrix} 1 & 0 & 0 & 3 & 1 & 2 \\ 0 & 1 & 0 & 3 & 5 & 0 \\ 0 & 0 & 1 & 6 & 0 & 2 \end{bmatrix}$$

- in $\mathbb{Z}_{11}$:

$$\begin{bmatrix} 1 & 0 & 0 & 10 & 7 & 9 \\ 0 & 1 & 0 & 4 & 8 & 1 \\ 0 & 0 & 1 & 10 & 0 & 2 \end{bmatrix}$$

Quindi in tutti i casi la matrice è invertibile.

Esercizio 3

La matrice da modificare per ottenere la matrice inversa è: $\begin{bmatrix} 4 & 2 & 1 & 1 & 0 & 0 \\ 1 & -2 & 2 & 0 & 1 & 0 \\ 3 & 4 & -1 & 0 & 0 & 1 \end{bmatrix}$

Col metodo di GaussJordan si ottiene, nei vari casi:

- in $\mathbb{Q}$:

$$\begin{bmatrix} 1 & 0 & \frac{3}{5} & 0 & \frac{2}{5} & \frac{1}{5} \\ 0 & 1 & \frac{-7}{10} & 0 & \frac{-3}{10} & \frac{1}{10} \\ 0 & 0 & 0 & 1 & -1 & -1 \end{bmatrix}$$

  si vede che la matrice non è invertibile, infatti l'ultima riga non consente di proseguire il calcolo;

- in $\mathbb{Z}_5$:

$$\begin{bmatrix} 1 & 3 & 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 4 & 4 \end{bmatrix}$$

- in $\mathbb{Z}_7$:

$$\begin{bmatrix} 1 & 0 & 2 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 6 & 5 \\ 0 & 0 & 0 & 1 & 6 & 6 \end{bmatrix}$$

- in $\mathbb{Z}_{11}$:

$$\begin{bmatrix} 1 & 0 & 5 & 0 & 7 & 9 \\ 0 & 1 & 7 & 0 & 3 & 10 \\ 0 & 0 & 0 & 1 & 10 & 10 \end{bmatrix}$$

Quindi in tutti i casi la matrice non è invertibile.

Esercizio 4

La matrice da modificare per ottenere la matrice inversa è: $\begin{bmatrix} 3 & -1 & 2 & 1 & 0 & 0 \\ 1 & -2 & 2 & 0 & 1 & 0 \\ 3 & 4 & -1 & 0 & 0 & 1 \end{bmatrix}$

Col metodo di GaussJordan si ottiene, nei vari casi:

- in $\mathbb{Q}$:

$$\begin{bmatrix} 1 & 0 & 0 & \frac{6}{5} & \frac{-7}{5} & \frac{-2}{5} \\ 0 & 1 & 0 & \frac{-7}{5} & \frac{9}{5} & \frac{4}{5} \\ 0 & 0 & 1 & -2 & 3 & 1 \end{bmatrix}$$

  si vede che la matrice è invertibile;

- in $\mathbb{Z}_5$:

$$\begin{bmatrix} 1 & 3 & 0 & 0 & 3 & 1 \\ 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 3 & 3 \end{bmatrix}$$

  In questo caso invece la matrice non è invertibile, visto che i primi tre elementi dell'ultima riga sono nulli. quindi la stessa matrice può essere invertibile se i coefficienti sono in un campo e non invertibile in un altro campo;

- in $\mathbb{Z}_7$:

$$\begin{bmatrix} 1 & 0 & 0 & 4 & 0 & 1 \\ 0 & 1 & 0 & 0 & 6 & 5 \\ 0 & 0 & 1 & 5 & 3 & 1 \end{bmatrix}$$

- in $\mathbb{Z}_{11}$:

$$\begin{bmatrix} 1 & 0 & 0 & 10 & 3 & 4 \\ 0 & 1 & 0 & 3 & 4 & 3 \\ 0 & 0 & 1 & 9 & 3 & 1 \end{bmatrix}$$

Quindi la matrice è invertibile, a parte il caso in cui i coefficienti sono in $\mathbb{Z}_5$.